UNIVERSITI TEKNOLOGI MARA
Cawangan Kelantan

ACADEMICA
PRESS SOLUTIONS

GSISS2023

Proceedings of 1st Glocal Symposium on Information and Social Sciences (GSISS) 2023

20 - 21 June 2023, Kelantan, Malaysia

eISBN
978-629-97536-6-7

DOI: 10.5281/zenodo.8201436

Proceedings of Glocal Symposium on Information and Social Sciences (GSISS) 2023

Published 1 August 2023

eISBN 978-629-97536-6-7

Collection URL: **https://zenodo.org/communities/gsiss**

DOI: 10.5281/zenodo.8201436

Published by:
Academica Press Solution 003428568-X
Batu 23, Kg Jias,
17000 Pasir Mas,
Kelantan, MALAYSIA
Email: contact.digit360@gmail.com

Table of Contents

Research Article

Exploring the Ethical Dimensions of Information Systems: Challenges and Opportunities

Nur Ratihah Ramzi[1], Siti Nur Huwaida Mohamed[2], Umie Izzati Ismail[3], and Ghazali Osman[4*]

[1] UiTM Kelantan Branch, Malaysia; 2020602174@student.uitm.edu.my; 0009-0007-3552-2166
[2] UiTM Kelantan Branch, Malaysia; 2020872934@student.uitm.edu.my; 0009-0000-8870-6398
[3] UiTM Kelantan Branch, Malaysia; 2020828328@student.uitm.edu.my; 0009-0002-9569-8175
[4] UiTM Kelantan Branch, Malaysia; ghaza936@uitm.edu.my; 0000-0001-5167-5292
[*] Correspondence: ghaza936@uitm.edu.my, +6019-9198994.

Abstract: *This article explores the ethical dimensions of information systems, focusing on the challenges and opportunities they present. It examines five key areas: privacy and data protection, security and cybersecurity, algorithmic bias and fairness, social impact and inequality, and intellectual property and digital rights. The article highlights the significance of ethical considerations in these areas, emphasising the need to balance data-driven insights with privacy rights, ensure security and protection against cyber threats, address biases in algorithmic decision-making, promote social equity, and respect intellectual property. It discusses organisations' ethical challenges in these areas and explores ethical decision-making frameworks that can guide responsible behaviour. The paper sheds light on the complicated environment that ethical decision-making organisations confront by highlighting their ethical problems in various areas. It discusses the necessity for ethical frameworks that can direct moral behaviour and judgement to help organisations successfully deal with these difficulties. The article also acknowledges the opportunities for ethical innovation and positive societal impact that responsible information systems present. By understanding and addressing these ethical dimensions, organisations can navigate the challenges, seize opportunities, and promote the development of ethical information systems. Overall, this study emphasises how critical it is for information systems to consider ethical considerations. It encourages businesses to recognise and solve the ethical issues they confront while maximising the chances for morally righteous behaviour.*

Keywords: Information systems, ethical conduct, societal influence, property rights, and judgement.

DOI: 10.5281/zenodo.8180679

1. INTRODUCTION

Information systems have become a vital part of our daily lives in today's digitally connected world, revolutionising the way we communicate, work, and access information. However, the unmatched power and reach of these technologies also bring with them significant ethical conundrums that demand careful thought. Thus, the article dives into the multidimensional landscape of ethical considerations surrounding information systems, shining light on both the obstacles and potential for responsible and sustainable technological growth. As we navigate the enormous and ever-changing world of information technologies, it becomes increasingly important to consider the ethical implications of its deployment. This study goes beyond technical considerations to investigate the enormous influence information systems have on individuals, societies, and the planet. From privacy problems and data breaches to algorithmic biases and the ethical governance of artificial intelligence, the piece confronts the intricate ethical challenges that require immediate attention.

Furthermore, this article emphasises the substantial opportunities that exist within this ethical framework. Organisations and politicians may promote an atmosphere that fosters responsible and inclusive innovation by recognising and addressing these obstacles. Ethical information systems could improve openness, safeguard privacy, promote fairness, and advance societal progress. The purpose of this paper is to shed light on these prospects and function as a catalyst for meaningful discussions and actions in the field of information systems. This paper invites readers to embark on a thought-provoking trip through a thorough examination of case studies, theoretical frameworks, and real-world situations. It investigates the ethical elements of data collection, storage, and use, by considering the implications to individuals' autonomy, equity, and well-being. It also examines the ethical considerations of emerging technologies such as blockchain, the Internet of Things (IoT), and machine learning, as well as their potential benefits and threats. The main problem is lacking comprehensive exploration and clear guidelines for addressing the ethical dimensions of information systems poses challenges in ensuring responsible and ethical use, while also limiting the opportunities for trust, fairness, and accountability in the digital landscape.

Finally, this paper aims to provide a broad review of the ethical difficulties and opportunities presented by information systems. It attempts to empower individuals, organisations, and politicians to make informed decisions that prioritise ethical behaviour and social responsibility by promoting a sophisticated awareness of these concerns. We can navigate the changing digital landscape while preserving the values and ideals that are vital for a just and equitable society.

2. METHODOLOGY

This study's methodology relies on a comprehensive review of relevant previous research and scholastic papers to ensure a comprehensive understanding of the topic. The paper collected valuable insights, hypotheses, and empirical evidence by examining previous work, such as academic publications, conference papers, and relevant research projects. Meanwhile, the evaluation entails selecting key publications addressing information systems' ethical aspects and associated challenges and opportunities. All papers were subjected to in-depth analysis and evaluation to extract pertinent data, ideas, and conclusions. The technique also evaluated the credibility and applicability of selected publications, considering the authors' previous research, the study's rigour, and the data analysis precision.

This paper aims to expand on the material body and advance our understanding of the ethical aspects of information systems by using the findings from previous studies. The methodology allows the integration of many viewpoints, ideas, and empirical data to present a thorough overview of the subject and offer insightful information on challenges and opportunities in this field.

3. LITERATURE REVIEW

Information systems are altering industries, transforming economies, and revolutionizing how people interact with technology in modern life. However, in recent years, there has been a lot of discussion about the ethical implications of information systems. This literature review's goal is to look at the existing research and scholarly debate on the ethical elements of information systems, stressing the challenges and potential for ethical decision-making and responsible innovation. The survey of the literature reveals a variety of ethical issues concerning information technology. Ethics serve as a guide for ensuring that individuals act with honesty and integrity. The same principles are anticipated in the domain of information technology, where technology is expected to operate in a helpful and supportive manner. Information technology (IT) is continuously developed, monitored, and used following a code of ethics. The management of personal information should not be used for detrimental or negative purposes. As the influence of technology grows, the encompassing ethical framework must also evolve to protect the interests of IT-reliant individuals and businesses. Data administration and privacy represent significant obstacles in the field of information technology. In order to assure the preservation and dependability of data, it is essential to address these challenges with consistency and seriousness, taking ethical considerations in IT into account. This includes the creation, organization, deletion, and controlled access to information, among other facets. By adhering to ethical principles in IT, professionals can effectively address these challenges and prioritize the required safeguards, nurturing a trustworthy environment (McCann School of Business & Technology, 2023).

Privacy and data protection are two major concerns. Researchers have emphasized the need to safeguard individuals' privacy rights, obtain informed permission, and establish rigorous security measures to preserve sensitive information in light of the widespread gathering and use of personal data (Acquisti & Mittelstadt, 2016). Data breaches, monitoring practices, and the monetization of personal information have spurred concerns about how to strike a balance between data-driven innovation and individual privacy rights. Fairness and algorithmic bias have emerged as key challenges in information systems. The growing dependence on algorithms in decision-making processes, such as those used in hiring, criminal justice, and financial systems, has prompted worries about biases being perpetuated or exacerbated (Barocas et al., 2016). Scholars have investigated the ethical issues related to algorithmic decision-making, emphasizing the importance of addressing biases, ensuring fairness, and providing options for recourse or restitution in cases of algorithmic harm. Furthermore, the assessment of the literature emphasizes the digital gap and its ethical consequences. Access disparities to information and communication technology have the power to amplify already existing societal divides (Warschauer, 2003). Addressing inequities in access, fostering digital inclusion, and ensuring that technology improvements do not perpetuate or worsen social injustices are all examples of ethical considerations in information systems (Van Dijk, 2006).

Opportunities for ethical information systems have evolved amid these obstacles. The importance of transparency and explainability in ethical decision-making cannot be overstated. Researchers have investigated approaches for making algorithms, and decision-making processes more transparent, allowing individuals to understand the factors impacting outcomes and dispute or question the conclusions (Doshi-Velez et al., 2017). Transparent information systems can improve accountability, foster confidence, and motivate organisations and institutions to act responsibly. The ethical regulation of artificial intelligence (AI) has received much attention recently. The rapid evolution of artificial intelligence technology has generated concerns regarding the responsible creation and deployment of these systems. Researchers have proposed frameworks, rules, and principles for ethical AI governance, emphasising the value of multidisciplinary partnerships, ethics boards, regulatory procedures, and stakeholder engagement (Floridi et al., 2018). Ethical AI governance seeks to connect AI systems with social norms, prioritise human well-being, and limit possible risks (Jobin et al., 2019).

Ethical design and user-centricity are critical issues for responsible information systems. Design ethics creates a relationship between a product and a user, encouraging responsible and moral behaviour. The ethical design focuses on a product's "goodness" element to benefit the consumer, environment, and society. Practically speaking, there is no precise definition of an "ethical" design system (*Ethical Designs: Meaning, Guide for Designers | NetBramha Studios*, n.d.). Researchers have advocated for including ethical issues in the design and development process, emphasizing the relevance of user empowerment, autonomy, and well-being (Friedman et al., 2002; Friedman & Kahn Jr, 2003). Ethical design practices entail incorporating inclusion, accessibility, and user privacy into developing information systems and promoting technologies aligned with social requirements and ideals.

The literature study demonstrates the complex ethical environment that surrounds information technology. Important issues, including privacy, algorithmic biases, social inequalities, and the digital gap, highlight the need to make moral decisions and act responsibly. On the other hand, there are many chances to promote transparency, fairness, responsible AI governance, and user-centric design, all of which help to develop moral information systems. Policymakers, organisations, and individuals can design, implement, and use information systems that prioritise social responsibility, sustainability, and preserving individual and societal values by carefully examining the insights and recommendations presented in the literature.

4. Findings

We reviewed numerous articles and journals for this study using an online database, and the review has concluded that several ethical issues exist in various contexts, including privacy and data protection, security and cybersecurity, algorithmic bias and fairness, social impact and inequality, and intellectual property rights. understanding and addressing these challenges are essential for fostering responsible and ethical use of technology while protecting individual rights and societal values.

4.1 Privacy and data protection

An information system (IS) requires collecting, storing, and utilising personal data. Privacy and data protection issues result from difficulties balancing preserving individuals' privacy rights using data-driven insights. According to France Belanger and Robert E. Crossler (2011), information privacy is a subset of the broader concept of privacy. The authors have identified four (4) dimensions of privacy: the privacy of a person, the privacy of personal behaviour, the privacy of personal communication, and the privacy of personal data (France Belanger & Robert E. Crossler's, 2011). The authors discovered that most interpretations of privacy concepts refer to a human right, albeit in varied contexts (France Belanger & Robert E. Crossler's, 2011). Since most privacy research has been conducted on this concept, France Belanger and Robert E. Crossler's (2011) review is centred on information privacy. This singular focus is unsurprising, given that technology is the underlying cause of numerous information privacy issues (and related solutions).

Organisations face a dilemma due to legal protections when acquiring data. Organisations face a challenge when attempting to collect relevant and meaningful information while respecting the privacy of individuals. They are responsible for ensuring that data is collected in an ethical, transparent, and justifiable manner. Transparency is required regarding the categories of data collected, the specific purposes for which it will be used, and any third parties managing it. Concerns about privacy and confidentiality arise when sharing data. Companies must evaluate with whom and under what conditions they share information. They should establish contracts and procedures for data sharing that adhere to ethical standards and privacy laws. Discussion of data-sharing policies and receipt of their information is the most crucial step in protecting privacy. Each company should support both proprietary and shared data in practice. Since it is required for company management, only those personnel would have access to the confidential information (Stefansson, 2002).

Users' autonomy and privacy must be respected by obtaining their informed assent. Organisations should provide transparent and readily comprehensible information about their data collection and usage practices, allowing users to make informed decisions. However, obtaining valid consent can be difficult, as users may not always comprehend the ramifications of their data-sharing decisions.

4.2 Security and Cybersecurity

Security and cybersecurity are essential because they protect private data, prevent unauthorised access, and mitigate potential information system threats. Organisations must prioritise robust security measures to secure data, maintain system dependability, and preserve the trust of users and stakeholders. The prevalence of data breaches, which can have severe repercussions for individuals and organisations, is one of the most pressing security concerns. Data breaches may expose sensitive personal information, resulting in identity theft, financial loss, and reputational damage. Unauthorised access may lead to a denial-of-service attack. The corruption of system software and the malfunctioning of system hardware are equally severe consequences. Sundeswaran et al. (2018) state that data breaches frequently result in a loss of revenue for the company or industry. Businesses must implement safeguards such as firewalls, intrusion detection systems, and encryption procedures to protect themselves from external threats and unauthorised access to sensitive data.

Cyber threats constantly evolve as malicious actors seek to exploit vulnerabilities in information systems. These threats include malware, phishing schemes, ransomware, and social engineering techniques are among these threats. Sundareswaran et al. (2018) proposed standard methods for preventing data intrusions, such as reducing data transfer: Since losing removable media poses a danger to the data, it would be preferable for an organisation to prohibit data transfer between devices. Therefore, material bondholders and discs permanently erase the selected data files without leaving a copy of the file body. Consequently, removing sensitive data prevents data breaches. Next, the prohibition of non-encrypted devices increases the likelihood of data leakage. Therefore, ensuring that all unsecured portable devices used in an organisation are prohibited is essential. a password generated at random, among other factors. Creating a password that is difficult to anticipate and unpredictable is crucial for preventing unauthorised data access. In addition, it is advisable to alter passwords frequently. In addition, there are automated security measures: Automated systems can evaluate the server and firewall configuration, password settings, and other security settings to reduce the likelihood of data breaches. Lastly, establishing a breach response strategy would assist in notifying management by informing them of a data breach.

Information system vulnerabilities may result from both technological and human factors. Inadequate security measures, outdated software, and improper configurations can cause technical vulnerabilities. Human vulnerabilities include insider attacks, social engineering, and inadequate password management. Organisations must routinely audit their security procedures and evaluate their risks to identify vulnerabilities and implement the corresponding countermeasures.

4.3 Algorithmic Bias and Fairness

Fairness and algorithmic bias are significant ethical concerns of information technology. There is an increasing fear that as automated decision-making systems proliferate, they may inadvertently reinforce biases and produce unfair and discriminatory outcomes. The difficulty with algorithmic bias is that the data used to construct and train the algorithms may contain biases. If the training data is biased or unrepresentative, the algorithm may detect and amplify prejudices, leading to discriminatory outcomes. The increasing prevalence of automated decision-making systems in sectors such as human resources, lending, criminal justice, and healthcare could have far-reaching consequences.

For instance, bias in artificial intelligence (AI) can significantly affect individuals and society. Discrimination is a major concern regarding biased artificial intelligence systems, as they can perpetuate and exacerbate existing inequalities (Sweeney, 2013). In the criminal justice system, for instance, biased algorithms can unjustly treat certain groups, especially people of colour, who are more likely to be wrongfully convicted or receive harsher sentences. Then, AI bias may negatively impact the accessibility of essential services such as finance and healthcare. Due to the underrepresentation of certain groups in credit scoring systems due to biased algorithms, such as people of colour and those with a lower socioeconomic status, it can be more challenging for them to obtain loans or mortgages (Dwork et al., 2012).

Developing inclusive algorithms and ensuring that the training set contains diverse, objective, and representative data is essential to combat algorithmic bias. It is crucial to consider any possible biases in the data and take steps to eliminate them. Correcting imbalances and ensuring impartiality may require pre-processing techniques such as data augmentation or sampling techniques.

4.4 Social Impact and Inequality

The societal effects of information systems extend far beyond their technical applications. These technologies can exacerbate social disparities and digital divides between individuals and communities. Recognising these implications to promote equal access to technology and mitigate its negative effects on marginalised communities is essential. The most disadvantaged and marginalised individuals are at imminent risk of digital exclusion (Heponiemi et al., 2021). According to findings from the author's previous investigations, the internet exacerbates existing social inequalities.

Access to technology may be difficult for marginalised individuals, such as those living in rural or low-income areas, due to disparities in infrastructure, cost, or a lack of digital literacy. Due to this, certain groups of people experience a "digital divide," in which they have limited or no access to the opportunities and resources provided by information technologies. It is necessary to implement measures that promote the use of accessible, affordable technology by all and enhance digital literacy and skill development among underserved populations.

Information systems can also influence the dynamics and power structures of society. They can affect individuals' interactions, access to information, and participation in social, economic, and political activities. These systems may either reinforce existing power disparities or provide opportunities for participation and empowerment. Systems must be designed with inclusivity, participation, and democratic principles as top priorities to foster positive societal outcomes. The development and implementation of information systems can be made to better reflect the requirements and aspirations of local communities by involving various stakeholders and considering their perspectives (Heponiemi et al., 2021). To mitigate the negative effects on marginalised communities, promoting digital inclusion, assuring equal access, and addressing their challenges should be the top priorities. It necessitates collaboration between government entities, organisations, and community-based initiatives to provide resources, promote the growth of digital infrastructure, and provide training and educational programs.

4.5 Intellectual property rights and digital rights

Digital and intellectual property rights are major ethical concerns in information technology. These rights encompass owning and preserving original art, innovations, and digital content. In order to promote responsible and ethical information use, organisations must manage intellectual property issues such as plagiarism, attribution, and fair use.

Plagiarism is a severe issue in the digital age, where a vast amount of material is easily accessible and can be copied or reproduced without proper attribution. Plagiarism is the practice of using someone else's ideas or labour without giving them credit. According to Nurhidayah et al.'s (2021) statement, the actions may include relabeling and repackaging counterfeit goods to conceal their country of origin. n. Although the rules in Malaysia grant, the Royal Customs Office the authority to take enforcement action against counterfeiters by requesting information on any activity at free trade zones from the operators (Nurhidayah et al., 2021), the Royal Customs Office has not exercised this authority. Organisations should develop guidelines and training sessions that emphasise originality and correct attribution to maintain ethical standards.

The most important part of intellectual property rights attribution involves identifying and crediting the original authors or information providers. In addition to respecting artists' rights, accurate attribution fosters accountability, transparency, and confidence in information systems. Organisations should encourage users and staff to provide accurate and exhaustive citations, references, and acknowledgements when using or sharing digital content. By encouraging a culture of attribution, organisations promote the ethical and accountable transmission of knowledge.

5. Discussion

Based on the highlighted findings, organisations must emphasise the ethical collection, storage, and use of personal information. It is included that data should be as accurate, truthful, or reliable as possible that adhere to privacy laws and ethical norms. When it comes to protecting private data, preventing unauthorized access, and lowering potential hazards, organizations need to establish stringent security measures. These include the implementation of protective measures such as firewalls, intrusion detection systems, and encryption protocols. Information systems have the potential to either exacerbate current social imbalances or give opportunities for empowerment. Information systems can exacerbate social disparities and create digital divides. Access to technology may be limited for marginalized individuals due to infrastructure disparities, cost, or lack of digital literacy. Bridging the digital divide requires efforts to promote equal access to technology, enhance digital literacy, and provide resources for underserved populations (Cheety.K, 2018). Inclusive information system design and involving stakeholders in decision-making processes can help address social inequalities and empower marginalized communities. Initiatives should be made to close the digital divide by increasing access to technology, developing digital literacy, and addressing infrastructure and economic hurdles.

Plagiarism, attribution, and fair use are examples of intellectual property rights challenges that organisations must handle. By promoting a strong understanding of intellectual property rights, organisations can promote responsible information use and respect for the creative contributions of others. This approach helps encourage integrity, transparency, and credibility in information systems and reinforces ethical practices within the organisation and beyond. Organizations should establish guidelines and training sessions to promote originality, proper attribution, and ethical standards. Accurate attribution not only respects artists' rights but also promotes accountability, transparency, and confidence in information systems. These findings draw attention to the difficulties and moral issues that surround information technology. In order to address these concerns and establish a digital environment that respects privacy, provides security, encourages justice, lowers inequality, and defends intellectual property and digital rights, organisations, policymakers, and individuals must work together. Information systems can be used for the benefit of society while minimising any potential drawbacks by embracing ethical practices. e licences, and refraining from unauthorised distribution or replication of digital content.

6. Conclusion

This study has examined the ethical implications of information systems. There is a need to increase awareness and action regarding the ethical aspects of information systems both as a principle and as practice. However, this quick development in IS has given rise to several ethical issues that must be resolved. The study explored many significant ethical issues affecting information systems, such as bias and discrimination, cybersecurity, privacy and data protection, and the digital divide.

Organisations, policymakers, and individuals must be aware of the ethical ramifications of their choices when it comes to information systems. Furthermore, this research underlined the benefits of implementing ethical norms in information systems. It can create a more egalitarian and inclusive digital landscape by including ethical considerations in the design, development, and usage of information technologies. Ethical information systems can empower people, promote social justice, and build user trust. Organisations must develop strong ethical norms and frameworks to guide the development, deployment, and use of information systems. Legislators and regulators should adopt legislation and regulations that defend individuals' rights, protect data privacy, and promote ethical behaviour in the digital sphere. Further study can aid in the identification of emerging ethical concerns and the development of innovative solutions to resolve them. By consistently implementing ethical practices, we can build the full potential of information systems, thereby fostering positive societal outcomes.

Acknowledgements: The authors would like to express our gratitude to God, on whom we ultimately rely for direction. Our deepest appreciation is also extended to Dr Ghazali bin Osman, for his invaluable guidance, support, and expertise throughout the duration of this paper. We also want to thank the faculty members of Information System Management for their commitment to providing a conducive learning environment. Their teachings and lectures have broadened my knowledge and helped me develop the necessary skills for this undertaking.

References

Acquisti, A. (2011). Privacy in the Age of Augmented Reality. *Carnegie Mellon University*. https://pdfs.semanticscholar.org/b169/609adfd0962d6c6fd20622dca783266c0dab.pdf

Barocas, S., & Selbst, A. D. (2016). Big Data's Disparate Impact. *California Law Review*, 104(3), 671-732. https://www.courts.ca.gov/documents/BTB24-2L-2.pdf

Belanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *Management Information Systems Quarterly*, 35(4), 1017. https://doi.org/10.2307/41409971

Chetty, K., Qigui, L., Gcora, N., Josie, J., Wenwei, L., & Fang, C. (2018). Bridging the digital divide: measuring digital literacy. Economics, 12(1).

Doshi-Velez, F., & Kim, B. (2017). Towards A Rigorous Science of Interpretable Machine Learning. *arXiv preprint arXiv:1702.08608*. https://www.scinapse.io/papers/2594475271

Dwork, C., Hardt, M., Pitassi, T., Reingold, O., & Zemel, R. (2012). Fairness through awareness. *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, 214-226. https://doi.org/10.48550/arXiv.1104.3913

Ethical Designs: Meaning, Guide for designers | NetBramha Studios. (n.d.). https://netbramha.com/blogs/ethical-design-meaning

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Luetge, C. (2018). AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*, 28(4), 689-707. https://link.springer.com/article/10.1007/s11023-018-9482-5

Friedman, B., & Kahn Jr, P. H. (2003). Human Values, Ethics, and Design. *Handbook of Human-Computer Interaction*, 2, 1177-1201. https://depts.washington.edu/hints/publications/Human_Values_Ethics_Design.pdf

Friedman, B., Kahn Jr, P. H., & Borning, A. (2002). Value Sensitive Design and Information Systems. *Human-Computer Interaction in Management Information Systems: Foundations*, 348-372. https://www.researchgate.net/publication/229068326_Value_Sensitive_Design_and_Information_Systems

Heponiemi, T., Gluschkoff, K., Leemann, L., Manderbacka, K., Aalto, A., & Hyppönen, H. (2021). Digital inequality in Finland: Access, skills and attitudes as social impact mediators. *New Media & Society*, 146144482110230. https://doi.org/10.1177/14614448211023007

Jobin, A., Ienca, M., & Vayena, E. (2019). The Global Landscape of AI Ethics Guidelines. *Nature Machine Intelligence*, 1(9), 389-399. https://www.nature.com/articles/s42256-019-0088-2

McCann School of Business & Technology. (2023). Why Ethics Are Important in Information Technology. *McCann*. https://www.mccann.edu/importance-of-ethics-in-information-technology/#:~:text=Part%20of%20ethics%20in%20information,gains%20to%20meet%20our%20needs.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The Ethics of Algorithms: Mapping the Debate. *Big Data & Society*, 3(2), 2053951716679679. https://journals.sagepub.com/doi/10.1177/2053951716679679

Mkuzangwe, N. N. P., & Khan, Z. C. (1999). Cyber-Threat Information-Sharing Standards: A Review of Evaluation Literature. *The African Journal of Information and Communication*. https://doi.org/10.23962/10539/29191

Nurhidayah Abdullah, Hanira Hanafi & Nazli Ismail Nawang. (2021). Digital Era and Intellectual Property Challenges in Malaysia. *Pertanika Journal of Social Science and Humanities*, 29(S2). https://doi.org/10.47836/pjssh.29.s2.14

O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. *Crown Publishing Group*. https://edisciplinas.usp.br/pluginfile.php/4605464/mod_resource/content/1/%28FFLCH%29%20LIVRO%20Weapons%20of%20Math%20Destruction%20-%20Cathy%20ONeal.pdf

Stefansson, G. (2002). Business-to-business data sharing: A source for integration of supply chains. *International Journal of Production Economics*, 75(1–2), 135–146. https://doi.org/10.1016/s0925-5273(01)00187-6

Sundareswaran, V., Divyalakshmi, M., & Poornima, M. (2018). Study Of Cybersecurity in Data Breaching. *International Journal of Advance Engineering and Research Development*, 5(03), 1513–1516. https://www.researchgate.net/publication/325300571_STUDY_OF_CYBERSECURITY_IN_DATA_BREACHING

Sweeney, L. (2013). Discrimination in online ad delivery. *Communications of the ACM*, 56(5), 44-54. https://doi.org/10.48550/arXiv.1301.6822

Van Dijk, J. (2006). Digital Divide Research, Achievements, and Shortcomings. *Poetics*, 34(4-5), 221-235. https://pdf.sciencedirectassets.com/271764/1

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Transparent, Explainable, and Accountable AI for Robotics. *Science Robotics*, 2(6), eaan6080. https://discovery.ucl.ac.uk

Research Article

A Review of Cybersecurity Awareness Focusing on Software and Email Security

Nur Zubaidah Izzati Abdullah[1, *], Nur Azrin Asyiqin Mohd Sedi[2], Nurul Muniroh Muhamad[3], and Noor Rahmawati Alias[4]

[1] Universiti Teknologi MARA, Kelantan Branch, Malaysia ; 2020477194@student.uitm.edu.my; 0009-0004-6808-050X

[2] Universiti Teknologi MARA, Kelantan Branch, Malaysia ; 2020846668@student.uitm.edu.my; 0009-0006-1069-1513

[3] Universiti Teknologi MARA, Kelantan Branch, Malaysia ; 2020627458@student.uitm.edu.my; 0009-0000-8331-5451

[4] Universiti Teknologi MARA, Kelantan Branch, Malaysia ; rahmawati@uitm.edu.my; 0000-0001-5788-4343

[*] Correspondence: 2020477194@student.uitm.edu.my; 0187642676.

Abstract: *This paper describes the literature related to cybersecurity awareness with specific reference to software security and email security in general. The aim of the paper is to collect information from previous research on cybersecurity awareness with special reference to software security and email security in general. The authors applied the method of non-systematic review of articles from few online databases in order to collect information related to the topics mentioned above. Through a non-systematic literature review on cybersecurity awareness that focuses on software and email security, this is considered as an attempt to educate everyone about the need for cybersecurity awareness. Cybersecurity awareness is necessary for people, businesses, and organisations to securely navigate the digital domain. Cybersecurity and software security work mutually beneficial when it comes to protecting computer systems and data from harmful actions. Email security is a vital component of cybersecurity since email is still one of the most commonly used communication methods for both individuals and businesses. It was found from the literature review that the cybersecurity awareness either regarding email security or software security is very important for the organisations and individuals, so that they will take all kinds of precautions and measures to remain secured and protected from the cyber threats.*

Keywords: cybersecurity; software security; email security; cybersecurity awareness.

DOI: 10.5281/zenodo.8180686

1. INTRODUCTION

The Internet is a global network of computers that allows individuals to connect and exchange information in real time. There is a lot of material available on the internet in almost every field. Direct engagement, business transactions, and leisure activities such as internet surfing, advertising campaigns, financial transactions, and Internet shopping are examples of Internet applications. With all of the advantages that the Internet provides, it is also responsible for security and privacy issues. The internet is the source of all publicly available information that is exploited, such as through visiting new websites, engaging in Internet fraud, and unwittingly providing information to third parties. The validity of the path by which the information is conveyed is under doubt.

Spamming and phishing are serious network security issues because they attempt to steal money and personal information. Everyone with an Internet connection has a significant impact on a company's cyber security. An institution's Internet security is the sum of all vulnerable security breaches caused by personnel habits and vulnerabilities. A corporation's human attack surface comprises negligence, mistakes, disease, mortality, insider threats, and media manipulation risks. Spyware is a popular and successful social manipulation technique that takes advantage of the human attack surface.

Therefore, cybersecurity awareness, or information security awareness, has become an important issue today. Cybercriminals continuously develop new strategies to exploit weaknesses and obtain unauthorised access to sensitive information, making cybersecurity knowledge critical in protecting against cyber threats. Individuals and organisations may better recognise and respond to possible threats by increasing cybersecurity knowledge, lowering the probability of being a victim of a cyberattack.

The remainder of the paper is structured as follows: Section 2 provides the literature review on cybersecurity awareness, software security and email security; Section 4 discussion; and Section 5 is the conclusion section and references.

2. Literature Review

2.1 Cybersecurity Awareness

Cybersecurity is defined as the component of information security that focuses primarily on preserving the confidentiality, integrity, and availability (CIA) of digital information assets against dangers that may develop as a result of such assets being compromised via (using) the internet (Von Solms, B.,2018). It was also said that the term "cybersecurity" has a broad definition (ISO, 2018) and cyber security may help with risk management and prevent cyber attacks and data breaches. Security assaults, which come in two varieties (active and passive attacks), and security objectives are among the features of security that are defined by the security architecture (Stallings, 2006). The definition of cybersecurity according to ITU-T (2008) is "the collection of things, consisting of security concepts, policies, tools, guidelines, security safeguards, actions, risk management methods, training, technologies, assurance and best practises, which can be applied to protect users' assets as well as the organisation and cyber environment".

In academic writing, the phrase "cybersecurity awareness" is referred to as "information security" (Vazquez, 2019). A successful programme would be created and effective tactics would be chosen for the intended audience with the help of an overview of users' present level of awareness and perceptions. In addition to offering training programmes for users or employees, cybersecurity awareness raises users' or workers' knowledge of cybersecurity in an organisation and teaches them how to recognise threats to or assaults from it (Nachin et al., 2019; NIST, 2011). Hwang et al.(2021) described information security awareness as a phenomenon that tries to assist users in noticing the security vulnerabilities or problems that may develop and responding in an appropriate way. Naturally, it also seeks to keep the security phenomena on the internet at the forefront of the user's thoughts. Hwang's remarks were echoed by Khan et al.(2015) who defined information security awareness as people having knowledge about security and acting within the scope of recognised regulations.

Typically, security awareness is evaluated in the first phases of software development. A reference model of awareness-related needs is thought to determine the functional scale of security awareness programmes, according to a number of studies. These programmes generally work to increase users' knowledge of the most common cyberthreats, the laws and policies of their nation and institution, and the procedures that must be adhered to in order to secure their digital assets (Hansche, 2001; Maqousi et al., 2014; Sabillon et al., 2019). The frequency and severity of cyberattacks have increased due to the lack of internet information about cybercrime and the high degree of concern. During the pandemic, a number of cyberattacks were recorded against healthcare providers, government agencies, support platforms, efforts to advertise COVID-19 remedies fraudulently, and more (Lallie et al., 2020; Pranggono and Arabo, 2021).

In cybersecurity awareness, a number of variables are present, including human factors. Age, gender, education, university credentials, and IT experience are some of these determinants (Bordonaba-Juste et al., 2020; Jeong et al., 2019; Li et al., 2020). According to Daengsi (et al., 2021) simulations of security risk scenarios, cybersecurity drills, and awareness training should all be included in a strategy. A plan should be employed as a component of the organization's cybersecurity awareness programme in order to increase employee cybersecurity awareness. Such a tailored programme might be used as a tool to inform, teach, and raise awareness among staff members or users in each organisation on how to defend themselves and their companies against cyberattacks.

As the Internet has expanded, individuals' lives are becoming more affected by cyberthreats (such as the disclosure of personal information). According to Yeom (et al., 2020) most security systems are weak because users do not understand how to use the technology, which leads to frequent information leaks by insiders. According to Tom Olzak (2006) a security awareness programme that focuses on the realisation aspect and active participation of the people involved in the software development and usage process for maintenance on three fronts confidentiality, integrity, and secure availability of the information with the aim of creating a fully aware workforce.

According to Mohammed A. Alqahtani (2022), all actions carried out online facilitate many activities, but adversely, they open themselves to cyberattacks that might reveal user data and information to unauthorised parties. With the help of cyber security awareness, users may be taught about the dangers that lie online, how to avoid them, and what to do in the case of a security crisis. Additionally, it fosters in them a proactive feeling of obligation to protect the privacy of others. For it to be most useful and successful, users' awareness of cyber security must be a widespread endeavour. John Steven, Ken van Wyk (2006) proposed that the development team, security team, and operational team should be trained in order to raise awareness among them. Programmes for cybersecurity education and awareness may contribute to national security and should be well-organized to provide individuals a foundational understanding of the subject (Al-Janabi, S.; Al-Shourbaji ; 2016).

2.2 Software Security

Saikath Bhattacharya, Munindar P. Singh, and Laurie Williams (2021) claim that software security is a major issue since software flaws might result in cyber-attacks, breach user privacy, or result in financial loss. The President's executive order on criteria to assess software security was motivated by recent supply chain breaches, including the Solar Winds cyber-attack. Businesses must evaluate the security of their products before releasing them in order to reduce cyber-attacks. Based on operational performance indicators, software businesses track software test data and determine the programme's readiness for release. Software releases, however, depend on a variety of factors, including software providers, stakeholders, and client business requirements.An early or late release might have a detrimental impact on the product's performance overall, return on investment, consumer happiness, and manufacturing costs. By extrapolating the decrease in vulnerabilities during testing, software security growth charts the growth in software security. Software security preparedness determines the ideal release window by taking security growth into account. Companies frequently use specialised software security testing tools and dedicate extra testing time to analyse software security, delaying the delivery of software as a result. It might be difficult for management, software testers, and developers to provide a secure software release on schedule.

According to Mcafee (2017) on a computer or mobile device, software or applications must be updated. Software updates are essential because they typically contain crucial security fixes. Skipping software updates puts you at danger of identity theft, financial loss, and other problems since it gives hackers access to your personal information. Software upgrades may provide new or better capabilities, as well as increased compatibility with other hardware or software, in addition to security patches.)They can also increase the stability of your programme by deleting outdated features.

The amount of services offered on the Internet is growing, argues Atsuo Hazeyama and Hiroto Shimizu (2012). The proliferation of mobile terminals or data electronics in the near future will ensure the continuation of this trend. Computer security is becoming more crucial along with this development. In recent years, as more and more services have been implemented using software and as software complexity has increased, it has become clear how important software security technologies are in addition to network security technologies like encryption or access control. Software security is concerned with security across the whole software development process, which means it goes beyond merely integrating network security technologies into software systems to include a variety of security-related tasks. According to Mano Paul, the right technology should be chosen, the process should be hack-resistant, and the people should be made aware, educated, and informed appropriately in order to create safe software.

Malicious software programmes called internet threats are intended to target consumers when they use the internet and Internet browsers account for 61% of the vulnerabilities utilised in cybercrime assaults against home users, according to the kind of attacking application software (Kaspersky Lab, 2015a).

According to Benbasat and Moore (1991) because the internet may be a dangerous and unsettling environment, cautious security software selection is crucial for online protection. This calls for research into how factors including relative advantage, compatibility, usability, visibility, voluntariness, image, probability of results, and testability affect the likelihood that people would use internet security software.

2.3 Email Security

According to Mcafee (2017) email may be used to communicate with people, obtain information, and submit applications for employment, internships, and scholarships, among other things. Depending on the user's objectives, the formality, target audience, and intended effect of the message the user delivers will vary. Email is typically used to convey spam, malware, and phishing assaults from unidentified senders. Therefore that data and information may be safeguarded, it is crucial to understand email security.

Email security is the process of defending against email risks in order to ensure the availability, integrity, and authenticity of email communications. Email allows billions of people and organisations to send messages to one another. Email is central to how people use the internet, and it has long been a target for hackers (Kerner, S. M. 2022). Online identity theft has a kind known as phishing. To (thousands of) potential victims, it is typically carried out by sending emails (Ayodele et al., 2012, p. 208). Phishing is one type of dangerous cyber-attack in this day and age. In these attacks, phishers typically employ phoney email accounts and/or phoney websites to attempt to obtain users' login information (Chaudhry et al., 2016).

Phishing attacks are defined as criminal actions utilising both technological and social engineering approaches (Aleroud & Zhou, 2017; Bahnsen et al., 2017; Peng et al., 2018). Phishing may be simple to avoid, but developments in the phishing community are making phishing schemes harder for victims to spot (Vayansky & Kumar, 2018).

Phishing is a sort of social engineering in which attackers try to fraudulently get sensitive information from the victim by posing as a reliable third party, according to the study on "Social Phishing" (Jagatic et al., 2005). Phishing assaults are unquestionably a common tactic used by online fraudsters. It is argued that part of the blame for why phishing attacks are so successful could be shifted towards email clients. Therefore, email clients should use a reliable and secure protection method to safeguard email users in this way (Mohammed A. Alqahtani, 2022).

Anyone with an email address might be the victim of phishing. Due to the wide distribution of phishing emails, it can be inferred that the majority of email users may become a target of such attacks. However, in order to effectively prevent phishing attempts, users must also be aware of these assaults, and the onus of spotting them should not just fall on the software side. The email client software should thus be built and developed in such a way that it "educates" the users. Furnell (2005, p. 276) asserts that the programme should always "provide a visible indication of the security status" because this is one of the main reasons why users are uneasy about the security of their software.

According to Luga (et al., 2016) phishing is a technique used by attackers to trick users into divulging sensitive information. This type of cyber-attack or threat aims to trick victims into disclosing sensitive information in order to steal money from them or install malware on their devices, such as usernames, passwords, and financial information (Bahnsen et al., 2017; Chaudhry et al., 2016; Peng et al., 2018).

According to Jagatic (et al., 2005) The closing inquiry, "Do you know the sender of the email?" can be called into question to some extent because phishing emails rarely impersonate a person. Remember that phishing is a type of social engineering in which an attacker tries to obtain sensitive information from a victim fraudulently by pretending to be a reliable third party.

According to Furnell (2005, pp. 274-279) titled "Why consumers should not use security," said "some obvious awareness issues remain to be overcome, and unfortunately there is sufficient evidence to show that consumers do not actually understand security well in the first place." With that, in order for their phishing attacks to be successful, phishers use vulnerabilities in email clients. To reduce phishing attacks, these vulnerabilities must be addressed. The failure of the software (email client) to identify the email as a phishing attack and the user's belief in the email being authentic is what leads to the success of the phishing attack.

3. DISCUSSION

The study's findings indicate that there is a lot of information available on security awareness, including information about software security and email security, which really present a lot of potential for crime if users do not pay attention to it. In today's digital world, cybersecurity knowledge is fundamental. Individuals, businesses, and organisations must be aware of the possible dangers and hazards that exist online as their reliance on technology and the internet grows. Education is a critical component in increasing cybersecurity awareness. Cyber dangers such as phishing, malware, ransomware, and social engineering must be educated on. They should be informed of how these threats may affect them and the consequences of succumbing to them.

Individuals who are aware of these risks can take the necessary precautions to safeguard their personal information and digital assets. Adopting claimed safe browsing practices is another critical component of cybersecurity knowledge. Security precautions include using strong and unique passwords for different accounts, enabling two-factor authentication, keeping software and operating systems up to date, and exercising care when clicking on links or downloading files from unfamiliar sources. Backing up data on a regular basis is also essential since it may help reduce the damage of a prospective cyberattack.

Organisations also play an important role in raising cybersecurity awareness. They should provide extensive staff training programmes to ensure that everyone understands the importance of cybersecurity and how to recognise and respond to possible attacks. Establishing clear policies and practices for managing sensitive information, as well as performing regular security audits, may also help foster a cybersecurity culture inside an organisation. Government and regulatory entities are also responsible for raising cybersecurity awareness. To safeguard individuals and organisations from cyber risks, they might organise public campaigns, develop cybersecurity rules and standards, and enforce legislation. Governments may cooperate to create a safer digital environment for everyone by encouraging collaboration between the public and commercial sectors.

Cybersecurity awareness is also vital for individuals, businesses, and organizations to traverse the digital realm safely. By educating ourselves, adopting best practices, and being attentive, we can limit the dangers of cyberattacks and secure our digital life. It is a continuing activity that demands continuous learning and adaptation to keep one step ahead of the ever-evolving cyber Hence, cybersecurity and software security work mutually beneficial when it comes to protecting computer systems and data from harmful actions.

Software security refers to the procedures used during the software development process to guarantee that software programmes are resistant to assaults and vulnerabilities. There is relevance of software security in the field of cybersecurity. Software security has become essential because many cyberattacks target flaws in software programmes. These vulnerabilities might be unintended code mistakes, design faults, or poor security measures. Attackers routinely hunt for these flaws to obtain illegal access, steal sensitive information, or disrupt the functioning of software systems. There are certain crucial factors to consider while discussing software security, such as secure development practices. Adopting safe coding methods is vital to limiting vulnerabilities in software systems. Developers should follow secure coding rules and frameworks, undertake thorough testing, and conduct code reviews to discover and address any security problems before delivering the product. Then, regular updates and patching: Software manufacturers should routinely deliver updates and fixes to address reported vulnerabilities. It is vital for consumers to keep their software apps UpToDate to guarantee they have the latest security updates. Validating and sanitising user input is critical for preventing attacks such as SQL injection, cross-site scripting (XSS), and command injection.

Software developers can reduce the danger of these sorts of attacks by ensuring that user input is properly handled and sanitised. Authentication and authorization, proper authentication and authorization procedures must be implemented to prevent unauthorized access to software systems. Effective security methods include strong password restrictions, multi-factor authentication, and role-based access controls. Thereafter, security awareness and training. Promoting security awareness among software developers and users is vital. Training programmes may educate employees on common security risks, recommended practices, and the need to maintain software security throughout the development and deployment lifecycle. By emphasising software security, firms may drastically lower the risk of cyberattacks and data breaches. It's crucial to include security measures in the software development process from the very beginning and regularly monitor and upgrade software programmes to keep ahead of emerging risks.

Apart from that, email security is an important area of cybersecurity because email is still one of the most regularly utilised communication channels for both individuals and enterprises. It is critical to protect email accounts and the information contained inside them to avoid unauthorized access, data breaches, phishing attempts, and other email-related dangers. Let us go through some crucial concerns for email security. Firstly, strong passwords. Using secure, unique passwords for email accounts is vital. Passwords should be complicated, having a combination of uppercase and lowercase letters, numbers, and special characters. It's vital to avoid using easily guessable information such as birthdays or frequent phrases. Additionally, activating two-factor authentication (2FA) adds an extra layer of protection by requiring a second form of verification, such as a code texted to a mobile device. Secondly, encryption: encrypting email exchanges guarantees that the content of emails stays private and safe. Secure methods such as Transport Layer Security (TLS) encrypt the connection between mail servers, whereas end-to-end encryption encrypts the email message itself. End-to-end encryption ensures that only the intended receiver can decrypt and read the communication, offering a higher level of security.

Phishing assaults are a frequent approach used by attackers to deceive users into providing sensitive information. It is crucial to be cautious when clicking on links or opening attachments in emails, especially from unfamiliar or dubious sources. Verify the validity of the email and sender before submitting any sensitive information or interacting with the material. Keep in mind that email security is a joint responsibility of service providers, people, and businesses. By putting these precautions in place and remaining watchful, you can greatly improve the security of your email conversations and keep critical information from getting into the wrong hands.

4. CONCLUSION

This review describes the literature related to cybersecurity awareness with specific reference to software security and email security in general. Cyber awareness based on both software and email security is vital in today's digital world. As for software security, regular updates, safe coding techniques, and vulnerability assessments are crucial to defending against potential attacks and fixing flaws. Secure deployment, setup, and integration of security into the software development lifecycle (SDLC) further increases software security. Moreover, for email security, the knowledge of users plays a significant role in combating email-based attacks such as phishing. Educating consumers about spotting malicious emails, avoiding clicking unfamiliar links or downloading attachments, and using email filtering and encryption technologies are crucial to lowering risk. Thus, by emphasising cyber awareness in both software and email security, firms may strengthen their cybersecurity posture, lower the risk of cyber attacks, and secure critical information. Ongoing training, user education, and coordination between IT professionals and end users are vital to establishing a successful cyber protection plan.

Acknowledgments: We would like to express our appreciation to Madam Salliza Md Radzi, our course instructor for her continuous guidance and support. Special gratitude to Universiti Teknologi MARA Kelantan Branch for the opportunity and support given for our team to enable completion of this paper.

References

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review*, *5*(1).

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, 160–196. https://doi.org/10.1016/j.cose.2017.04.006

Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information & Knowledge Management*, *15*(01), 1650007. https://doi.org/10.1142/s0219649216500076

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2), 23.

Alsmadi, D., Maqousi, A., & Abuhussein, T. (2022). Engaging in cybersecurity proactive behavior: awareness in COVID-19 age. *Kybernetes*, (ahead-of-print). https://doi-org.ezaccess.library.uitm.edu.my/10.1108/K-08-2022-1104

Alqahtani, M. A. (2022). Cybersecurity awareness based on software and e-mail security with statistical analysis. *Computational Intelligence and Neuroscience*, *2022*.

Ansari, M. F., Sharma, P. K., & Dash, B. (2022). Prevention of phishing attacks using AI-based Cybersecurity Awareness Training. *Prevention*.

Ayodele, T., Shoniregun, C. A., & Akmayeva, G. (2012, June 1). *Anti-phishing prevention measure for email systems*. IEEE Xplore. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6280179&isnumber=6279697

Banerjee, C., & Pandey, S. K. (2010). Research on software security awareness: problems and prospects. *ACM SIGSOFT Software Engineering Notes*, *35*(5), 1-5.

Bahnsen, A. C., Bohorquez, E. C., Villegas, S., Vargas, J., & González, F. A. (2017, April 1). *Classifying phishing URLs using recurrent neural networks*. IEEE Xplore. https://doi.org/10.1109/ECRIME.2017.7945048

Bhattacharya, S., Singh, M. P., & Williams, L. (2021, October). Software Security Readiness and Deployment. In *2021 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)* (pp. 298-299). IEEE.

Chawathe, S. (2018, August). Improving email security with fuzzy rules. In *2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)* (pp. 1864-1869). IEEE.

Cram, W. A., & Mouajou-Kenfack, R. (2022). Show-and-tell or hide-and-seek? Examining organizational cybersecurity incident notifications. Organizational Cybersecurity Journal: Practice, Process and People, (ahead-of-print).

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2021). Cybersecurity awareness enhancement: a study of the effects of age and gender of Thai employees associated with phishing attacks. *Education and Information Technologies*, 1-24.

Daengsi, T., Wuttidittachotti, P., Pornpongtechavanich, P., & Utakrit, N. (2021). A Comparative Study of Cybersecurity Awareness on Phishing Among Employees from Different Departments in an Organization. *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*. https://doi.org/10.1109/icscee50312.2021.9498208

Douha, N. G. Y. R., Renaud, K., Taenaka, Y., & Kadobayashi, Y. (2023). Smart home cybersecurity awareness and behavioral incentives. *Information & Computer Security*.

Erendor, M. E., & Yildirim, M. (2022). Cybersecurity awareness in online education: A case study analysis. *IEEE Access*, *10*, 52319-52335.

Furnell, S. (2005). Why users cannot use security. *Computers & Security*, *24*(4), 274–279. https://doi.org/10.1016/j.cose.2005.04.003

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2021). Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems*, *61*(4), 345-356.

Hazeyama, A., & Shimizu, H. (2012, August). Development of a software security learning environment. In *2012 13th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing* (pp. 518-523). IEEE.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94–100. https://doi.org/10.1145/1290958.1290968

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an Improved Understanding of Human Factors in Cybersecurity. *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*. https://doi.org/10.1109/cic48465.2019.00047

Jian, N. J., & Kamsin, I. F. B. (2021, September). Cybersecurity Awareness Among the Youngs in Malaysia by Gamification. In *3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)* (pp. 487-494). Atlantis Press.

Kaspersky Security Bulletin 2015. Overall statistics for 2015. (n.d.). Securelist.com. https://securelist.com/kaspersky-security-bulletin-2015-overall-statistics-for-2015/73038/

Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 5766-5781.

Kerner, S. M. (2022, January). What is Email Security? – Definition from SearchSecurity.com. SearchSecurity. https://www.techtarget.com/searchsecurity/definition/email-security

Lötter, A., & Futcher, L. (2015). A framework to assist email users in the identification of phishing attacks. *Information & Computer Security*, *23*(4), 370-381.

Mcafee, "Why software updates are so important," 2017, https://www.mcafee.com/blogs/internet-security/software-updates-important/

Miranda, M. J. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review*, *14*(2), 5-10.

Nachin, N., Tangmanee, C., & Piromsopa, K. (2019). How to increase cybersecurity awareness. *ISACA Journal, 2*, 45–50.

NIST. (2011). *Information Technology Security Training Requirements*. *Special Publication (SP) 800–16*, USA, from http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137- Final.pdf

Okokpujie, K., Kennedy, C. G., Nnodu, K., & Noma-Osaghae, E. (2023). Cybersecurity Awareness: Investigating Students' Susceptibility to Phishing Attacks for Sustainable Safe Email Usage in Academic Environment (A Case Study of a Nigerian Leading University). *Planning*, *18*(1), 255-263.

Olzak, T. (2006). *Strengthen Security with an Effective Security Awareness Program*. https://www.adventuresinsecurity.com/Papers/Build_a_Security_Awareness_Program.pdf

Pawlicka, A., Pawlicki, M., Kozik, R., & Choraś, M. (2022). Human-driven and human-centred cybersecurity: policy-making implications. *Transforming Government: People, Process and Policy*, (ahead-of-print).

Shaheen, K., & Zolait, A. H. (2023). The impacts of the cyber-trust program on the cybersecurity maturity of government entities in the Kingdom of Bahrain. *Information & Computer Security*. https://doi-org.ezaccess.library.uitm.edu.my/10.1108/ICS-06-2022-0108.

Sharma, K., Zhan, X., Nah, F. F. H., Siau, K., & Cheng, M. X. (2021). Impact of digital nudging on information security behavior: an experimental study on framing and priming in cybersecurity. *Organizational Cybersecurity Journal: Practice, Process and People*, *1*(1), 69-91.

Vafaei-Zadeh, A., Ramayah, T., Wong, W. P., & Md Hanifah, H. (2018). Modelling internet security software usage among undergraduate students: A necessity in an increasingly networked world. *VINE Journal of Information and Knowledge Management Systems*, *48*(1), 2-20.

Van Wyk, K. R., & Steven, J. (2006). Essential Factors for Successful Software Security Awareness Training. *IEEE Security & Privacy Magazine*, *4*(5), 80–83. https://doi.org/10.1109/msp.2006.119

Vayansky, I., & Kumar, S. (2018). Phishing – challenges and solutions. *Computer Fraud & Security*, *2018*(1), 15–20. https://doi.org/10.1016/s1361-3723(18)30007-1

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security–what goes where?. *Information & Computer Security*, *26*(1), 2-9.

Yeom, S., Shin, D., & Shin, D. (2020). Scenario-based cyber attack·defense education system on virtual machines integrated by web technologies for protection of multimedia contents in a network. *Multimedia Tools and Applications*, *80*(26-27), 34085–34101. https://doi.org/10.1007/s11042-019-08583-0

Research Article

Information Systems Security Issues and Preventive Measures

Maizatul Aqilah Zakariah[1], Muhammad Nor Nabihan Norzeri[2], and Nurhidayah Muhammad Nadzri[3, *]

[1] Universiti Teknologi MARA; Maizatul Aqilah; 2020496272@student.uitm.edu.my; 0009-0000-1436-5201

[2] Universiti Teknologi MARA; Muhammad Nor Nabihan; 2020853126@student.uitm.edu.my; 0009-0000-9663-2341

[3] Universiti Teknologi MARA; Nurhidayah ; 2020859204@student.uitm.edu.my; 0009-0005-6577-2284

[*] Correspondence: 2020859204@student.uitm.edu.my; +60105340574.

Abstract: *Information security, sometimes abbreviated as InfoSec, is the practice of protecting information by mitigating information risk. Typically, it involves preventing or reducing the likelihood of unauthorized or inappropriate access to data or unlawful use, disclosure, disruption, deletion, corruption, modification, verification, recording, or invalidation of information. This includes measures designed to reduce the adverse effects of such incidents. The primary focus of information security is the balanced protection of the confidentiality, integrity, and availability of data, also known as CIA, with an emphasis on efficient policy implementation without compromising business productivity. Based on our research, Information security may be divided into three major categories network security, physical security and personnel security and there some issues will involve users are worldwide and can be used without limits.*

Keywords: Security, Network, Malware, Threats, Vulnerabilities.

DOI: 10.5281/zenodo.8180713

1. INTRODUCTION

The primary reason for 30 years of failure in the Information System Security industry stems from a failure to recognise one of the most fundamental security principles: no security solution is ultimately stronger than its weakest link. This notion, when combined with human nature and the inherent dynamics of the marketplace, has resulted in many of us in the business being forced to promote "fake cures" rather than actual answers.

Information security may be divided into three major categories: network security, physical security and personnel security. First, network security relates to the protection of the infrastructure utilized for data storage and transmission. This is generally accomplished through the use of technology and hardware such as intrusion detection systems (IDS), firewalls, routers, and so on. Antivirus software and rules for access control and authentication are examples of software.

Second, physical security relates to the protection of the building, work locations, gadgets, and data stored in the form of papers. This is accomplished mostly by access control devices such as security guards, ID cards and swipe cards, limited movement of media such as CDs, floppies, and documents, and video monitoring such as fire safety. Physical controls monitor and govern the work environment and computer facilities. Doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, and other devices are used to monitor and regulate access to and from such buildings. ("Information security - Wikipedia") ("Information security - Wikipedia") Physical controls include dividing the network and workplace into functional regions. Separation of tasks is an important physical control that is usually disregarded. It assures that an individual cannot perform a key task by himself. For example, an employee who files a reimbursement request should not be allowed to also authorise payment or print the cheque. An applications programmer should not also be the server or database administrator; these positions and responsibilities must be kept distinct.

Third, personnel security refers to preparations established to combat the possible threat posed by offshore vendor personnel. Background checks, such as reference checks and police checks, non-disclosure and confidentiality agreements, such as internet access policies and mobile computing rules, training and awareness, business continuity and disaster recovery are some of the security methods utilized. Refers to the procedures used to obtain information and deliver ongoing services in the event of an emergency. Data backups at remote sites, risk assessment and restoration methods, fire, link, and power exercises, and alternate site management are some of these practices.

This paper aims to look into the previous studies discussing the information systems security with special focus on the issues related to information systems security and the suggested solutions to cater the threats that often occur. It is organized into four sections; Section 1 is the introduction; Section 2 discusses information systems security issues; Section 3 explains about the information system security threats and preventive measure; Section 4 provides the conclusion of this study.

2. INFORMATION SYSTEMS SECURITY ISSUES

Information system security managers play a very important role in knowing about the assets of their organisations, the vulnerability of their information systems to different threats, and their potential damages. Each threat and vulnerability must be related to one or more of the assets requiring protection. Logical and physical assets can be grouped into five categories:

1. Information- Documented data or intellectual property used to meet the mission of an organization
2. Software- software applications and services that process, store or transmit information
3. Hardware- information technology physical devices considering their replacement costs
4. People- the people in an organization who possess skills, knowledge and experience that are difficult to replace
5. Systems- information systems that process and store information

The various units of value or metrics for the valuation of assets may be in use. The common metric is monetary, which is generally used for data that represents money where the threat is direct financial theft or fraud. Some assets are difficult to measure in absolute terms but can be measured in relative terms. The value of information can be measured as a fraction or percentage of total budgets, assets, or the worth of a business in a relative manner. The impact of information security incidents may well be financial in the form of immediate costs and losses of assets. ("(PDF) INFORMATION

SYSTEMS SECURITY TRENDS & ITS IMPACT - ResearchGate"). There are few issues related to information systems security namely:

2.1 Downtime prevention

The importance of ensuring that digital networks used by companies for their revenue and operations are always available. Downtime refers to periods of time when a system is not operational which can result in financial losses and other negative impacts. To reduce downtime, companies can use several techniques including fault-tolerant computer systems that use hardware or software to detect hardware failures and automatically switch to backup systems. High-availability computing environments use backup servers, distribute processing among multiple servers and have high-capacity storage to recover quickly from a system crash. Recovery-oriented computing involves designing systems to recover quickly and implementing capabilities and tools to help operators pinpoint the sources of faults in multicomponent systems and easily correct their mistakes. ("Chapter 8 - Summary Management Information Systems") Disaster recovery planning and business continuity planning are also important to restore computing and communications services after they have been disrupted by an event such as earthquake, flood or terrorist attack. Business continuity planning focuses on how the company can restore business operations after a disaster strikes. Some companies outsource security functions to managed security service providers (mssps) that monitor network activity and perform vulnerability testing and intrusion detection. ("What are the most important tools and technologies for ... - HKT Consultant")

2.2 Network storage

The security vulnerabilities that arise when sensitive data is stored on remote servers maintained by third-party storage vendors. The cost of storage management is much higher than the initial acquisition costs. Most third-party storage vendors do not provide assurances of data confidentiality and integrity [CNN, 2006]. To protect the data, security systems should offer users assurances of data confidentiality and access pattern privacy. This ensures that the data remains encrypted throughout its lifetime on the server and is only decrypted by the client upon retrieval. (Gartner. ;1999)

2.3 Cell phone issue

The spread and impact of computer viruses and worms on cell phones through email attachments, internet downloads, mms attachments and Bluetooth transfers. The most common type of cell phone infection occurs when a phone downloads an infected file from a pc or the internet. Phone-to-phone viruses are on the rise, particularly those that infect phones running the Symbian operating system. One of the obstacles to mass infection is the large number of proprietary operating systems in the cell phone world. Cell phone virus writers have no windows-level market share to target, so any virus will only affect a small percentage of phones. ("Cell-phone Virus Basics - How Cell-phone Viruses Work - HowStuffWorks") ("Cell-phone Virus Basics - How Cell-phone Viruses Work - HowStuffWorks") Infected files often disguise themselves as applications like games, security patches, add-on functionalities and free stuff. Infected text messages may steal the subject line from a message received from a friend which increases the likelihood of opening it. (Radmilo Racic Et Al. ;2008)

2.4 Other issues

The security risks associated with cloud computing which is a technology that allows users to access and store data and applications over the internet instead of their own computers [Jonathan et.al, 2009]. Cloud computing has many benefits such as cost savings and increased flexibility but it also poses security risks because users do not have control over the hardware and infrastructure that their data is stored on. The only way to mitigate these risks is through contractual agreements with cloud providers. The current services level agreements (slas) and contracts offered by most cloud providers do not provide adequate coverage for the increased risks involved [Rana Gupta, 2008]. This means that companies and organizations need to carefully evaluate the security measures and contractual terms offered by cloud providers before deciding to use their services.

3. INFORMATION SYSTEMS SECURITY THREATS AND PREVENTIVE MEASURES

This section provides brief discussion on the information systems security threats by looking into the computer crimes and the possible preventive measures suggested by few studies. Many materials are talking about hacking of the systems.

A hacker is someone who attempts to obtain unauthorized access to a computer system. Crackers are often hackers with nefarious intentions. Hacker’s spoof or misrepresent themselves by using bogus email accounts or impersonating someone else. Theft of products and services, system damage, and cyber vandalism, such as the purposeful interruption, defacement, or even destruction of a Web site or business information system, are all examples of hacker actions. Spoofing includes things like hiding the hacker's actual identity or email address, or diverting a Web link to a different website that benefits the hacker. Sniffing is an eavesdropping programme that analyses network traffic and can allow hackers to obtain private information transmitted across the network. DoS attacks, such as flooding a network or server with thousands of fake communications in order to crash or impair the network. A distributed denial-of-service (DDoS) assault employs hundreds or even thousands of machines to flood and overload the network from several ports of entry. Hackers can infect the PCs of thousands of unsuspecting users with malicious software, forming a botnet of resources for launching a DDoS attack. A zombie computer, often known as a bot, is a computer that may be used by a hacker to distribute spam or execute Distributed Denial of Service (DDoS) assaults. When a victim executes seemingly harmless code, a link is established between their computer and the hacker's system. The hacker can then use the victim's computer to perpetrate crimes or disseminate spam in stealth. (B.Premkumar. ;2022)

In cyber security, hacking is the use of devices such as computers, smartphones, tablets, and networks to cause harm or corruption to systems, acquire information on users, steal data and documents, or disrupt data-related activity. A hacker is traditionally portrayed as a lone rogue programmer who is extremely competent in coding and changing computer software and hardware systems. However, this limited perspective does not address the underlying technical nature of hacking. Hackers are becoming more sophisticated, employing covert attack tactics meant to go undiscovered by cybersecurity software and IT professionals. They are also competent at developing attack vectors that dupe users into opening infected attachments or URLs and freely disclosing sensitive personal data.

In computer crime, the computer can be either the victim or the perpetrator. DoS assaults, virus introduction, service theft, and computer system interruption are the most economically devastating types of computer crime. Identity theft is another type of digital crime. An imposter collects critical personal information in order to impersonate another individual and gain credit, products, or phony credentials. Phishing is the practice of creating phony websites or sending e-mail messages that look real in order to compel consumers into providing private information. Other phishing strategies include evil twins, which are wireless networks that masquerade as genuine Internet hotspots and are used to steal personal information, and pharming, which involves converting visitors to fake Websites that masquerade as valid Websites. Click fraud happens when a human or computer programme clicks on an internet advertisement without intending to learn more about the advertiser or make a transaction. Click fraud can also be committed using software programmes to click, and bot networks are frequently used for this reason.

3.1 *Information Systems assets and threats*

According to (Icove et al. ;1999) divided information threats into seven categories: software, hardware, data, network, physical, personnel, and administration, which includes security regulations and policies. Threats to IS assets are frequently categorised according to the type of assets involved. (Loch et al ;1992). A four-dimensional IS threat classification system was developed. Sources, perpetrators, intent, and consequences are Loch's four dimensions. The origins of threats to IS assets can come from within or outside the organisation, the attackers can be human or nonhuman, their activities can be unintentional or intentional, and the outcomes can include disclosure, modification, destruction, and denial of service. Posthumus (2004) also identified three primary dangers to company information security: risks from natural disasters, risks from technology, and risks from people. In their analysis of how businesses responded to IS threats, White et al. (1996) made a distinction between internal and external information security activities. On the basis of the NIST SP800-30 security standard, internal functions relate to technical difficulties whereas external functions deal to non-technical aspects, such as management and operation security (NIST, 2002).

All of the works mentioned above divide IS resources and related dangers into two categories: IT-related and non-IT-related. Software, hardware, data, and network threats are classified as IT-related, whereas people, administrative, and physical/environmental facilities hazards are classified as non-IT-related. According to (Icove, 1999) the main personnel challenges are technical training, user education regarding security obligations, and reporting processes for occurrences. The majority of a company's security policies and procedures are decided internally, according to Madnick (1978), in addition to externally sought requirements like privacy laws or governmental restrictions. In several recent research (Birch et al., 1992; Siegel et al., 2002; Gordon et al., 2003), it is recommended that administrative policies include risk transference and insurance.

Both IT- and non-IT-related factors need to be taken into account for information security to be effective (Madnick, 1978; Straub, 1990; lnes, 1994; Kankanhalli et al., 2003; Posthumus, 2004). Instead of being limited to individual products or systems, such security should be evaluated across the entire IT environment (Von Solms, 1996). Clear definitions of administrative regulations are necessary (Madnick, 1978; lnes, 1994; Siegel et al., 2002). Additionally, managers and users must both get training to make clear the rules and penalties for abusing IS (Straub, 1990; Goodhue and Straub, 1991; Thomson and von Solms, 1998).

3.2 *Security countermeasures*

According to Peltier (2001), a security countermeasure is a risk-mitigating measure that identifies, averts, or reduces loss from a particular IS danger or class of threats. According to Straub (1990), Straub and Nance (1990), Forcht (1994), Kankanhalli et al. (2003), it can be either preventive or a deterrent. According to Kankanhalli et al. (2003), advanced security software or controls, such as advanced access control, intrusion detection, firewalls, and surveillance mechanisms, are deployed as preventive measures to safeguard IS assets.

The creation of security policy statements and guidelines, training seasoned auditors to audit IS asset usage, educating users about what constitutes legitimate use of IS assets and the repercussions of illegal use of IS assets are all examples of deterrent measures. Businesses that incorporate preventative security software and deterrent administrative procedures into their security countermeasures dramatically lower levels of computer misuse (Straub 1990).

By putting non-IT countermeasures in place, internal error-related dangers could be significantly reduced. An information security policy offers management guidance and support for information security (BS7799-2, 2002), and it should be distributed to users throughout an organisation in a way that is pertinent to their work, easily available, and comprehensible (Fulford and Doherty, 2003). The IS security policy should also include general guidelines for dividing up security roles and duties inside a company. In addition to the core controls mentioned above, a security measure must stop violations of internal regulations, contractual responsibilities, and criminal and civil laws in order to be compliant with legal requirements. Risk-transferring controls are those that make an effort to transfer the risk to a different organisation, like a security service provider or an insurance.

Job description, resource allocation, and responding to security problems and malfunctions are typical countermeasures related to personnel security (BS7799-2, 2002). To limit human error and make sure users are aware of information security hazards and concerns, appropriate training and education for IS system processes and security courses are required (Straub and Welke, 1998). Additionally, both routine and irregular audits may help to reduce the possibility of facility abuse, fraud, or human theft (Vroom and von Solms, 2004).

4. CONCLUSION

Many of us in the industry are now driven to push "fake cures" rather than real solutions due to this idea, human nature, and the underlying dynamics of the market. Three main categories can be used to categorize information security:. The first aspect of network security is the defense of the equipment used for data transmission and storage. Second, physical security deals with safeguarding the office, work areas, technology, and paper-based data. Most often, security guards, ID cards, swipe cards, the restricted movement of media like CDs, floppies, and documents, and video surveillance for things like fire safety are used as access control technologies. Third, personnel security describes measures put in place to counter the potential threat provided by employees of offshore vendors. Some of the security measures used include background checks, such as reference and police checks, non-disclosure and confidentiality agreements, internet access restrictions, mobile computing rules, training and awareness, business continuity, and disaster recovery. Refers to the processes used to supply continued services and collect information during an emergency.

Worms are autonomous computer programmes that independently replicate themselves across a network without the help of other programmes or data. Many worms make it their mission to detect the presence of debugging tools and modify or stop functioning. Information system security managers must be aware of the resources within their companies, as well as how vulnerable such systems are to various threats and potential harm. It is possible to utilize different measures or units of value for asset valuation. Information security incidents may have a financial impact in the form of out-of-pocket expenses and asset losses.

In conclusion, it is evident that the three categories of IS assets and threats—network, personnel, and regulation/legality—are insufficient as means of protecting businesses across all industries. Additionally, the majority of businesses in poor nations still rely only on technical solutions to tackle IS security-related issues, placing more emphasis on managerial controls than technical ones, which may portend future catastrophes. The findings are consistent with earlier research on small enterprises (Keller et al., 2005; Gupta and Hammond, 2005). A security strategy should be created, and responsibility for it should be assigned, for organisations with lesser information threats, such as conventional manufacturing, distribution, or service companies or enterprises with minimal levels of computerization. Organisations that face significant information risks, on the other hand, should think about risk transference strategies to reduce financial losses and strengthen security related to regulations and the law.

Acknowledgments: We would like to thank Madam Salliza binti Md Radzi, our subject lecturer for IMS657, Legal & Ethical Aspects for Information System for her guidance and encouragement throughout the process of completing this assignment. Students can refer to the notes, as well as the live and recorded lectures, at any time. Furthermore, a clear reference to the ethics of writing assignments (guidelines) was provided.

References

Panel, E. (2023, March 7). 15 Precautions To Take With Online Banking, According To Experts. Forbes. https://www.forbes.com/sites/forbesfinancecouncil/2023/03/07/15-precautions-to-take-with-online-banking-according-to-experts/?sh=786330c727e0

Online Banking Security - Edubirdie. (2023, April 26). Edubirdie. https://edubirdie.com/examples/online-banking-security/

Kumar, P., & Kamalakkannan, P. (2010). Information systems security trends & its impact. National Conference on Role of Information Technology in Management, Chennai, India.. https://www.researchgate.net/publication/302953486_INFORMATION_SYSTEMS_SECURITY_TRENDS_ITS_IMPACT

Kshetri, N. (2015). India's Cybersecurity Landscape: The Roles of the Private Sector and Public-Private Partnership. IEEE Security & Privacy, 13(3), 16–23. https://doi.org/10.1109/msp.2015.61

Welcome to Central Bank of India | Central Bank of India. (n.d.). http://www.centralbankofindia.co.in/

Yin, H., Liang, Z., & Song, D. (2008). HookFinder: Identifying and Understanding Malware Hooking Behaviors. ResearchGate. https://www.researchgate.net/publication/221655500_HookFinder_Identifying_and_Understanding_Malware_Hooking_Behaviors

Patriciu, V., Iustin, P., & Sebastian, N. (2006). Security metrics for enterprise information systems. ResearchGate. https://www.researchgate.net/publication/26452440_SECURITY_METRICS_FOR_ENTERPRISE_INFORMATION_SYSTEMS

What Is Hacking? Types of Hacking & More | Fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-hacking#:~:text=A%20commonly%20used%20hacking%20definition,data%20theft%20by%20cyber%20criminals.

Internet Banking Security to Keep Fraudsters Away. (2023, April 19). www.kaspersky.com. https://www.kaspersky.com/resource-center/preemptive-safety/internet-banking-security-keep-fraudsters-away

CrowdStrike. (2023, April 27). Malware Analysis: Steps & Examples - CrowdStrike. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/

Pollack, K. (2022, November 17). Security impact analysis – What, Why, and How? | CalCom. CalCom. https://www.calcomsoftware.com/security-imapct-analysis/

What is hacking? (n.d.). [Video]. Malwarebytes. https://www.malwarebytes.com/hacker

George, A. (2017). Precautions for Safe Use of Internet Banking: Scale Development and Validation. IIM Kozhikode Society & Management Review. https://doi.org/10.1177/2277975217704049

Peng, Y., Chen, W., Chang, J. M., & Guan, Y. L. (2010). Secure online banking on untrusted computers. https://doi.org/10.1145/1866307.1866409

Jung-Ting Chang, A., & Yeh, Q. (2006). On security preparations against possible is threats across industries. Information Management & Computer Security, 14(4), 343–360. https://doi.org/10.1108/09685220610690817

Mummadi, A., Yadav, B. M. K., Sadhwika, R., & Shitharth, S. (2022). An appraisal of cyber-attacks and countermeasures using machine learning algorithms doi:10.1007/978-3-031-21385-4_3 Retrieved from www.scopus.com

Bekri, W., Layeb, T., Jmal, R., & Fourati, L. C. (2022). Intelligent IoT systems: Security issues, attacks, and countermeasures. Paper presented at the 2022 International Wireless Communications and Mobile Computing, IWCMC 2022, 231-236. doi:10.1109/IWCMC55113.2022.9825120 Retrieved from www.scopus.com

TimesofIndia. (2009). Azad warns against excessive use of cell phones. Accessed from https://indiatimes.com.

Research Article

Cloud Security: The Use and Significance in Information Security Management

Nuur Athirah[1], Nur Arifah Syahadah[2], Nurul Naffisah[3], Nur Shaliza Sapiai[4], and Norhafizan Awang[5,*]

[1] Universiti Teknologi MARA; 2020602604@student.uitm.edu.my; 0009-0000-1244-933X

[2] Universiti Teknologi MARA; 2020470266@student.uitm.edu.my; 0009-0005-6160-1090

[3] Universiti Teknologi MARA; 2020847638@student.uitm.edu.my; 0009-0005-5139-3136

[4] Universiti Teknologi MARA; nurshaliza@uitm.edu.my; 0000-0003-1109-2230

[5] Universiti Teknologi MARA; hafizanawang@uitm.edu.my; 0009-0001-2979-1403

* Correspondence hafizanawang@uitm.edu.my; 019-3860150.

Abstract: *Cloud security is another term for security in cloud computing. It is a set of policies, controls, procedures, and technologies that come together to develop cloud security to secure the infrastructure, data and cloud-based systems. These security procedures are set up for protecting cloud data, assisting regulatory compliance, protecting consumer privacy, and establishing authentication policies for certain users and devices. Computer, IT, and information security are all closely related to cloud security. Each individual and organisation requires IT infrastructure on a regular basis, therefore security is an important aspect in this context. Cloud security is an important key term in the computing field, and it is becoming more common in many organisations and institutions. In this paper the use and significance influence of cloud security has been described. There are explanations on how cloud security works and reasons why cloud security is an important aspect in information security management. This paper is purposely to identify how far this cloud security is influencing information security.*

Keywords: cloud security; information technology (IT); significance

DOI: 10.5281/zenodo.8180732

1. INTRODUCTION

The cloud provides an accessible way for storing and accessing data from anywhere by using an internet connection. Users may easily save their local data on a distant server with a cloud application. The term "cloud computing" also refers to the technology that supports the cloud, which typically consists of some type of virtualized IT infrastructure, such as servers, operating systems, networking, and other infrastructure that has been abstracted using specialised software to enable pooling and dividing across physical hardware boundaries. Virtualization enables cloud providers to maximise the use of their data centre resources. Not surprisingly, many organisations are starting to depend on cloud services. For the data of their users to remain private and secure, cloud providers must abide by security and privacy policies. Cloud security is another term for security in cloud computing. Cloud security is one type of cybersecurity. It is a collection of technology, protocols, and best practises that secure cloud computing environments, applications operating in the cloud, and data kept in the cloud. Cloud security works to offer access control, data governance and compliance, disaster recovery, and storage and network protection against internal and external threats. Securing cloud services starts by understanding exactly what is being protected and the system aspects that must be managed. Cloud security guards against theft, leakage, and deletion of data stored online via cloud computing platforms. Firewalls, penetration testing, obfuscation, tokenization, virtual private networks (VPN), and avoiding public internet connections are some techniques for providing cloud security. Controls and process enhancements for cloud security include those that strengthen the system, alert prospective attackers, and track down problems when they do happen. A business continuity plan and data backup strategy should be considered when thinking about cloud security in the event of a security breach or other emergency. For the hybrid cloud, private cloud, and public cloud, there are several cloud security solutions using a variety of methods. In public cloud settings, the security of hardware and software is the responsibility of the cloud provider, and the user is in charge of protecting their own assets, such as virtual machines, apps, and data.

2. DISCUSSION

2.1 The Use of Cloud Security

Most organisations use cloud security as their security tools for the organisation's data, as cloud security is a set of practices and tools created to handle both internal and external security risks to organisations. Organisations need cloud security to implement their modernization plans and integrate cloud-based tools and services into their infrastructure. So, this shows that cloud security has several uses that make it so important for organisations. There are several reasons why most organisations or companies use cloud security as their security tool.

The first is that organisations use cloud security as their guard for their servers. It is because the ordinary and basic network did not properly provide any type of protection to guarantee the servers' complete security, so the threats have to be avoided by the servers themselves. So, by using cloud security, a bunch of data is sent to the cloud rather than going straight to the servers. Only authorised users are granted access once the cloud analyses the data. The cloud also prevents an unapproved bunch of data from reaching the server. Apart from that, cloud security is also a technological element that prevents threats from happening on the server. The accessibility and exposure of sensitive data can be restricted by clients and providers using the tools and technology of cloud security. To make this happen, encryption is the most suitable technique or method of cloud security to prevent threats from occurring. The client’s data is encrypted to prevent unauthorised parties from decrypting it. It will be impossible to access and useless if the client’s data disappears or is taken.

The second is that organisations use cloud security to manage data and secure encryption. It is because complex algorithms are used in encryption techniques to hide and secure data. These techniques allow the identification of data that is managed via cloud security, which also restricts access from unknown software that may decrypt the encrypted files. Apart from that, the organisation may encrypt its data both at rest and in transit to further protect it while it is stored in the cloud. Without the organisation's confidential decryption key, it is very difficult for anybody to view the data.

The third one is that the organisation uses cloud security to examine and sort data. It is because the applications in conventional systems analyse the data before it gets to the server, plus the applications are expensive and difficult to keep up with. After it enters the application network, it filters the data that arrives. The devices in the organisation occasionally experience overload and may shut down, obstructing both good and bad data and possibly failing to perform as planned. But, by using cloud web security services, a bunch of data is diverted to the security cloud first, where it is screened before being forwarded to the application system. With this, the data in the organisation will be secured, and sort of like cloud security, it will be filtered first to make sure no bad data or information can enter the systems.

The fourth one is that the organisation uses cloud security because it has a private cloud option. The private cloud option means any cloud service created specifically for use by only one organisation. The organisation will not share its cloud computing resources with any other organisation. Private clouds can be tailored to a company's specific business and security requirements. Organisations may now manage compliance-sensitive IT operations without sacrificing the security and performance that used to be only possible with specialised data centres on premises, thanks to increased visibility and control over the infrastructure. In addition, the private cloud option assures security against issues with shared resources.

The last one is that the organisation uses cloud security because it provides legal compliance for organisations. It is because clients and organisations privacy must be protected in order to be in accordance with the law. In order to protect the database's security, cloud-based security has established compliance guidelines that must be properly adhered to. Apart from that, it is also the law and regulations that were set by the government. It is because governments are now aware of how crucial it is to prevent the commercial exploitation of private information. Therefore, organisations must obey the regulations in order to maintain their policies. Plus, laws and regulations require the organisations to uphold strict privacy and client data protection requirements so that the client's data and the organisation's data itself will be protected. In addition, these are some of the uses of cloud security that benefit the users, which are organisations or companies, in order for them to keep their data safe from any harm or threats.

2.2. Key of Cloud Security Use Case

Use cases are a way of locating, outlining, and organising system needs in system evaluation. The use case consists of a number of potential interactions between people and systems in a certain environment that are connected to a specific objective. The procedure generates a document that lists each step a user took to finish a particular task. Cloud security also has its own use cases. Besides, there are also some excellent potentials for cloud security services, which sometimes depend on the distinctive characteristics of the cloud environment itself. There are a few key use cases for cloud security that will be discussed.

The first one is privileged account access. Account management is one of the most important security controls in a cloud environment. It is because accounts must be set up with the "least privileges" necessary for them to carry out their tasks, and their usage must always be watched. Apart from that, for administrator accounts on cloud platforms, this is especially crucial. It would be simple for an intruder to modify firewall configurations or add services where necessary if an account like this were compromised. So, to impose responsibility, general accounts like admin, administrator, or root should not be utilised. It's important to keep an eye on unusual behaviour and compare it to planned adjustments. Plus, any access from places outside of where an organisation anticipates conducting its operations should be noted and looked into. This will give the user a privileged account to access their own account without any problems, such as hackers' problems hacking accounts, and to keep the information private.

The second one is data exfiltration. Data exfiltration is the act of an authorised individual removing information from secured systems where it belongs and either sharing it with uninvited people or transferring it to unsecure systems. The majority of the time, a cloud environment has a wealth of useful data for an intruder. So, organisations move systems into the cloud due to the importance of the data as well as the requirement for highly accessible and available platforms. This will prevent data exfiltration from happening as the organisation moves important and useful data to the cloud security system. Although there may not be much data in the cloud environment itself, the technology may be used to smuggle local data out of the on-premises network, perhaps getting around firewall restrictions and traffic alarms. Any suspicious data leaving the cloud systems that may be huge in bulk, apply a questionable network port, or include certain strings or headers needs to be at least monitored and additionally prevented depending on the confidence of the detections. In addition, organisations must incorporate security knowledge and best practices into their culture in order to lower the likelihood of data exfiltration. Every contact with computer networks, devices, applications, data, and other users must be continually risk-evaluated.

The third one is a man-in-the-cloud attack. It is a hacker who has the ability to access users' entire drives, including all of the papers stored there, and steal data. So, this use case focuses on an authentication token that can be found on a computer or mobile device. A local application can apply this token to use automated user authentication on cloud platforms. By replacing that token with a different one, a hacker hopes to divert the user and their data to their own cloud account. The outcome can be a direct synchronisation of the victim's data with the hacker's system. This behaviour might be found and often stopped by keeping track of connections to unfamiliar cloud instances through endpoint monitoring, network SSL decryption, or a Cloud Access Security Broker (CASB).

The last one is threat intelligence analysis. Threat intelligence data offers insight on attacker origins, compromise indications, and behavioural trends connected to assaults against various types of cloud services, as well as usage patterns for cloud accounts. Learning machine engines in the cloud may be used to collect and evaluate threat intelligence inputs on a large scale. Additionally, data for probability or prediction models can be handled. This cloud security use case could be an ideal addition to a cloud security system given the rise in cloud assaults, including account hijacking attempts. Microsoft's Advanced Threat Analytics is one example of threat intelligence analysis software.

2.3 The Significance of Cloud Computing

The main significance of cloud computing is the strategic development of services. Strategic development, in its simplest terms, refers to how the organisation generates revenue from current core plans and core resources by optimising or reimagining how the service or product is offered. Cloud services make it possible to access the most recent software without the need for extra installation resources, giving traders a strategic edge. The rapid installation of the latest software enables businesses to increase their computer capacity while avoiding large capital investments and expensive programming expenses. Next, the second significance of working with cloud computing is its excellent service controllability. According to the cloud service level agreement (SLA), cloud service solutions include services such as security, problem-solving, management of the infrastructure, and maintenance. These services may be designed to meet specific business requirements that can eliminate the need for businesses to purchase expensive servers and allow companies to manage their own information technology (IT) systems.

Next, cloud-based computing is chosen due to its low cost. Cloud computing is less expensive than physical infrastructure. It may replace hardware like hard drives, network switches, servers, and generators with just one system that is simple to analyse and manage. With all this, it makes cloud services more cost-effective in the long term. Furthermore, cloud computing has a tiering or tiered system, which means that there is less overhead and organisations simply pay for the capabilities and space they demand.

One of the most significant advantages of cloud computing is collaboration. The cloud service is widely used because of its electronic data interchange. Data interchange using cloud-based computing requires less time than physical services, and it allows several people to update and execute the exact same file at the same time. Many cloud services also have social capabilities that enable teams to interact, share, and use data in the cloud more efficiently. Following that, cloud computing is significant due to its unpredictability in batch processing. Continuous development and growth involve the management of massive volumes of data by an organisation. Cloud services allow for the quick batch processing of massive amounts of data without the need for human interaction, which boosts the quality of the data and business productivity.

Another significance of using cloud computing is the simplicity with which it may be implemented. Businesses may simply move to and adapt to the use of cloud services. This kind of action allows businesses to keep their applications without the need for extra technological capabilities, making the shift to the cloud faster and easier. Additionally, cloud computing eliminates the need for hardware. Servers, physically or electronically, need the acquisition and upkeep of expensive hardware and software. However, cloud computing, on the other hand, requires no hardware and eliminates the requirement for data in physical storage. Companies may thus develop a cloud system that matches their demands and simply extend it if necessary.

Cloud-based computing is also quite accessible. Organisational downtime can result in financial losses, company disruption, loss of revenue, and negative reputational consequences. As a result, it matters a lot for businesses to have minimal or no downtime. Because of its decentralised operations, the cloud service enables outstanding usability for organisations, which is one of its most significant advantages. Ultimately, cloud computing gives employees security of employment. Reliability is essential for the smooth functioning of companies of all sizes. The cloud service prevents security breaches, outages, and disruptions. The service also maintains, updates, and upgrades these services on a regular basis. Furthermore, the cloud successfully manages failure scenarios and guarantees that recovery operations are automated.

3. CONCLUSION

Cloud computing security is a new technology development that has the potential to have a great influence on information security management. It has many uses and has a significant influence on its users. To ensure the security of the assets hosted in the cloud, select the finest cloud security service. Cloud security is the precaution taken to safeguard digital assets and data kept online via cloud services. Additionally, it is obvious that cloud security is ideal for information security management given its widespread use and significant influence.

Acknowledgments: We would like to express our sincere gratitude to all the individuals that have contributed to this paper, without their support and guidance it would not have been possible. We would like to thank our lecturers, Madam Salliza Md Radzi, Madam Nur Shaliza Sapiai and Madam Norhafizan Awang for their invaluable guidance and support throughout the completion of this paper. Their expertise and insights were instrumental in shaping the direction and focus of our research. We are also grateful to the Faculty of Information Management at Universiti Teknologi Mara for providing us with the resources and support we needed to complete this paper.

References

Brush, K. (2022, November 28). *What is a use case?*. Software Quality. https://www.techtarget.com/searchsoftwarequality/definition/use-case

Cloud (2022). What is Cloud Computing & Why is it Important? |. [online] Accenture.com. Available at: https://www.accenture.com/ro-en/cloud/insights/cloud-computing-index.

Cloud Mask Team. (n.d.). *Man-in-the-cloud (MITC) attacks; risk and solution*. Cloudmask. https://www.cloudmask.com/blog/man-in-the-cloud-mitc-attacks-risk-and-solution#:~:text=Dubbed%20%22man%2Din%2Dthe,and%20all%20the%20documents%20inside.

Cloud security: Definition, how cloud computing works, and safety. (2017, February 6). Investopedia. https://www.investopedia.com/terms/c/cloud-security.asp

Google. (n.d.). *Preventing data exfiltration - documentation - google cloud*. Google. https://cloud.google.com/docs/security/data-loss-prevention/preventing-data-exfiltration#:~:text=In%20this%20document%2C%20data%20exfiltration,system%20administrators%2C%20and%20trusted%20users.

Habib Gill, S., Abdur Razzaq, M., Ahmad, M., M. Almansour, F., Ul Haq, I., Jhanjhi, N., Zaib Alam, M., & Masud, M. (2022). Security and privacy aspects of cloud computing: A smart campus case study. Intelligent Automation & Soft Computing, 31(1), 117-128.

https://doi.org/10.32604/iasc.2022.016597

Hendre, A., & Joshi, K. P. (2015). A semantic approach to cloud security and compliance. 2015 IEEE 8th International Conference on Cloud Computing. https://doi.org/10.1109/cloud.2015.157

Kumar, A. (2017, October 20). *How does cloud-based security work: Blog*. JK Tech. https://jktech.com/blogs/how-does-cloud-based-security-work/

Muhammad Raza. (2020, August 31). *Public vs private vs hybrid: Cloud differences explained*. BMC Blogs. https://www.bmc.com/blogs/public-private-hybrid-cloud/

Saha, M. (2022). The Significance of Cloud Computing – Relecura. [online] relecura.com. Available at: https://relecura.com/the-significance-of-cloud-computing/ [Accessed 5 Jun. 2023].

Shackleford, D. (2020, May 27). *Top 6 cloud security analytics use cases: TechTarget*. Security. https://www.techtarget.com/searchsecurity/tip/Top-6-cloud-security-analytics-use-cases

Siemons, F. (2019, February 13). *5 Key Cloud Security Use Cases*. Infosec Resources. https://resources.infosecinstitute.com/topic/5-key-cloud-security-use-cases/

What is cloud security? cloud security defined. IBM. (n.d.). https://www.ibm.com/topics/cloud-security#:~:text=Cloud%20security%20is%20a%20 collection,as%20part%20of%20their%20infrastructure.

What is cloud computing? (n.d.). IBM - United States. https://www.ibm.com/topics/cloud-computing

What is cloud security? - Definition & challenges | VMware. (2023, May 17). VMware. https://www.vmware.com/topics/glossary/content/cloud-security.html

What is cloud security? | Google cloud. (n.d.). Google Cloud. https://cloud.google.com/learn/what-is-cloud-security

What is cloud security? (2021, May 6). Forcepoint. https://www.forcepoint.com/cyber-edu/cloud-security

Yerukala, M. (2021, April 22). what is cloud security: Benefits of cloud security. Mindmajix. https://mindmajix.com/what-is-cloud-security

Research Article

Inside the Mind of Cybercriminals: Investigating the Influence of Socioeconomic Factors on the Ethical Decision-Making of Cybercriminals

Ahmad Syamil Ismail[1], Muhammad Adam Muqhlis Mohamad Haniff[2], Muhammad Nazmi Md Radzi[3] and Mohamad Rahimi Mohamad Rosman[4,*]

[1] Universiti Teknologi MARA Kelantan Branch; 2020852852@student.uitm.edu.my; 0009-0002-4660-7775
[2] Universiti Teknologi MARA Kelantan Branch; 2020476482@student.uitm.edu.my; 0009-0009-3880-9247
[3] Universiti Teknologi MARA Kelantan Branch; 2020609058@student.uitm.edu.my; 0009-0001-4101-0008
[4] Universiti Teknologi MARA Kelantan Branch; rahimimr@uitm.edu.my; 0000-0001-9715-2905
* Correspondence: rahimimr@uitm.edu.my; 019-9891306.

Abstract: *Cybercriminals engage in illicit actions and purposefully exploit weaknesses in computer systems, networks, and users' information for personal benefits. Their activities are unethical by definition since they violate the ideals of privacy, integrity, and honesty. Ethical behaviour considers the repercussions of one's actions, respect the rights and well-being of others, and adhere to society norms and legal systems. Unethical behaviour has substantial consequences towards people, organisations and nations. Cybercriminals, by definition, put their own interests before ethical concerns. It was discovered that in this digital era, most internet users have been impacted by the ramifications of digital manipulation strategies such as scamming, luring, misleading information on social media and et cetera. The altering or modification of digital material, such as photographs, videos, audio, or text, to intentionally deceive or mislead the audience is referred to as digital manipulation. It entails the use of digital tools and software to alter the original information in ways ranging from modest upgrades to outright fabrications. In this study, we gathered material by collecting research papers via online databases as well as utilising the Google search engine to acquire definitions and case studies connected to the topic. This paper has identified factors that are influencing the ethical behaviours of perpetrators to perform such devious acts upon other users. Some of these factors were for profit motive, unaware of the consequences, anonymity, peer influences or subcultures and user dependency on technologies. We also constructed a conceptual framework at the end of the research to analyse the relationship between factors of cyber-crimes and the ethical behaviour of perpetrators.*

Keywords: Ethical Behavior; Cybercriminal; Digital Manipulation.

DOI: 10.5281/zenodo.8180744

1. INTRODUCTION

In an era dominated by technology and the widespread accessibility of information, the power of digital manipulation has emerged as formidable challenges. The rapid emergence of digital tools and platforms has transformed how people interact, exchange ideas, and consume information. However, these developments bring with them a risk: the distortion, manipulation, and propagation of false narratives on an unprecedented scale.

Digital manipulation refers to a variety of fraudulent tactics used to change, manipulate, or distort digital material such as photos, videos, audio recordings, and text. Individuals or groups may change visual and audio aspects with astounding accuracy when equipped with advanced editing tools, blurring the border between truth and illusion. Manipulation can range from harmless upgrades to more subtle deceptions designed to manipulate public perception, destroy trust, or advance personal or political objectives. In the modern digital age, ethical behaviour towards data manipulation is critical. Given individuals and organisations have access to huge amounts of data and the ability to broadcast information globally, ethical standards must be followed in order to maintain trust, integrity, and social well-being.

As technology has become more sophisticated over the previous decade, complaints of cybercriminal activities have surged. In comparison to 2010, there have been approximately 4.7 million reports of cybercrime in 2020. This sudden growth will cost the economy trillions. Cybercriminals are growing more devious as they evolve. Their attack vectors are continually altering dependent on the targets they chose. The perpetrators utilised a variety of strategies, including internet scamming, luring, identity theft, online sexual harassment, distributing false information and more. These strategies can have influence on enterprises, degrade other people's reputations, and misuse other people's information for personal gain. Hence, it is of the utmost importance that users become cognizant of the current cybercrime events that have been plaguing nations throughout the world and take measures to prevent being victimised.

The study and application of ethical concepts and values in connection to the gathering, dissemination, storage, and use of information is referred to as information ethics. It includes ethical issues and obligations related to information technology, digital media, data privacy, intellectual property, and information access. Information ethics aids in the development of trust in digital systems, organisations, and institutions. It promotes public trust and confidence by encouraging openness, accountability, and ethical behaviour in the processing of information, as well as investigating the larger social and ethical implications of information technology. This examines themes such as cyberbullying, online harassment, disinformation, and the influence of digital technology on social interactions, democracy, and human rights.

2. METHOD & MATERIAL

This study was carried out by collecting research papers from online databases as well as references from the internet, including case examples correlating with the subject under discussion and developing a conceptual research model.

2.1. Research Paper Collection

We discovered quite a number of research articles that investigate the same topic as our discourse. These articles serve as our references for additional understanding and discussion, allowing our readers to grasp the fundamental goal of our research. These materials were obtained via numerous online databases, including Emerald, Scopus, and even Google Scholar.

2.2. Google Search Engine

We managed to seek out definitions and sample cases related to the stated topic through the use of the Google search engine. By doing so, we were able to justify our arguments based on the findings that were provided by Google.

2.3. Conceptual Framework

We developed a conceptual framework, to show the correlation between the factors of cybercrimes which included (profit motive, anonymity, peer influenced and subcultures, user dependency on technology and unaware of the consequences) and the ethical behaviour of perpetrators.

3. FINDINGS

According to our research, we uncovered a variety of attributes that affected cybercriminals' ethical behaviour in carrying out such deceitful crimes on their victims. The above attributes included:

3.1 Profit Motive

For cybercriminals, financial gain is a powerful motivator. The possibility of making rapid and large earnings through acts such as hacking, identity theft, ransomware, or fraud can lead to persons prioritising selfish gain over ethical considerations. According to (Mohd Zaharon and Mohd Ali, 2021) Malaysian authorities have seen an upsurge in cybercrime phishing incidents, which result in large monetary losses. A different case in fact is the Central Bank of Malaysia (BNM), which recorded a loss of 0.00002% on any financial transaction as a result of phishing schemes. (Sharifah er al., 2019). These perpetrators employ a variety of tactics to entice their victims into their schemes. For instance, phishing which is "an act of deception whereby impersonation is used to obtain information from a target" (Lastdrager, 2014). Phishing attacks are the fifth most prevalent source of security breaches and have the greatest success rate. (Verison, 2019). Cybercrimes such as internet scams, frauds, or phishing can result in criminal penalties under the Personal Data Act 2010. Penalties may differ based on the amount of money involved, the number of victims, and the perpetrator's purpose. Convictions in some situations can result in three years in prison, penalties, or both.

Furthermore, since the emergence of COVID-19, online purchase fraud cases in Malaysia have escalated dramatically during the Movement Control Order (MCO). Cybercriminals may target people, organisations, or even governments in order to gain sensitive information such as credit card numbers, bank account information, or personal information, which may then be monetized in a variety of ways. It was reported in Malaysia, where 6187 people were scammed by online vendors (Bavani, 2020). Profiteering, not showing pricing, false representation and deceiving consumers about items, selling counterfeit goods and services that have already been paid for, and pyramid scheme-type businesses were among the cases. Thus, it is important that consumers acknowledge the neverending fraud cases in order to avoid falling victim to online scams. By providing sufficient education on the importance of cybersecurity and raising awareness of scamming concerns, the number of scamming incidents would gradually decrease.

3.2 Unaware of the Consequences

In other circumstances, cybercriminals may believe they are unlikely to be detected or face legal penalties for their crimes. Because of the global nature of cybercrime, jurisdictional problems, and differing enforcement capacities across nations, cybercriminals may believe they may act with impunity. One of the motives that prompted these offenders to perform such atrocities was the rapidly evolving nature of cybercrimes that often outpaces the development of legal frameworks and enforcement mechanisms. Existing laws may not effectively handle new types of cyberattacks or strategies, making it harder to prosecute hackers. Given the advancements in the electronic medium, the rate of cybercrime victimisation during the stay-at-home order has grown (Kranenbarg et al., 2019). According to research, perpetrators have developed a new ransomware known as "CoronaVirus" and a fraudulent browsing application (connected to medicine treating coronavirus) to encrypt end-user data. It was also revealed that most hackers try to share personal videos/photos of their victims, compose negative remarks about these individuals, or spam emails, interactive websites, malware, and Trojans to their victims during the stay-at-home order. (EUROPOL, 2020). The creation, distribution, or use of harmful software, such as malware or ransomware, is frequently considered a severe offence under the Computer Crime Act of 1997. For example, the dissemination of ransomware may result in severe sanctions since it involves extortion and possible financial loss to victims. Fines, jail, or both are possible penalties.

Moreover, most cybercrimes went unreported due to issues such as victims' unwillingness to come forward, fear of negative publicity, or confusion about where to report such instances. Underreporting might lead to the sense that cybercrime is not being addressed sufficiently. Evidently, in the case of cyberstalking, anonymity allows offenders to reach more potential victims with less chance of identification or punishment (Marganski, 2019). As a result, people on the receiving end tend to have a lower quality of life, likely to adjust their school or work-related routines, acquire poor psychological outcomes such as depression or anxiety, incur financial consequences, suicidal thoughts, or begin to distrust others (Marganski, 2019). It was stated that cyberstalking has long been infamously difficult to prosecute since most victims are hesitant to disclose such events owing to social ramifications (Marganski, 2019). Hence, reporting cybercrime and being aware of the issue at hand are critical, since reporting cybercrime assists law enforcement and cybersecurity specialists to take action to avoid potential collateral damage. By contributing knowledge of cyber risks through reporting events, allowing authorities to detect patterns, trends, and new attack vectors. Such information may be utilised to create preventative actions and strengthen cybersecurity defences.

3.3 Anonymity

The internet's obscurity has the potential to motivate users to engage in immoral behaviour. Cybercriminals can hide behind digital identities, making it difficult to track their movements and lowering their fear of being detected and held accountable. Due to the fact that anonymity allows cybercriminals to create and utilise fictitious identities, it is easier for them to impersonate people online. This may be used in a variety of cybercrimes, including identity theft, phishing, and social engineering crimes. Perpetrators can deceive victims by appearing as trustworthy entities, increasing susceptibility and allowing for effective exploitation. Most internet fraudsters used a well-planned and sophisticated technique to defraud their potential victims, especially when it occurred to fake lotteries, romance scams, gaming scams, and prize draw scams. (Ketchell, 2019). It is noticeable that individuals frequently become victims due to the art of persuasion (Broadhurst et al., 2020). For instance, many hackers construct fictitious female or male usernames in chat rooms to lure their victims in. Notably, people with female identities got an average of 100 threatening or sexually explicit messages each day, whereas males received just 3.5 messages per day (Nadim & Fladmoe, 2021). According to the Communication and Multimedia Act 1998, it forbids the publication of online content that is vulgar, indecent, false, threatening, or insulting in nature. This might be used to report online sexual harassment, vile comments, and threats of murder or rape. The conviction under section 233, an infraction under this section is punished by up to one year in jail, a fine of up to RM50,000, or both. Social Control Theory, on the other hand, explains why people respect laws and how behaviour conforms to societal expectations. According to Social Control Theory, internal limitations emerge during childhood, and crime develops as a result of inadequate constraints. In other words, free will provides offenders with the ability to choose and so take responsibility for their deviant action. The argument that online anonymity encourages permissiveness is supported by Social Control Theory. Individuals are obligated to stop from unlawful and deviant activity when social controls, such as social ostracism and legislation, are present, according to Social Control Theory. However, deviation increases where controls or the perceived strength of controls are absent or reduced (Rogers, Siegfried, & Tidke, 2006).

Anonymity makes it challenging to pin down cybercrime to specific individuals or groups. Due to the use of anonymization techniques and worldwide reach, investigating agencies frequently confront challenges in tracing cybercriminal actions to real-world identities. It can be used by individuals with malicious intent to lure and exploit victims online. This can be seen in another case where several child sex offenders appeared to be the same age as the adolescents in order to easily approach them (Maras, 2019). Females are also readily enticed by perpetrators using a number of methods such as false promises of love relationships, falsified career prospects with high pay in another nation, or false pledges to make them more renowned. In addition to this, females are victimised by internet luring in a variety of ways, including gender-based slurs or harassment, cyberstalking, slut-shaming, sextortion, electronically facilitated trafficking, and unwanted pornography (Maras, 2019). Internet luring is defined as a deceptive practice in which individuals attempt to deceive their potential victims by using various online platforms such as chat rooms, employment websites, email, and et cetera. Therefore, the stated cases above justify why the anonymity of the internet and de-individualization in cyberspace can reduce self-regulation and lead to uninhibited behaviour.

3.4 Peer Influence or Subcultures

Peer influence may have a substantial impact on cybercrime, both encouraging and discouraging it. Peer standards and social pressure are important in moulding behaviour, including participation in cybercrime. Individuals may be more prone to participate in cybercriminal acts to fit in or acquire social status if such behaviours are regarded normal or even applauded within a certain peer group. Individuals may be discouraged from participating in cybercrime if their peer group strongly rejects it, for fear of social disapproval. Social pressure to conform causes us to act in ways that contradict or are incongruent with our inner convictions. (Ajzen, 1991). To some extent, the predatory influence of recession, exposure to low living standards, and an uncooperative socioeconomic atmosphere of their situation with people with comparable life chances. For example, the shared conditions of unemployment, poverty, pessimism, and a grim future elicit comparable emotions throughout the population in the group. In an unemployment perspective, one of the causes is that businesses may curtail or freeze hiring during periods of economic recession or slowdown, resulting in increased unemployment rates. This can be triggered by a variety of circumstances, including global economic conditions, financial crises, or changes in the business. According to Sobieralski (2020), travel limitations imposed by governments have had a significant influence on the mobility of people throughout the world, while also having a detrimental impact on various downstream businesses such as tourism, hospitality, and transportation. Flight cancellations and capacity cuts have forced the airline sector to struggle for survival. Due to numerous cash flow challenges during the one-year lockdown period due to COVID-19, certain domestically developed airlines, such as Malindo Air, had thrown up the towel, resulting in the bulk of its personnel losing their employment, with just 1000 staying employed (Ram 2020; Birruntha 2020).

As youths band together to build a shared path towards surviving an agonising socioeconomic catastrophe, the peer impact becomes more effective. For instance, a group of people stumbles onto a website that sells high-end equipment at ridiculously low costs. They urge each other to take advantage of the discount, despite their suspicions that the website is engaged in fraudulent operations. They then use stolen credit card information to make purchases and encourage others to do the same. Credit card fraud is commonly defined as the use of stolen credit card information without the cardholder's authorization. This can include making transactions online, in-person, or over the phone with stolen credit card information. Most incidents of credit card fraud that result in criminal charges are handled at the state and municipal levels. Fraud is prosecuted differently in various states. The severity of the sentence is determined by a variety of variables, including the fraudster's previous past, the amount taken, and whether he or she has criminal intent. According to the Department of Justice, fraudulent credit card use can also be classified as computer fraud, mail fraud, wire fraud, and financial institution fraud, with penalties of up to 30 years in jail. Research has shown individuals are impacted not just by the behaviour of their significant others in the social context, but also by the behaviour of others with whom they have similar characteristics and dispositions (Philip & Cartensen, 1986).

3.5 User Dependence on Technology

Technological breakthroughs have permitted previously unimaginable levels of connectedness. People may communicate with one another internationally and get information by using the internet, wireless networks, and communication technologies. Technology, notably social media platforms, has transformed communication by giving immediate and simple means to communicate with people all over the world. People may now communicate with friends, family, and coworkers in real time, exchange updates, and engage in real-time dialogues, building a sense of togetherness and community. Furthermore, social media sites provide a wide range of entertainment alternatives, including films, games, and interactive material. They give a forum for self-expression, creativity, and the exchange of ideas with others. For many people, social media has become an essential element of their leisure activities. However, technology has its own setbacks. The rapid advancement of technology has made it increasingly difficult to detect cybercrimes. In fact, according to (Norton, 2016) 689 million people in 21 countries have experienced cybercrime in their daily lives in the past couple of years. This has made people equally fearful of online risks as they are of real-world risks. Indians are becoming the largest users of several mobile applications and websites, which has made it more challenging for security service providers to ensure safety. Cybercriminals take advantage of this by attacking online through fake apps by putting them in the play store. Such applications are intended to trick users and do dangerous actions. They may promise to provide services such as free downloads, game cheats, or access to exclusive material, but they infect devices with malware, steal personal information, or engage in fraudulent activities.

Mobile banking malware is becoming more sophisticated, and attackers are stealing more than just credit card data by staying under the radar and bypassing security mechanisms. According to Nilesh Jain, vice president, Southeast Asia and India, Trend Micro, "With banking increasingly becoming an integral part of mobile device usage, attackers have begun building more sophisticated capabilities into their mobile banking malware." One of the most famous cases of cybercrime in the virtual world is "The game Blue Whale challenges," created by 21-year-old Russian Phillip Bedecking. The game was played by children in the virtual world and claimed an estimated 130 lives across the world during 2015-2016. According to Symantec, 45% of the most popular Android apps and 25% of the most popular iOS apps request location tracking, 46% of popular Android apps and 24% of popular iOS apps request permission to access the device's camera, and email addresses are shared with 44% and 48% respectively. This highlights the importance of being cautious when granting permissions to apps. Consumers are more likely to experience cybercrime than get the flu, and 76% of consumers say they are more alarmed than ever about their privacy. Additionally, 95% believe that it's very important to require companies and organisations to give consumers control of their personal data, including 44% who believe it is necessary that companies do this, or consequently be fined. It's crucial for individuals to take necessary precautions and for companies to prioritise data privacy and security.

4. DISCUSSION

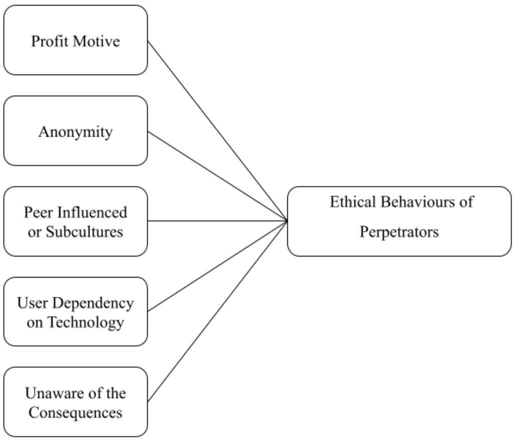

Profit Motive
Anonymity
Peer Influenced or Subcultures
User Dependency on Technology
Unaware of the Consequences
Ethical Behaviours of Perpetrators

Figure 1. Conceptual Framework

The relationship between criminals' ethical behaviour and the profit incentive in cybercrime is complicated and interconnected. For cybercriminals, the economic motivation, motivated by the desire for financial gain, frequently trump's ethical considerations. The chance of quickly and significantly increasing one's profits through acts such as hacking, identity theft, ransomware, and fraud can cause people to prioritise their own self-interest over ethical limits. Financial gain is one of the primary reasons for cybercriminals. To fool their victims and get sensitive information that may be monetized, they use numerous strategies such as phishing, online scams, and fraud. The allure of money advantages can distract criminals to the ethical ramifications of their activities, especially when there is a perceived minimal chance of detection or legal consequences. The profit motivation may be evident in situations of online purchase fraud, where individuals are duped by fraudulent online retailers, in the context of cybercrime. Profiteering, misleading representation, and selling counterfeit goods are all practices used by offenders to maximise their financial profits at the expense of unwary consumers. This exemplifies how profiteering may lead to immoral behaviour in the cyber sphere.

Furthermore, the unawareness of the consequences might contribute to ethical violations in cybercrime. Because of the worldwide nature of cybercrime and the constraints of jurisdictional concerns and enforcement capacity, cybercriminals may assume they are unlikely to be identified or suffer legal ramifications. The dynamic nature of cybercrime frequently outpaces the development of legal frameworks and enforcement procedures, making prosecution of perpetrators more difficult. This absence of penalties, or the perception of impunity, might motivate unethical behaviour in the quest of financial gain.

Additionally, Anonymity is a strong motivator for people to engage in unethical behaviour in cyberspace. Because of the internet's anonymity, cybercriminals may hide behind digital identities, making it harder to monitor and hold them accountable. This anonymity may be used to mimic others, which can lead to a variety of cybercrimes such as identity theft and phishing. The capacity to deceive victims by posing as trustworthy institutions boosts the success of cybercriminal actions, emphasising the relationship between anonymity and unethical behaviour even more.

Peer influences and subcultures can also impact cybercriminal behaviour. Individuals may participate in cybercrime due to social pressure and the desire to fit in or obtain social prestige within a certain peer group. Individuals may be more likely to engage in immoral behaviour if such behaviours are normalised or celebrated within their social group. Individuals may be discouraged from participating in such behaviour if there is a strong condemnation of cybercrime within their peer group.

Last but not least, user dependence on technology and the rapid advancement of digital platforms have produced an environment conducive to cybercrime. The growing number of users and their dependency on mobile applications and websites has made it difficult for security service providers to assure their customers' safety. Cybercriminals take advantage of this by exploiting flaws in the technical infrastructure and targeting naive consumers with tactics such as mobile banking malware and bogus apps. The rise of personal data sharing and app permissions increases privacy and security issues, underscoring the need for consumers and businesses to prioritise data protection. Conclusively, the profit motive, unawareness of consequences, anonymity, peer influences, and user dependence on technology are all aspects that lead to ethical breaches in cybercrime. Understanding these dynamics is critical for designing successful measures to prevent cybercrime and encourage ethical digital behaviour. Education, knowledge, robust regulatory frameworks, and increased cybersecurity measures are critical in minimising the impact of profit-driven immoral behaviour in the cyber realm.

5. CONCLUSION AND IMPLICATIONS

In conclusion, prioritising cybersecurity and information ethics is critical for people, organisations, and governments. Education and understanding of cybersecurity threats are critical for empowering consumers to protect themselves and avoid being victims of cybercrime. To dissuade cybercriminals and hold them accountable for their acts, legislative frameworks and enforcement tools must be strengthened. To safeguard individuals, organisations, and society as a whole from the dangers and repercussions of cybercrime, it is of the utmost importance to create a safer and more secure digital environment.

Preventing cybercrime necessitates being proactive and practising excellent digital hygiene. Look for phishing indications such as misspelt email addresses, generic welcomes, frantic requests for personal information, or unknown URLs. Furthermore, users should exercise caution while disclosing personal or sensitive information online. Avoid sharing too much personal information on social media networks, and restrict access to your profiles by adjusting privacy settings. Moreover, it is critical to remain up to date on the latest cyber threats and frequent frauds. Educate yourself on recommended practises for internet safety on a regular basis, such as spotting warning signals and adopting secure behaviours.

Acknowledgments: We would like to express our appreciation to Dr. Mohamad Rahimi Mohamad Rosman, the paper's co-author. He has guided us through the process of completing this research paper. This work is also supported through funding by the UiTM Campus Machang Academic Affairs via the KW3P system. This research paper would not have been completed without all the support provided to us.

References

Bandura, A. (1990). Mechanisms of moral disengagement. In W. Reich, *Origins of Terrorism; Psychologies, Ideologies, Theologies, States of Mind* (pp. 161-191). New York: Cambridge University Press.

Bandura, A., Barbaranelli, C., Caprara, G., & Pastorelli, C. (1996). Mechanisms of moral disengagement in the exercise of moral agency. *Journal of Personality and Social Psychology* , 71, 364-374.

Rogers, M. K., Siegfried, K., & Tidke, K. (2006). *Self-reported computer criminal behavior: A psychological analysis.* Lafayette: The Digital Forensic Research Conference.

Gilbert,J. Archer, N. (2011). Consumer Identity Theft Prevention and Identity Fraud Detection Behaviours. *Journal of Financial Crime*, *19*(1), 20–36.

Singh, Arpita & Singh, Sanjai. (2019).Technology Revolution Gives Cybercrime A Boost: Cyber-Attacks And Cyber Security 1.

K, T. N., Mas'ud, F., & Hassan, Z. (2022). Level of Cybercrime Threat During the Outbreak of COVID-19 Pandemic: A Study in Malaysia. *International Journal of Academic Research in Business & Social Sciences*, *12*(5). https://doi.org/10.6007/ijarbss/v12-i5/13142

Lee, Y. C., Gan, C. K., & Liew, T. W. (2022). Phishing victimization among Malaysian young adults: cyber routine activities theory and attitude in information sharing online. *The Journal of Adult Protection*, *24*(3/4), 179–194. https://doi.org/10.1108/jap-06-2022-0011

Manoharan, S., Katuk, N., Hassan, S., & Ahmad, R. (2021). To click or not to click the link: the factors influencing internet banking users' intention in responding to phishing emails. *Information & Computer Security*, *30*(1), 37–62. https://doi.org/10.1108/ics-04-2021-0046

Jegede, A.E., Olowookere, E.I. & Elegbeleye, A.O. (2016). Youth identity, peer influence and internet crime participation in nigeria: a reflection. *Ife PsychologIA. 24*(1), 37-47.

Yik, C. S. (2022, January 7). *Basics of Cyber Security Law in Malaysia - Chia, Lee & Associates*. Chia, Lee & Associates. https://chialee.com.my/basics-of-cyber-security-law-in-malaysia/#:~:text=Personal%20Data%20Protection%20Act%202010%20%E2%80%93%20Compliance%20with%20PDPA%20Act%202010,years%20in%20jail%2C%20or%20both.

Cyber-Harassment Survivor's Kit – FAQs | MCCHR. (n.d.). https://mcchr.org/chsk_faq/#:~:text=Communications%20and%20Multimedia%20Act%201998,and%20death%20or%20rape%20threats.

Ransomware - The Malaysian Legal Perspective - Azmi & Associates. (2023, April 3). Azmi & Associates. https://www.azmilaw.com/insights/ransomware-the-malaysian-legal-perspective/#:~:text=a)%20Computer%20Crimes%20Act%201997%20(%E2%80%9CCCA%201997%E2%80%9D)&text=Section%205%20of%20CCA%201997,of%20contents%20of%20any%20computer.

Threatcop. (2022). An Increase in Cybercrime Continues to Haunt Cyber World. *Threatcop*. https://threatcop.com/blog/increase-in-cybercrime/

Muscanell, N. L., Guadagno, R. E., & Murphy, S. M. (2014). Weapons of Influence Misused: A Social Influence Analysis of Why People Fall Prey to Internet Scams. *Social and Personality Psychology Compass*, *8*(7), 388–396. https://doi.org/10.1111/spc3.12115

Nga, J. L., Ramlan, W. N. M., & Naim, S. (2021). Covid-19 Pandemic and its relation to the Unemployment situation in Malaysia: A Case Study from Sabah. *Cosmopolitan Civil Societies: An Interdisciplinary Journal*, *13*(2). https://doi.org/10.5130/ccs.v13.i2.7591

Bessette, C. (2023). How Serious a Crime Is Credit Card Theft and Fraud? *NerdWallet*. https://www.nerdwallet.com/article/credit-cards/credit-card-theft-fraud-serious-crime-penalty#:~:text=Make%20an%20online%20purchase%20with,and%20forfeiture%20of%20personal%20assets.

Research Article

Ethics in Business and Professional Ethics: Guidelines for Responsible Decision Making and Conduct

Ahmad Fauzi Ahmad Taufek[1], Ku Muhammad Hafiz Ku Suid[2], Muhammad Afieq Bahauddin[3], and Zaila Idris[4] *

[1] Universiti Teknologi MARA; 2020834338@student.uitm.edu.my; 0009-0009-4980-7490

[2] Universiti Teknologi MARA; 2020821976@student.uitm.edu.my; 0009-0009-8962-3004

[3] Universiti Teknologi MARA; 2021101157@student.uitm.edu.my; 0009-0004-0785-9798

[4] Universiti Teknologi MARA; zaila267@uitm.edu.my; 0000-0002-8287-6430

* Correspondence: zaila267@uitm.edu.my; 012-9329530.

Abstract: *This research paper examines the potential for commercializing ethics in business and professional ethics, focusing on guidelines for making responsible decisions and conducting oneself. In today's competitive market, organizations face growing pressure to demonstrate ethical behavior while also using it as a competitive advantage. Through a thorough analysis of existing literature, this study investigates the ways in which ethical practices can drive commercial success. By adopting and implementing ethical guidelines, organizations can bolster their reputation, appeal to ethical consumers, and differentiate themselves from competitors. Ethical conduct fosters trust and credibility among stakeholders, resulting in increased customer loyalty, a positive brand image, and long-term sustainability. The findings highlight that ethics is not solely a moral obligation but also a strategic driver for business. Organizations that embrace ethical principles and integrate them into their operations can gain a competitive edge, explore new market opportunities, and achieve long-term profitability. Ethical conduct also contributes to employee engagement, attracting and retaining talented individuals who value an ethical work environment. Overall, this research underscores the significance of ethics as a valuable commercial asset and offers insights into how organizations can leverage ethical guidelines to enhance their market position, attract ethical consumers and investors, and foster sustainable growth. By prioritizing responsible decision-making and ethical behavior, organizations can contribute not only to a better society but also realize substantial commercialization potential.*

Keywords: ethics, business ethics, professional ethics, responsible decision making, conduct.

DOI: 10.5281/zenodo.8180989

1. INTRODUCTION

In today's complicated and linked world, ethics in business and professional behavior is becoming increasingly important. As organizations face ethical difficulties and make decisions with far-reaching consequences, the importance of responsible decision-making and ethical behavior becomes crucial. This introduction gives an overview of the importance of ethics in business and professional ethics, emphasizing its difficulties, commercialization potential, and role in managing organizations toward responsible practices.

Ethics acts as a guiding framework that shapes organizational behavior and decision-making processes. Furthermore, the findings demonstrated that ethics is an intangible asset that influences an organization's competitiveness (Lee, 2020). In the interaction between the state and civil society, ethics have a significant impact on the efficacy of legal activities, support the system of social conditions, and support the institutions of power, its brands, authority, and image (Oleinykov, 2022).

The importance of ethics in business goes beyond its moral importance. It is becoming recognized as a strategic advantage that can have an impact on a company's reputation, brand value, and overall performance. It is concluded that developing work ethics is necessary in order to improve the performance quality of employees (Almahjob Jamal, 2018). Ethical behavior can increase customer loyalty, attract ethically conscious consumers, and differentiate businesses in competitive markets. Furthermore, ethical practices can develop beneficial relationships with employees, investors, and communities, promoting long-term sustainability and profitability.

The purpose of this research study is to investigate the commercialization possibilities of business and professional ethics. It tries to discover how organizations might use ethics as a competitive advantage by investigating the relationship between ethical practices and business success. This investigation will look into the effects of ethical behavior on market positioning, brand reputation, and customer trust. It will also look into the impact of ethics in fostering employee satisfaction and commitment, as well as establishing an engaging work environment and attracting top talent.

This research helps to a better understanding of the strategic role of ethics in driving business practices by highlighting the multiple links between ethics and commercial success. It emphasizes the importance of making sound judgments and acting ethically to maintain long-term viability, stakeholder trust, and societal influence. The study's findings will be valuable for organizations seeking to incorporate ethics into their core business practices and foster an environment of ethical awareness and responsibility. Finally, the goal of this research is to highlight the significance of ethics as a driver of long-term growth, profitability, and positive society consequences.

2. METHOD & MATERIAL

This paper introduces a broad literature review based on the previous paper, followed by an explanation of the topic that we want to explain. In particular, the authors use ethics in the business research literature as a case study for this literature analysis. This research paper adopts a literature analysis methodology to investigate the topic of business ethics and professional ethics. The primary goal is to critically study and analyze existing literature to get insights into guidelines for responsible decision making and organizational behavior.

2.1 Data Collection:

The data collection procedure includes gathering relevant scholarly papers and other trustworthy sources that investigate ethics in the context of business and professional ethics. Academic publications and online libraries, as well as electronic databases such as Emerald Insight, Scopus and Google Scholar, will be thoroughly searched using keywords related to the research topic. Inclusion and exclusion criteria will be utilized to choose relevant study material. A timeframe for selecting articles will be determined based on the research objectives and available resources. The timeframe that been used for this research paper has been set to the previous five years, with a focus on recent publications to capture the most recent information and insights.

2.2 Data Analysis:

The chosen literature will be thoroughly reviewed and analyzed to uncover essential themes, concepts, and conclusions concerning business and professional ethics. A systematic review of the literature will be conducted, as well as an evaluation of the theoretical frameworks, techniques, and empirical evidence offered in the research.

2.3 Limitations:

It is critical to recognize the limits of the methods used for literature analysis. The conclusions are influenced by the quality and relevancy of the literature used, which may induce biases. Furthermore, the study is limited to already published publications, and any gaps or restrictions in the literature may alter the conclusions' comprehensiveness.

3. FINDINGS

In this literature analysis, we looked at a wide range of scholarly works and academic papers on business ethics and professional ethics. The analysis aimed to uncover major findings and themes concerning rules for responsible decision-making and conduct. The following findings were drawn from the literature review:

3.1 A single code of professional ethics for the business community

Below is a single code of professional ethics for the business community that was created by Dinah Payne and Milton Pressley. This single code is created by the author so it can be used regardless of the venue or specialty of the marketing professional. It has been created by the author using the old and more broadly known theories of ethics, and currently-used codes of professional marketing ethics, including those from the American Marketing Association (AMA), the American Association of Advertising Agencies (AAAA), and the Sales and Marketing Executives International (SMEI), and by that theory of ethics and currently use code, the author has determined the most prominent, efficacious principles of ethics and to shape a single code of professional conduct.

Table 1. Transcendent code of ethics for marketing professionals. Adapted from "A transcendent code of ethics for marketing professionals" by Payne, D. & Pressley, M., 2013, Journal of Law and Management. https://doi-org.ezaccess.library.uitm.edu.my/10.1108/17542431311303822. Copyright 2013, Emerald Group Publishing Limited.

Concepts created from synthesised frameworks and principledly solidified	**Proposed standard business ethics code for marketing professionals**
Consistency Self-control	Use self-control to treat all consumers and stakeholders consistently, avoiding negative acts towards all stakeholders.
Magnanimity	Treat all stakeholders with dignity, fairness, and openness.

Generosity	Avoid using coercion or any other measures that undermine customer confidence.
Respect	In a setting of competition, offer a range of possibilities. By guaranteeing freedom of choice and supplying accurate, pertinent, and comprehensive information to all relevant parties, establish partnerships that are both mutually beneficial and open.
Utility Magnificence	Utilize the highest ethical standards in decisions effecting all stakeholders Be involved with all relevant communities and stakeholders through public service of significance
Autonomy Integrity Justice Courage	Recognising the autonomy that comes with specialisation and professionalism, make decisions that affect stakeholders with rationality and honesty. Ensure that customers have the chance to voice issues and complaints about products, and that the matter is addressed in a timely and competent way. Ensure that customers obtain an appropriate resolution of their legitimate claims. Be courageous in all decisions ensuring that justice is achieved Avoid dehumanizing actions
Competence	Adhere to all codal and ethical provisions
Sociability	Be kind and effective when interacting with people. Act in good faith to uphold your obligations to all stakeholders in terms of the law, business, philanthropy, and society. Recognise your responsibilities to vulnerable market segments. Assure that your products do not harm consumers or society when used and disposed of properly. Make certain that all acts contribute to a healthy environment.

A proposed uniform professional code of ethics for marketing professionals, academics, and students is presented here, and it comprises a number of figures and tables. Any business professional—indeed, any well-educated and well-intentioned person—should be able to understand it and put it to good use when faced with morally challenging decisions. The right-hand column represents the first steps in creating a uniform code of ethics that is expressly targeted at the marketing industry. Whole society, business professionals, and those working in marketing would all gain if those professionals relied on social and business ethics as a foundation for making morally sound marketing judgements. Reviewing the suggested rules demonstrates how rational it is to have a single code of ethics for all business professionals, including marketing specialists, and how it might be a useful solution for those professionals who face moral conundrums.

3.2 Ethics Training and Communication.

Organizations must offer ethics training and encourage open communication to ensure the proper implementation of ethical standards. Ethics training sessions play a crucial role in equipping staff members with a strong understanding of moral principles, decision-making frameworks, and real-world ethical dilemmas. This knowledge empowers employees to navigate complex ethical situations with confidence and integrity. It is also critical to build good communication channels within the organization. When faced with ethical problems, these channels allow employees to express their concerns, seek direction, and request support. Communication that is open and transparent develops a culture in which ethical issues may be addressed quickly and constructively.

According to Place (2019), moral growth can advance through time and with professional experience. By investing in ongoing ethics training and professional development opportunities, organizations can facilitate the moral development of their employees. This, in turn, enables practitioners to traverse the frequently intricate moral grey regions with the aid of education, professional training, and experience (Coleman and Wilkins, 2009; Place, 2019). Ethical leadership and effective leader-member ethical communication are also crucial elements in promoting ethical behavior within organizations. According to Abu Bakar and Connaughton (2022), the findings of their study imply that ethical leadership, in conjunction with perceived leader-member ethical communication, may improve organizational citizenship behavior. Leaders who embrace ethical language and foster a culture of ethical behavior can motivate their team members to actively participate in ethical decision-making and communication. This not only strengthens ethical conduct within the team but also extends the influence of ethical behavior beyond the team's boundaries.

Moreover, Rodriguez Gomez et al. (2020) study emphasizes the importance of ethical training in educational contexts. Their research shows that a practical training strategy based on an idealistic ethical approach and driven by stakeholder theory provides a solid basis for business students to make ethical decisions. Ethical training can enable students to manage difficult situations and contribute to the ethical growth of future business professionals by adopting a constructive, proactive, and care-oriented approach.

3.3 Role of Ethical Culture in Organizations

A strong ethical culture within organizations is essential for promoting responsible decision making and conduct. The ethical culture encompasses the shared values, beliefs, and norms that guide the behavior of individuals within the organization. Several key aspects highlight the importance of an ethical culture:

a) Influence on Employee Behavior:

An ethical culture influences employee behavior by setting clear expectations for ethical conduct. It establishes a framework for individuals to make decisions aligned with ethical principles and promotes consistency in behavior across the organization. According to Dewantara and Damayanti (2021), the study's findings indicate that work ethics have a significant and positive effect on employee performance.

b) Transparency and Integrity:

An ethical culture promotes transparency and integrity in all organizational activities. It encourages open communication, honesty, and fairness in interactions with both internal and external stakeholders. With the help of this investigation, we can see how cosmopolitan business ethics is implemented with the concepts of trust, transparency, and integrity through corporate governance, with an emphasis on the incorporation of accountability into corporate strategy (Rendtorff, 2019).

c) Impact on Reputation and Stakeholder Relationships:

Organizations with a strong ethical culture tend to enjoy a positive reputation and establish trust with stakeholders. Ethical behavior sends a signal to customers, investors, and partners that the organization operates with integrity and values its interests. It adds to the discussion about balancing ethics and sustainability as components of business strategies for reputation building and value creation by identifying key stakeholders and ethics-based non-financial disclosures made by contemporary business organisations (Kumarasinghe et al., 2021).

d) Compliance with laws and regulations:

An ethical culture promotes compliance with laws, regulations, and industry standards. It ensures that the organization operates within legal boundaries and holds itself accountable to the highest ethical standards (Klebe Treviño et al., 2001).

To establish and maintain an ethical culture, organizations should prioritize ethical leadership, promote ethical behavior through policies and codes of conduct, provide ethics training and education, and create mechanisms for reporting and addressing ethical concerns. It requires a commitment from top-level management to set the tone and lead by example, as well as continuous reinforcement of ethical values throughout the organization.

4. Discussion

The research's findings emphasise the need for a unified code of ethics for the business world. The author created this single code of ethics because anyone who has a problem with an ethical marketing issue would find it helpful, possibly easing the challenges associated with difficult ethical dilemmas in marketing as well as igniting more debate and discussion on ethical marketing standards. The author uses and incorporates ideas from examinations of the requirements for marketing ethics standards and the profession of marketing itself regarding the ethical dilemmas marketers face and the stakeholders who are impacted by marketing decisions in order to create this single code of ethics. Milton Pressley and Dinah Payne (2013) conducted the study.

The author uses and incorporates ideas from examinations of the requirements for marketing ethics standards and the profession of marketing itself regarding the ethical dilemmas marketers face and the stakeholders who are impacted by marketing decisions in order to create this single code of ethics. In order to ensure that whatever the codal provisions are, they would benefit the marketers who utilise them, the author also looked at the purposes of professional codes of ethics. As a result, the author created a single code of ethics that not only marketers can use, but also other members of society can identify with and feel confident in. This eliminates worries about mistrust or misunderstanding between those marketing goods and services and the stakeholders in society, in which case the author draws on traditional frames of ethics and combines those principles with principles found in the marketing ethics literature.

The Hunt and Vitell (1986, 2006) Theory of Ethics, which on paper seems to be a potentially overly hard model to implement, served as the inspiration for the current endeavour, which is why authors write this single code. The model was created with marketing professionals, marketing ethics instructors, and general business ethicists in mind. The Hunt-Vitell model is wonderful in many aspects, not the least of which is the fact that it has inspired a tonne of theoretical and empirical research. The model's complex structure is what makes it challenging, though. 32 are in the model. thirty causal relationships between components. According to the author, there are two issues with the model as a very helpful tool for solving marketing ethical issues. First, the model's complexity may intimidate potential users, preventing them from referencing it and eliminating the need for the model altogether. Second, we worry that business professionals who are brave enough to use the model might not have enough background knowledge on some of its 32 components to use it effectively and/or efficiently because they are unfamiliar with ethical debate.

The author's intent code is arguable and is unlikely to end up being the model. The proposed code, in the authors' opinion, will encourage more investigation, debate, and formulation. The inability of the marketing decision-maker to comprehend that there can be ethical considerations in a decision must be overcome, according to the author. Furthermore, the difficulty of examining many codes may hinder moral judgements and obviously bad circumstances. The authors hope that the code in Table will inspire additional research, discussion, and formulation since they believe that a single code would be helpful to everyone involved in making decisions in any part of marketing.

The findings presented in this research highlight the critical importance of ethics training programs and communication channels within organizations. By offering ethics training sessions, organizations can educate their staff members about moral principles, decision-making frameworks, and real-world ethical dilemmas. This knowledge empowers employees to make informed and ethical decisions in their day-to-day work. Furthermore, the establishment of effective communication channels allows employees to express their concerns, seek guidance, and request assistance when faced with ethical challenges. Open and transparent communication creates an environment where ethical issues can be addressed promptly and collaboratively. The research conducted by Place (2019) supports the notion that moral growth can advance through time and professional experience. This suggests that ongoing ethics training and professional development opportunities are crucial for nurturing the ethical development of employees. The study emphasizes the importance of providing professionals with the necessary tools and resources to navigate the complex and evolving ethical landscape, particularly in light of the integration of social and digital media into public relations and communication practices. By investing in ethics training and professional development, organizations can equip their employees with the knowledge and skills needed to navigate ethical challenges effectively.

The findings of Abu Bakar and Connaughton (2022) highlight the role of ethical leadership and leader-member ethical communication in promoting organizational citizenship behavior. Ethical leaders who embrace ethical language and foster a culture of ethical behavior can motivate their team members to actively participate in ethical decision-making and communication. This not only strengthens ethical conduct within the team but also extends the influence of ethical behavior beyond the team's boundaries. Therefore, organizations should focus on developing and promoting ethical leadership practices and fostering an environment that encourages ethical communication at all levels. The study conducted by Rodriguez Gomez et al. (2020) emphasizes the importance of ethical training in educational settings, specifically within a business studies faculty. The research demonstrates that a practical training approach, grounded in an idealistic ethical approach and guided by stakeholder theory, lays a solid foundation for business students to make ethical decisions. By adopting a constructive, proactive, and care-oriented approach, ethical training equips students with the skills and mindset necessary to navigate difficult ethical circumstances they may encounter in their future careers. This contributes not only to their personal ethical development but also to the broader philosophical approach to business ethics.

Furthermore, an ethical culture plays a vital role in shaping employee behavior and promoting ethical conduct. It establishes clear expectations for ethical behavior, which in turn influences employees to act ethically. When employees perceive that ethical behavior is valued and rewarded, they are more likely to make responsible decisions and uphold ethical standards. Additionally, an ethical culture fosters transparency and integrity within an organization. By promoting open communication, honesty, and fairness, it creates an environment that discourages unethical practices such as fraud and corruption.

Next, an ethical culture emphasizes individual and collective accountability. It encourages employees to take responsibility for their actions and consider the ethical implications of their decisions. By promoting a sense of accountability, organizations empower employees to make ethical choices and act in the best interest of stakeholders. Moreover, an ethical culture has a positive impact on an organization's reputation and stakeholder relationships. When organizations operate with integrity and ethical behavior, they build trust and credibility with customers, investors, and partners. This enhances their reputation and fosters stronger relationships, ultimately contributing to long-term success.

Lastly, an ethical culture ensures compliance with laws, regulations, and industry standards. It reinforces the organization's commitment to operating within legal boundaries and upholding the highest ethical standards (Klebe Treviño et al., 2001).

To establish and maintain an ethical culture, organizations should prioritize ethical leadership, implement policies and codes of conduct, provide ethics training and education, and establish mechanisms for reporting and addressing ethical concerns. Top-level management plays a crucial role in setting the ethical tone and leading by example, while continuous reinforcement of ethical values throughout the organization is essential.

5. CONCLUSION

In conclusion, the development and implementation of a uniform professional code of ethics for marketing professionals, as presented in this study, holds significant potential for addressing ethical challenges in the field. The proposed guidelines offer a comprehensive framework that can be easily understood and applied by marketing professionals, academics, and students alike. By providing clear ethical principles and standards, this uniform code equips individuals with the necessary tools to make informed and responsible decisions when faced with moral dilemmas. This research also emphasizes the importance of ethics training programs and communication channels within organizations. The findings highlight that providing employees with the necessary knowledge, skills, and resources to navigate ethical dilemmas enhances ethical decision-making and behavior. Open communication channels allow employees to express their concerns and seek assistance, fostering a culture of ethical behavior. Ethical leadership and leader-member ethical communication play a vital role in promoting organizational citizenship behavior. Additionally, ethics training in educational settings equips students with the skills to make ethical decisions. Overall, investing in ethics training and communication channels is crucial for promoting ethics and contributing to a positive ethical environment within organizations.

A strong ethical culture within organizations is crucial for promoting responsible decision making and conduct. The presence of such a culture has several significant implications. Firstly, it influences employee behavior by setting clear expectations and providing a framework for ethical decision making. Research results by Dewantara and Damayanti (2021) support the notion that work ethics positively impact employee performance. Secondly, an ethical culture fosters transparency and integrity, promoting open communication and fairness in all organizational activities. This is in line with the concepts of trust, transparency, and integrity highlighted in the investigation by Rendtorff

(2019) regarding cosmopolitan business ethics and corporate governance. Lastly, an ethical culture contributes to reputation building and stakeholder relationships. By balancing ethics and sustainability, organizations can create value and enhance their reputation through practices such as identifying salient stakeholders and incorporating ethics-based non-financial disclosures, as discussed by Kumarasinghe et al. (2021).

Acknowledgments: Because this study is based on existing literature, no direct participation with human subjects or ethical approval is required. However, ethical concerns are addressed by appropriately attributing and recognizing the authors and sources of the literature used in the research. This research article attempts to contribute to existing information on business and professional ethics by using a literature analysis methodology. The study's findings will provide significant insights and assistance for responsible decision making and ethical behavior in organizations. The authors would like to acknowledge the valuable contributions of Madam Zaila Idris from MARA University of Technology (MARA), who provided expert guidance and constructive feedback that greatly enhanced the quality of this research. The authors also would like to extend their deepest appreciation to all the participants who directly or indirectly contributed to this research. Their involvement and valuable insights were instrumental in the successful completion of this study.

References

Abu Bakar, H. & Connaughton, S.L. (2022). Ethical leadership, perceived leader–member ethical communication and organizational citizenship behavior: development and validation of a multilevel model. *Leadership & Organization Development Journal, 43*(1), 96-110. https://doi.org/10.1108/LODJ-07-2021-0356

Coleman, R. & Wilkins, L. (2009). The moral development of public relations practitioners: a comparison with other professions and influences on higher quality ethical reasoning. *Journal of Public Relations Research, 21*(3), 318-340.

Dewantara, F.A., & Damayanti, E. (2021). Effect of work ethics and the work environment on performance of employees of PT. Berlian Indah Abadi Nusantara Surabaya. *Jurnal Ekonomi*. https://doi.org/10.29138/je.v21i1.127

Hunt, S.D. & Vitell, S.J. (1986). The general theory of marketing ethics. *Journal of Macromarketing, 6*, Spring, 5-15.

Hunt, S.D. & Vitell, S.J. (2006). The general theory of marketing ethics: a revision and three questions. *Journal of Macromarketing, 26*(2), 1-11.

Almahjob Jamal, A. A. (2018). The role of business ethics in improving the quality of job performance. *Journal of Entrepreneurship & Organization Management, 7*(1). http://dx.doi.org/10.4172/2169-026X.1000224

Klebe Treviño, L., Butterfield, K.D. & McCabe, D.L. (2001). The ethical context in organizations: influences on employee attitudes and behaviors. *The Next Phase of Business Ethics: Integrating Psychology and Ethics, 3*, 301-337. https://doi.org/10.1016/S1529-2096(01)03018-8

Kumarasinghe, S., Peiris, I.K., & Everett, A.M. (2021). Ethics disclosure as strategy: a longitudinal case study. *Meditari Accountancy Research*. https://doi.org/10.1108/medar-01-2020-0669

Lee, D. (2020). Impact of organizational culture and capabilities on employee commitment to ethical behavior in the healthcare sector. *Service Business*, 14, 47–72. https://doi.org/10.1007/s11628-019-00410-8

Oleinykov. S. (2022). Ethics and legal aspects of public institutions' legal activities. *Grail of Science*, (14-15), 140–145. https://doi.org/10.36074/grail-of-science.27.05.2022.022

Payne, D. & Pressley, M. (2013). A transcendent code of ethics for marketing professionals. *International Journal of Law and Management, 55*(1), 55-73. https://doi-org.ezaccess.library.uitm.edu.my/10.1108/17542431311303822

Place, K.R. (2019). Moral dilemmas, trials, and gray areas: exploring on-the-job moral development of public relations professionals. *Public Relations Review, 45*(1), 24-34.

Rendtorff, J.D. (2019). The honest businessperson: cosmopolitan theory and cultural praxis (the example of denmark and scandinavia). *Ethical Economy.* https://doi.org/10.1007/978-3-030-04351-3_4

Rodriguez Gomez, S., Lopez Perez, M.V., Garde Sánchez, R. & Rodríguez Ariza, L. (2020). Factors in the acquisition of ethical training. *Education + Training*, *63*(3), 472-489. https://doi.org/10.1108/ET-01-2019-0006

Research Article

Ethics in Social Media and Digital Spaces

Nik Afiqa Mohd Zamri[1], Nurelmysha Anuar[2], Rabiatul Ainnuha Ridzuan[3], and Mohamad Syauqi Mohamad Arifin[4] *

[1] Universiti Teknologi MARA; 2020872652@student.uitm.edu.my 0009-0007-8513-345X

[2] Universiti Teknologi MARA; 2020845126@student.uitm.edu.my 0009-0000-7000-7468

[3] Universiti Teknologi MARA; 2020846694@student.uitm.edu.my 0009-0005-4381-4172

[4] Universiti Teknologi MARA; Mohdsyauqi@uitm.edu.my 0000-0002-8224-9330

* Correspondence: Mohdsyauqi@uitm.edu.my Telephone: 0103521919

Abstract: *This article explores the field of ethics and its importance in social media and progressive spaces. It talks approximately about the objectivity of ethical measures, the closeness of ethical truths, and the definition of moral concepts inside the space of second-order. As development and social media stages get to be continuously arranged into our lives, ethical thoughts in these computerized circumstances have finished up essential. The article highlights the requirement for ethical benchmarks and rules to supervise behavior in progressed spaces, tending to commitments of individuals, organizations, examiners, and chiefs. It emphasizes the centrality of ethical behavior and the potential comes about of deceitful sharpens, drawing thought to the ethical challenges stood up to by social media stages. The concept of progressed citizenship is displayed as a framework for careful and ethical development utilizing distinctive exercises,appearance, and aptitudes essential for investigating the computerized environment. The article proposes methods for progressing ethical behaviour in a few settings, checking instruction, news scope, organizations, and advancing. It emphasizes the consequence of raising mindfulness, building up rules, progressing instruction and planning, and taking after too careful measures to develop ethical conduct in progressed spaces. The composing review conducted for this article cantered on collecting noteworthy dispersions on ethics in social media and computerized spaces, utilizing specific watchwords and expressions to coordinate the see get ready through academic databases, ask approximately storage facilities, and reliable sources.*

Keywords: Ethics; Digital Spaces; social media.

DOI: 10.5281/zenodo.8181030

1. INTRODUCTION

Ethics may be a philosophical field that looks at moral measures, values, and the thought of right and off-base conduct. It looks to give a framework for assessing and comprehending human conduct in terms of morality. The objectivity of moral guidelines, the nearness of moral truths, and the meaning of ethical words are all investigated in the second-order. On controlling ethics, it looks at the different ethical theories and guidelines that affect moral speculations and measures that affect ethical inside the decision-making, such as consequentialism which is cantering based on comes approximately, in the rule-basic ethics which is canters on the commitment and laws, and convention and morals which are canters on the character and excellencies.

What is the nature of ethics concurring with second-order? It investigates the nature of ethical attestations, moral considering, and moral regard foundations. This discipline is concerned with the objectivity of moral benchmarks, the closeness of moral realities, and the definition of ethical concepts. Associated Ethics is concerned with how ethical concepts are connected in certain settings. It includes the application of ethical considerations and concepts to real-life challenges and quandaries, such as biomedical ethics, common ethics, corporate ethics, and political ethics.

Ethics in social media and progressed circumstances insinuate the rules and guidelines that direct the online conduct and instinct of individuals, organizations, and stages. As development and social media stages are acquired more facilitated into our lives, ethical questions are continuously essential in this field. The interface between ethics in social media and progressing circumstances rose in reaction to the speedy advancement and wide utilization of advancement, strikingly the rise of social stages and the net. As these stages got progressively saturated in our day by day lives, it became clear that ethical thoughts were required to handle the specific issues and issues they were given. This association may be followed back to the early days of social media and the internet. As individuals began to relate online, challenges such as online goading, security concerns, and mental property infringement began to rise. These challenges underlined the prerequisite for ethical measures and measures to control conduct in computerized places.

Particular accessories, counting individuals, organizations, examiners, and executives, have seen the significance of morals in social media and advanced circumstances over time. They started examining and debating moral concerns, as well as making systems to get them. Making repeat of cyberbullying, the dispersal of disinformation, stresses about information security and security, and the impact of calculations on substance transport are sensible a modest bunch of the components that have powered the wrangle around morals in computerized circumstances.

Moreover, high-profile occasions of moral wrongdoing by individuals, organizations, and without a question social media organizations have pulled in thought to the prerequisite of moral conduct and the conceivable repercussions of degenerate homes. Unmistakable parties are reasonably tending to and examining moral issues in social media and computerized regions these days. Social media stages are setting up approaches and rules improvement, strive and genuine utilization, security, and the launch of harming data. People and organizations are pushing for computerized well-being, locks in legitimacy, and holding others tried and true for degenerate works out online. Scholastic inquiry around, corporate conferences, and open conversation all contribute to the nonstop upgrade and refinement of moral benchmarks and homes inside the computerized world.

The careful and ethical utilization of advancement, particularly in online circumstances, is insinuated to as progressed citizenship. It encompasses a wide run of exercises, states of intellect, and capacities that individuals need to have in order to investigate the computerized environment ethically. In various work circumstances, ethical security infers supporting and supporting progressed citizenship values interior specific capable settings.

Ethical review includes every aspect of every detail of the work in progress. These relate to the amount of work registered in a computerized utility. By teaching students online safety, online chivalry, and basic thinking skills for working with digital information, educators and instructors can foster responsible and progressive citizenship. Teacher educators can set rules and benchmarks for proper use of development, avoid cyberbullying, and further develop robust online learning environments. IT staff take data backup and security seriously and may take ethical concerns about their decisions to ensure that systems and computer programs are created and updated. We can advocate for the proper use of advertising data and help businesses develop and implement practices to protect customer data, prevent unauthorized access, and address ethical issues related to advertising activities.

Scientists can adhere to ethical rules when enumerating messages in advanced spaces, ensuring truth, fairness, and candor in their work. News outlets can set rules for ethical online specs, fact-checking, and combating duplicity. Professionals in this field can take the following ethical progressive steps: B. Provide accurate information, avoid confusing approaches, and keep customers safe while protecting and leveraging data generated at the time of publication. Beyond identifying affiliations and building content when promoting influencers, it can also alert large audiences. Ensure that computerised citizenship ethics are practised in all workplaces by cultivating mindfulness, creating norms and regulations, spreading education and organising, and encouraging cautious and ethical behaviour in computerised settings. This includes compliance with legal rules. In this way, individuals and organizations contribute to a more positive, inclusive and trustworthy computerized society.

2. Method & Material

This paper begins with a comprehensive literature review based on the previous author, followed by an explanation of the topic we wish to explain. For this literature review, the authors use the ethics in social media and digital spaces as a case study.

2.1 Data Collection:

Specific keywords and phrases linked to ethics in social media and digital spaces steer the search. To discover relevant publications on ethics in social media and digital spaces, a thorough literature search was undertaken through academic databases, research repositories, and reliable sources. Keywords used in the search included "ethics," "social media," "digital spaces," "online platforms," "digital ethics," and variations thereof. The goal was to collect a diverse set of publications covering many areas of ethical considerations in the digital environment.

2.2 Data Analysis:

Data analysis entails reviewing, synthesising, and interpreting the acquired data in order to generate relevant insights and draw conclusions. The data analysis thoroughly analysing each article and finding crucial information that will be used in the ensuing study. Authors, publication year, research aims, methodology, theoretical frameworks, sample characteristics, findings, and ethical frameworks or theories used in each study may be included in the retrieved data. Proper documentation assures that pertinent information from each article is accurately collected and accessible during the analysis phase.

2.3 Limitations:

It is critical to understand the limitations of the tools employed for literature analysis. The quality and relevance of literature studied influence the conclusions, which may introduce biases. There is a risk of publication bias in selected publications, which means that studies with significant or positive findings are more likely to be published, whilst research with null or negative results may be underrepresented. Furthermore, the study is confined to previously published papers, and any gaps or constraints in the literature may affect the comprehensiveness of the conclusions.

3.0 Findings

3.1 Risk of being Unethical in Digital Spaces

According to Luciano Floridi in his article *"Translating Principles Into Practices of DIgital Ethics: Five Risks of Being Unethical"* (2019), typically a positive improvement shows mindfulness of the significance of the subject and intrigued in handling it methodically. Within the computerized space, which is deadly and filled with gigantic sums of data, it has to be a critical thing that clients have as their every day premise, taking after the different online stages, social media systems, E-commerce websites and advanced communication channels. With the quick development of innovation and the broad utilization of the web, moral thoughts in computerized spaces have picked up a colossal sum of significance. Falling flat to upright the moral benchmarks in computerized spaces seem to lead to numerous dangers and results. Some are deadly and dangerous to customers.

Maligning of notoriety may well be the unscrupulous conduct within the computerized space that spreads quickly and can harm somebody or an organization's notoriety. Therefore, different digital platforms have different types of critics.Along with content that criticizes journalism in the same room as journalists,news (David Cheruiyot, 2022). Data is spreading at an uncommon rate much appreciated by control of social media and online communities. Untrustworthiness, dispersal of deception, and cyberbullying can have enduring negative impacts on your individual or proficient picture.

Luciano Floridi's study from 2019 shows that the moral concern is that this agitation creates a "market of principles and values." The article states that private and public stakeholders should aim for redesign of their current behavior, rather than changing their behavior to comply with socially accepted ethical frameworks. Misconduct, such as misleading advertising, fraud and unethical business practices, can seriously undermine the trust that individuals and customers have in individuals and companies. After a solid reputation has been damaged, it can be hard to get it back, and people's bad impressions of you can last for a long time. Similarly, spreading misinformation or participating in cyberbullying can have serious reputational consequences. False or misleading information can spread rapidly, and individuals and organizations involved in spreading such misinformation can lose credibility and credibility. This can lead to negative public perception, reduced user engagement, and potential loss of customers and opportunities.

Greenwashing is when a private or public player tries to look greener, more sustainable, or more environmentally friendly than it really is (Delmas and Burbano, 2011). This can be explained by the legal implications of various laws that apply to the digital space, such as copyright law, data protection law, and cybercrime law. Violations of these laws such as copyright infringement, hacking, and online fraud can lead to lawsuits. , fines, and other penalties. Such unethical behavior online may result in legal action. In copyright infringement, the digital space is prone to copyright infringements such as unauthorized disclosure or distribution of copyrighted material such as text, images, videos, software; Copyright owners reserve the right to take legal action against individuals or organizations that infringe their intellectual property rights (Delmas and Burbano, 2011). Penalties for copyright infringement include hefty fines and, in some cases, even imprisonment. As privacy and data protection laws become more important, individuals and organizations must Comply with appropriate requirements, such as General Data Protection Regulation (GDPR) of the European Union.Unethical practices such as unauthorized data collection, misuse of personal information, and inadvertent data breaches can lead to serious legal consequences, including fines and legal action by data subjects and regulators.

Using social media for recruiting for studies that provide benefits can draw ineligible respondents who attempt to answer the qualifying inquiries 'right' in order to gain entry into the research and access the reward (Danielle Arigo, el. at. 2018). Unethical digital activity is typically followed by deceptive actions such as phishing scams, information theft, and online fraud to prevent internet fraud. Unethical digital activity is typically followed by deceptive actions such as phishing scams, information theft, and online fraud to prevent internet fraud. These actions are illegal and may result in criminal prosecution, fines and imprisonment depending on the severity of the fraud committed. Online fraud includes various deceptive acts carried out in the digital space for the purpose of defrauding individuals or organizations for personal gain.

A phishing attack is a fraudulent practice in which online criminals impersonate trusted individuals to obtain sensitive information such as passwords, credit card information, and login credentials (Avisha Das, et. al., 2019) . They often send fraudulent emails and create fake websites that mimic legitimate organizations and financial institutions. Unwittingly falling for these scams and divulging your personal information can leave you a victim of identity theft and financial fraud. Online criminals use stolen personal information to make fraudulent transactions, open fraudulent accounts, or carry out other illegal activities that seriously damage the victim's finances and reputation.

3.2 Cyberbullying and Online Harassment

In the enormous world of social media and digital spaces, a dark and troubling phenomenon has emerged: cyberbullying and online harassment. The internet has become fertile ground for the perpetration of harm and the violation of ethical norms as a result of the rapid growth and widespread use of social media platforms. As people increasingly connect, communicate, and express themselves through digital media, it is more important than ever to address the ethical implications of cyberbullying and online harassment.

Cyberbullying is defined as "wilful and repeated harm inflicted through the medium of electronic text" (Patchin & Hinduja, 2006, p.152).Cyberbullying can occur in chat rooms, on personal websites, on social networking sites, on Internet bulletin boards, and in other web-based venues. Cyberbullying can take place via email, chat rooms over the Internet, and texts on mobile phones. Although traditional bullying behaviours (such as insults, spreading speculation or slanders, and making risks) frequently occur on the internet instead of in person, online harassment can also include Internet-specific behaviours that have no counterpart in traditional bullying. For instance, a victim of cyberbullying may be asked to "like" or "share" a post on a social networking website. On the other hand, online harassment refers to a broader range of harmful behaviours that occur in digital domains. Targeted harassment campaigns, hate speech, stalking, and the creation of phony profiles or accounts to deceive and manipulate people are all examples. Because of the anonymity and supposed distance given by the internet, abusers are often emboldened, making online harassment a prevalent issue affecting people from all areas of life.

Wolak, Finkelhor, Mitchell, and Ybarra (2007) and Ybarra and Mitchell (2004) found that the majority of young people who were harassed online or by phone either did not feel bothered or were able to block the person who was harassing them. The fact that these instances were so simple to end lends credence to the hypothesis that online harassment does not necessarily include power disparity in which victims have a tough time protecting against attackers . It also considers other characteristics to distinguish between bullying and harassment, such as the number of episodes and the level of discomfort indicated by the victim.

In the research that has been done on traditional bullying, it has been shown that there are challenges associated with employing the global key questions on bullying, whether received or perpetrated, are as follows. These challenges include age and disparities in cultural background. Studies that looked at cultural and linguistic differences (Smith, Cowie, Olafsson, and Liefooghe, 2002; Smorti, Menesini, and Smith, 2003) discovered differences in the semantic area of terms for 'bullying' and how close such terms are to their western scientific definition. The studies were conducted in 2002 and 2003 respectively.

The ethical implications of cyberbullying and online harassment become readily apparent when one takes into account the potential damage that can be done on victims and the responsibilities that social media platforms and digital spaces have to provide environments that are secure and welcoming to all social media users. These harmful behaviours have repercussions that extend beyond the immediate victims, causing harm to their mental health, their sense of self-worth, and their quality of life in general. The proliferation of hate speech and abusive behaviour undermines the standards of empathy, respect, and equality that are the foundation of a healthy digital society, which means that the ethical repercussions extend to the greater community. Therefore, when it comes to conventional bullying, there are challenges associated with depending solely on a worldwide definition and on global questions concerning this behaviour. In light of the methodological challenges that are present in the field of traditional bullying, we need to make further efforts to improve the ways in which we measure cyberbullying.

Cyberbullying and online harassment in social media and other digital places are urgent moral issues that need to be looked at and dealt with right away. (Hinduja & Patchin, 2018). The fact that these problems hurt the victims' health and violate values like respect, empathy, and human decency shows how important it is to solve them. So far, most of the scientific studies that have been done to figure out how to spot cyberbullying have focused on the content of the text that users write, not the information about users. Social media platforms and online communities have a moral obligation to create safe and welcoming spaces for their users by putting in place strong policies and tools to avoid cyberbullying and online harassment. Also, education, awareness campaigns, and building digital resilience are important ways to give people the tools they need to spot and stop abusive behaviour. Laws and regulatory frameworks are key to holding abusers accountable (Kowalski et al., 2014; Schneider et al., 2018). Working together to encourage ethical behaviour online can lessen the damage done by cyberbullying and online abuse and make the internet more caring and responsible place.

3.3 Data Misuse and Exploitation

Social media platforms and other digital environments amass vast amounts of user data that may be utilised for targeted advertising, market research, and political influence. When user information is used improperly, sold without authorization, or used to influence people's beliefs and behaviours, ethical issues are raised. Protecting user privacy and ensuring transparent data practices are crucial to addressing these concerns.

Data theft in the used goods sector. The private and personal data on the smartphone can only be substantially eliminated by uninstalling apps or performing a factory reset (Zhu et al., 2015). This makes smartphone data recovery easy. A lot of personal data is stored on modern cell phones, including login passwords, browser history, contacts, texts, images, videos, and even financial data. By erasing user-installed software and data, a factory reset often returns the device to its default configuration. As some leftover data may still be present on the device's storage, it might not necessarily be possible to completely delete all traces of personal data. Data recovery is useful to forensic investigators when they are looking into crimes like cyberbullying, racism, blasphemy, car theft, accidents, and so forth. But as more people purchase used electronic devices, the threat of privacy breaches through the extraction of sensitive data increases. This leaves an information gap regarding the scope of social media data breaches on used devices. Privacy violations, identity theft, and user profiling on social networks could come from the retrieval of any sensitive and private information from a smartphone that corresponds to the social media application used by the initial owner. Additionally, it can expose the owner's personal and private communications with other social network users.

There will undoubtedly be an expansion of cybercrime into new scenarios as time goes by (Greenberg, 2017). Which technologies will be targeted and used for illegal purposes is one angle on this. Experience has already demonstrated that cybercriminals quickly adopt new technologies as new entry points, with attacks specifically designed for mobile devices serving as a prime example. New opportunities are undoubtedly available through the Internet of Things (IoT), smart homes, and driverless vehicles as technology develops. Indeed, in late 2016, the Mirai botnet used vulnerable IoT devices to launch a widespread denial of service attack, providing early evidence of exploitation. Greenberg's research was carried out in 2017, and the topic of cybersecurity is still evolving quickly. Although it is legitimate to be concerned about how cybercrime is spreading into new situations, countermeasures have also improved over time. To handle new threats, security experts, academics, and policymakers are constantly advancing legislation, creating stronger defence systems, and raising public understanding of cybersecurity issues.

Privacy is a fundamental topic in technology ethics (Zwitter, 2014). As networks and cloud computing have been widely adopted, data storage on centralised platforms has evolved into industry standard.Both cloud service providers and consumers must implement the proper security precautions and privacy safeguards in order to handle these privacy issues. Implementing encryption methods, access restrictions, and data anonymization procedures are all part of this. Before sending their data to these platforms, businesses and people must be informed of the privacy rules and practices of cloud service providers and carefully weigh the ramifications. Privacy issues arise in light of potential data abuse for the benefit of those with unauthorized access to the data.The security of the raw data determines user privacy, making it crucial to the blockchain technology stack. Significant, all-encompassing privacy issues include What information should one share with others in order to engage in exchanges? What details ought to be kept private and solely visible to the individual? What are the ideal circumstances and procedures for data sharing? Understanding how the blockchain technology stack might handle these issues is therefore vital.

4. Discussion

Based on this result, there is much to be discussed. As these platforms evolve and shape our society, it becomes increasingly important to address the ethical challenges they pose. This discussion examines ethical considerations related the digital space, highlighting the responsibilities of users, platform providers, and society at large.

The presented results show that compliance with ethical standards is of great importance in the digital space. With the growing number of online platforms, networking sites, websites for e-commerce, and electronic means of communication, the digital world has had a significant influence on our everyday lives (Delmas and Burbano, 2011). However, the field is not without risks and consequences if ethical standards are violated. In today's connected world, information travels quickly thanks to the power of social media and online communities. Dishonest behavior, the spread of misinformation, and Cyberbullying may have serious consequences.Personal and professional personalisation has long-term consequences. As the speed of information transmission increases, the risk of damage increases. Therefore, it is important to act ethically online. Additionally, a study (2019) conducted by Luciano Floridi highlights the rise of *"guidelines and value propositions"* in progressive fields. The wonder is that private and open partners seek to rethink their morals to justify their current behavior rather than correcting their practices based on socially accepted ethical frameworks. Malicious behaviors such as theft, extortion, and unethical deal tightening may substantially harm the acceptability of individuals and firms.

The expanded space also features real recommendations. Special laws that consider copyright law, security law, and cybercrime law govern online works. Violation of these laws, including piracy, hacking, and online extortion, can result in bills, hefty fines, and, most certainly, imprisonment. Examples of copyright infringement include unauthorized disclosure or transmission of copyrighted text, and copyright owners have the right to pursue legal action against those who infringe their intellectual property rights. To do. Online extortion poses another fundamental danger to the computerized space. Fraud such as phishing scams, identity theft, and online extortion are overwhelming and illegal. These acts indicate that an individual or organization is being exploited for personal reasons. Failure to comply with ethical measures in this area can have multiple threats and consequences, many of which can be disastrous and arguably dangerous to our customers.

Second, the discussion gives a clear evaluation of the ethical ramifications of cyberbullying and online harassment in the context of media platforms and digital spaces ethics. The study article is based on linked publications from prior studies, which provide insights into the ethical dimensions of these detrimental behaviors (Danielle Arigo, el. at. 2018). Balancing freedom of expression with the avoidance of harm caused by cyberbullying and online harassment is an ethical challenge. While free expression is vital, it should not be used to justify bad behavior. Ethical frameworks can help guide the creation of laws and guidelines that achieve a balance between ensuring responsible expression and safeguarding individuals from harm. It may be the online version of changing one's routine, a method commonly employed to reduce the threat of being aimed or harassed offline (Karmen, 2007).

The articles emphasize the pervasiveness of cyberbullying and online harassment on social media and in digital settings. The ethical issues stem from harm done to the well-being of people and the violation of their rights. Cyberbullying and online harassment are in direct conflict with ethical concepts including respect, dignity, and justice. Bullying can also take several forms, including verbal, physical, and relational (Liu & Graves, 2011). These actions violate people's rights to privacy, safety, and a supportive digital environment. The ethical issues revolve around adhering to these ideals and providing a welcoming and respectful online environment. Cyberbullying and online harassment must be addressed ethically by social media platforms and digital service providers. The fact that cyberbullying can be done anonymously adds to its menacing nature (Dooley et al., 2009; Mishna, Saini, & Solomon, 2009). They must create and implement rules that prohibit and minimize these detrimental behaviours. Users have an ethical responsibility to promote appropriate digital behaviour and develop an online culture of respect and empathy.

Legal and regulatory measures are required to successfully combat cyberbullying and internet abuse. The papers emphasize the significance of explicit definitions of certain behaviours in the legal system, as well as adequate penalties for violators. To avoid unforeseen outcomes that may infringe on free expression or worsen monitoring practices, laws should be developed with ethical considerations in mind. Cyberbullying typically occurs in a medium where parents are rarely present, within the unseen realm of adolescent online interactions (Mason, 2008). Collaboration among researchers from other disciplines can provide a thorough grasp of the ethical concerns and help to inform the development of effective preventive and intervention techniques. Balancing freedom of expression with the protection of harm necessitates careful thought. Future study and collaboration can help to better understand and address the ethical issues raised by cyberbullying and online harassment.

Third, the goal of the study was to assess the occurrence of communications with a spiritual inspiration in the digital social sphere in order to comprehend how these messages are received, how they are interpreted, how people interact with them, and how these factors interact with one another. Different types of process participation were established, and it was demonstrated that consumer interpretations were related to participant roles. While decoded interpretations of these inspiring messages differed, a prevalent perception was spiritual motivation, which was revealed when researchers examined how people deciphered posted inspirational words that appeared in their news streams on Facebook. By Hartmann et al. (2015), a "direct consumptive moment" is described as when someone uses assistance to address a challenge or advance personally. It is obvious that an issue will resonate and create favorable sensations that lead to a higher agreement with the message than at another time when a social media user is "in an optimal frame of thought" and receptive. However, it was beneficial to the recipients' daily lives and mirrored the overall spiritual or religious guidance related to life advice.

Investigates the moral implications of data exploitation in academia and research (Davis, 2021). The article explores the potential for skewed or unethical research methods, like the unapproved use of people's data for studies without their knowledge or consent. Other examples include manipulating data to promote predetermined results. To combat data exploitation, the author promotes ethical and open research practises. The complexity and quick evolution of data exploitation make it difficult to regulate (Johnson, 2019). The author emphasizes the necessity for extensive legal frameworks and moral standards to safeguard people and guarantee organizations use data responsibly. In order to address data exploitation, it is critical to strike a balance between innovation and privacy.

According to (Anderson, 2017), who also highlights the ease with which people's private information can be accessed, edited, or used without their knowledge or consent, the ethical repercussions of data misuse are highlighted. In the digital era, the author explores the possibility of identity theft, unauthorised profiling, and the erosion of privacy rights. Misuse of data poses issues with people's autonomy, trust, and the balance of power between data collectors and users.In a variety of fields, such as business practises, cybersecurity, and research, data exploitation raises serious ethical issues and has societal repercussions. The possible concerns of data misuse, such as privacy violation, unauthorised profiling, and biassed results, must be understood and addressed. In order to avoid and mitigate data misuse, it is crucial to take ethical considerations, informed consent, transparency, and strong security measures into account.

5. CONCLUSION

In conclusion, in order to implement social justice, Social professionals must aid citizens in understanding ethics and realizing their civic responsibilities (Dominelli, 2014). How do they apply to online debates that affect people's well-being, their right to be free from abuse and violence, and their potential for work in the present or the future, and that have effects that go well beyond their existence in ethereal space? We contend that this issue should be taken up by national and international peer groups for social work because it transcends the purview of any one profession and calls for the development of comprehensive social work regulations for correspondence via the Internet. These guidelines should cover how to challenge commonly held beliefs and conduct oneself as an incredibly observant practitioner via the web.

Additionally, the defined affordances depend on the study's particular chronology and the continual evolution of what we refer to as digital spaces. While multi-sensoriality, for example, cannot yet be realised in the digital sphere, the safety that these spaces can provide and their potential to resurrect and replicate ethical consumption settings are both continually changing. In fact, initial designs of digital environments that allow for more multi-sensory experiences are progressively becoming a reality (Covaci et al. 2018).

By engaging in such behavior, social realities are created that change the demands and opportunities for contextual psychology. Because of this, we view online behavior as both a sign and a manifestation of communal selfhood. Important aspects of these processes may be captured by models and theories that focus primarily on the individual level of analysis or that primarily address single-directional losses. They lack the ability to adequately define their dynamic and cyclical character. Understanding online behavior is thus a transdisciplinary problem that will involve the fusion of many approaches and points of view (Adrian Luders et al., 2022).

Additionally, using ICT can help you carve out time for yourself, take a break from working through your emotions, and manage the difficulties of family life and spousal caregiving. It may be said that the message being sent is that one must take care of in order to preserve a sense of. To put it another way, and building on earlier research on ICT, senior citizens, and caring interactions (Magnusson et al., 2005; Blusi et al., 2013), ICT is seen as having the ability to help participants concurrently increase their sense of personal autonomy.

Acknowledgments: Without the financial assistance of Unit Kw3p, Uitm Machang, Cawangan Kelantan, this work would not have been feasible. We are especially grateful to Sir Mohamad Syauqi Mohamad Ariffin, who has always been supportive of our ambitions and has always provided us with direction in order for us to complete this piece. We extend our gratitude to everyone we had the opportunity the honour of working with on this as well as other related initiatives. Each member has offered considerable personal and professional assistance, as well as teaching each other a great lot about scientific research and everyday life in general. Nobody has ever been more essential to the success of the achievement of this mission than our family members. We'd want to thank those who raised us for their love and advice in anything we do. They are the ideal role models.

References

Arigo, D., Pagoto, S. L., Carter-Harris, L., Lillie, S. E., & Nebeker, C. (2018b). Using social media for health research: Methodological and ethical considerations for recruitment and intervention delivery. *Digital Health*, *4*, 205520761877175. https://doi.org/10.1177/2055207618771757

Cheruiyot, D. (2022). Comparing Risks to Journalism: Media Criticism in the Digital Hate. *Digital Journalism*, 1–20. https://doi.org/10.1080/21670811.2022.2030243

Dadvar, M., & De Jong, F. (2012). *Cyberbullying detection*. https://doi.org/10.1145/2187980.2187995

D'Arcy, A., & Young, T. (2012). Ethics and social media: Implications for sociolinguistics in the networked public[1]. *Journal of Sociolinguistics*, *16*(4), 532–546. https://doi.org/10.1111/j.1467-9841.2012.00543.x

Digital Citizenship with social media on JSTOR. (n.d.-b). https://www.jstor.org/stable/26273880

Towards an adaptive ethics on social networking sites (SNS): a cr. . .: Ingenta Connect. *www.ingentaconnect.com*. https://doi.org/10.1108/JICES-05-2021-0046

Finefter-Rosenbluh, I., & Perrotta, C. (2022). How do teachers enact assessment policies as they navigate critical ethical incidents in digital spaces? *British Journal of Sociology of Education*, *44*(2), 220–238. https://doi.org/10.1080/01425692.2022.2145934

Floridi, L. (2021b). Translating Principles into Practices of Digital Ethics: Five Risks of Being Unethical. In *Philosophical studies series* (pp. 81–90). Springer International Publishing. https://doi.org/10.1007/978-3-030-81907-1_6

Kaitatzi-Whitlock, S. (2021). *Toward a digital civil society: digital ethics through communication education*. https://philpapers.org/rec/KAITAD-5

Lenhart, A. (2007, July 4). *Cyberbullying and online teens*. https://apo.org.au/node/16745

Macnamara, J., & Zerfass, A. (2012). Social Media Communication in Organizations: The Challenges of Balancing Openness, Strategy, and Management. *International Journal of Strategic Communication*, *6*(4), 287–308. https://doi.org/10.1080/1553118x.2012.711402

Menesini, E., & Nocentini, A. (2009). Cyberbullying Definition and Measurement. *Zeitschrift Für Psychologie Mit Zeitschrift Für Angewandte Psychologie*, *217*(4), 230–232. https://doi.org/10.1027/0044-3409.217.4.230

Olweus, D., & Limber, S. P. (2018). Some problems with cyberbullying research. *Current Opinion in Psychology*, *19*, 139–143. https://doi.org/10.1016/j.copsyc.2017.04.012

Saurabh, K. (2022). *AI led ethical digital transformation: framework, research and managerial implications*. https://philpapers.org/rec/SAUALE

Schivinski, B., & Dabrowski, D. (2016). The effect of social media communication on consumer perceptions of brands. *Journal of Marketing Communications*, *22*(2), 189–214. https://doi.org/10.1080/13527266.2013.871323

Sengupta, A., & Chaudhuri, A. (2011). Are social networking sites a source of online harassment for teens? Evidence from survey data. *Children and Youth Services Review*, *33*(2), 284–290. https://doi.org/10.1016/j.childyouth.2010.09.011

SoK: A Comprehensive Reexamination of Phishing Research From the Security Perspective. (2020, January 1). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/892466

The Ethics of Digital Writing Research: A Rhetorical Approach on JSTOR. (n.d.). https://www.jstor.org/stable/20457031

Theoretical Dimensions and Introduction to the Symposium on JSTOR. (n.d.-c). https://www.jstor.org/stable/41427128

Toffoletti, K., Olive, R., Thorpe, H., & Pavlidis, A. (2021b). Doing feminist physical cultural research in digital spaces: reflections, learnings and ways forward. *Qualitative Research in Sport, Exercise and Health*, *13*(1), 11–25. https://doi.org/10.1080/2159676x.2020.1836513

Toledano, M., & Avidar, R. (2016). Public relations, ethics, and social media: A cross-national study of PR practitioners. *Public Relations Review*, *42*(1), 161–169. https://doi.org/10.1016/j.pubrev.2015.11.012

Williams, J., & Krisjanous, J. (2023). Spreading the word: exploring spiritual consumption on social media. *Journal of Consumer Marketing*, *40*(1), 124–135. https://doi.org/10.1108/jcm-02-2021-4450

Research Article

Factors Influence Social Media Crime Among Young Generations

Amirah Batrisyia Mohamad[1], Nur Athirah Zulriadi[2], Nur Malihah Zailani[3], and Meer Zhar Farouk Amir Razli[4, *]

[1] Universiti Teknologi MARA; 2020846546@student.uitm.edu.my; 0009-0000-3300-0312

[2] Universiti Teknologi MARA; 2020495442@student.uitm.edu.my; 0009-0007-5510-0665

[3] Universiti Teknologi MARA; 2020813178@student.uitm.edu.my; 0009-0007-8828-2020

[4] Universiti Teknologi MARA; farouk955@uitm.edu.my; 0009-0008-8849-336X

[*] Correspondence: farouk955@uitm.edu.my; 019-9846868.

Abstract: *Social media crime has received the greatest attention and has become a hot topic that is constantly rising as children, tweens, and teens use and accessibility of Internet networks has increased, exposing them to numerous types of social media crime. Therefore, this research paper aims to summarize, analyze, and disclose the findings and factors which influence awareness of social media crime among the young generation to protect their future as well as the country. A structured literature methodology was implemented to analyze and explore 22 previous studies from the UiTM EzAccess online database that are relevant to the aspects that affect social media crime among young generations while conducting this research article. The crucial analysis of the literature reveals that several aspects influence social media crime among young generations, including the type of social media crime, the factors, the impact, and the strategy of social media to influence the young generation. This research is one of several that provide a comprehensive review of the literature on the rising issue of factors that influence social media crime in the context of the young generation. Thus, in this structured literature analysis, further awareness in combating social media crime among the younger generations can be identified.*

Keywords: factors influence; social media; crime; young generations; literature review.

DOI: 10.5281/zenodo.8181042

1. INTRODUCTION

According to the Cambridge Dictionary, social media is a website, computer program, and kind of media that allows people to interact and exchange information via computers or smartphones over the Internet. In a nutshell, social media is the largest and most advanced digital medium that allows individuals and organizations to create, share, and exchange any kind of text, or multimedia such as images, videos, or voice recordings, as well as communicate with other users via voice calls or video calls over existing Internet networks and virtual communities. Nowadays, social media encompasses many forms, including messaging applications, social networks, blogs, forums, and more. It is well known that the most popular social media sites users frequently use include WhatsApp, Instagram, Facebook, YouTube, and so forth. This fundamental social media function normally features and distributes all material provided by users, as well as personalized profiles representing those people, allowing users to participate in standard social media activities such as sharing, likes, reviews, and discussions. People join social media sites to interact and communicate with others, to share their thoughts, experiences, or good things, to learn new things like tips and tutorials, and to stay updated with the newest hot news and market trends.

Smartphones and the Internet may be highly beneficial tools for the growth of teenagers, allowing them to stay in contact with family and friends while also providing numerous learning possibilities (Álvarez-García et al., 2019). Children, tweens, teens, adults, and the elderly are all among today's social media users. One in every three Internet users worldwide is a child or teenager under the age of 18 (UNICEF, 2017). Although social media is widely seen to provide several benefits in numerous aspects of life, keep in mind that nothing is perfect in today's world since anything that has advantages also has disadvantages. According to the Mayo Foundation for Medical Education and Research (MFMER), youngsters can be severely impacted by social media use, which can distract them, interrupt their sleep, and expose them to bullying, rumor spreading, inaccurate views of other people's lives, and peer pressure. Tweens (ages 8 to 12) increased their daily screen time to five hours and 33 minutes, up from four hours and 44 minutes, while teenagers (ages 13 to 18) increased their daily screen time to eight hours and 39 minutes, up from seven hours and 22 minutes (Moyer, 2022). Therefore, a situation like this might expose the younger generation to various forms of social media criminality. With more screen time for the younger population, there will be more involvement in social media crimes such as bullying, harassment, stalking, stealing information and accounts, and receiving threats online. Without solutions as well as awareness from themselves, parents, social media management, or the government, there is no hesitation that this issue will become more prominent in the future.

2. METHOD & MATERIAL

The literature review approach in the present research. Due to the prior study's use as a reference, such research methodology is employed to ensure of research technique is employed to make sure the author can carefully complete this research article. The research's materials include publications that were analyzed from a variety of sources and databases, including Academics Journal, Societies, International Journal, IEEE Explore, Emerald Insight, ProQuest, and Google Scholar. Previous research has demonstrated that social media exposure has a major impact on the public's view of crime, particularly among young individuals (Trninić et al., 2021).

3. LITERATURE REVIEW

The Economic Times (2023) has defined the term 'social media' as websites and programs that help people talk to each other, get involved, share information, and work together. Merriam-Webster dictionary also defined 'social media' as a form of electronic communication such as websites for social networking and microblogging through which users create online communities to share information, ideas, personal messages, and other contents, meanwhile the term 'crime' has been defined as an illegal act for which someone can be punished by the government. Macmillan Dictionary has defined 'young generations' as the youngest adults in society.

The peak of social media crime started during the pandemic of Coronavirus where it started normalizing people using the technologies as their norms. It shows that during Covid-19, parents' religious behaviors lead to teenagers' behavior on the Internet, especially towards cybercrime (Li, Li, Fang & Wang, 2021). In most developing countries, many of them are not concerned about the policy literature regarding social media which leads to crime existence (Asongu, Nwachukwu, Orim & Pyke, 2019). Most problematic teenagers are using multiple public and private social media platforms such as Facebook, Snapchat, Twitter, and YouTube as early signs of fear of missing out (FOMO) and phubbing behavior which slowly leads to cybercrime (Apoorva, Chaudhuri, Hussain, & Chatterjee, 2022). The openness behavior on social media including revealing private information brings an effect on cognitive behavior which brings risks to security and visibility and exposure to fraud (Murthy and Gopalkrishnan, 2022). Insufficient information and lack of knowledge among teenagers due to cultural poverty leads to social damage leads to a social emergency. Comparison between peers, media illiterate among parents, and less social skills will lead to crime in social media among children (Amini & Pashootanizadeh, 2019).

Moreover, teenagers' habit of video sharing on social media negatively impacts privacy limitations and allows access to personal information retrieval (Kang, Shiu & Hwang 2021). The behavioral intention toward cybercrime among students is mainly due to attitude, social norms, perceived behavioral control, excessive usage of social media, fewer parenting controls, and lack of regulations and knowledge (Alotaibi, 2019). Other than that, it is found that teenagers who experience psychosocial distress during their childhood may be likely to develop abnormalities in online social interaction as they see online violence as less threatening and more rewarding, compared to other types of interactions (Al-Samarraie, Bello, Alzahrani, Smith, & Emele, 2021). In addition, the modern criminal is targeting young users who have influence or have a high number of followers since most of them are less concerned about security and privacy (Cengiz, Kalem & Boluk, 2022). Therefore, it is found that teenagers that have a high privacy self-efficacy behavior tend to have a greater concern about online privacy compared to others. Self-efficacy helps the user to gain more general respect and ethics towards the technology's regulations. (Baker-Eveleth & Stone, 2021).

Not only that, but social media crime also can turn into sexual harassment as the exposure to dating apps to minimize, legitimize and excuse sexual harm are the core factors towards sexual harassment (Cama, 2021). The development of the web and technology also leads to minor exploitation where cyber libertarians or Internet hackers have brutally breached human rights which leads to serious child protection-related crime (Salter & Hanson, 2021). The interactions of teenagers through technology may involve sexism and racism which affect young people's being, becoming, and belonging to future identities (H€allgren & Bj€ork, 2022). It has also been found that most social media crime in youth the ones who have less relationship bonding between family members, and they have a higher exposure towards social media crime (Nalaka & Diunugala, 2020). Social media crime turns out more critical when it involves nonsensual circulated media which leads to traumas, especially for female teenagers (Gjika, 2020).

Social Media Disorders are one of the long-term impacts on the victims if they are experiencing a significant negative impact relating to social media crime (Norwood, 2022). Social media nowadays also normalizes hashtags some of them publicly posting photos and media of minors and teenagers. As it is simply seen as safe, it is encouraging criminals for cybercrime activities such as illegal editing, fake accounts, and digital kidnapping (Bare, 2020).

4. FINDINGS

There are a variety of factors that influence social media crime among the young generation that has been obtained by reading and study from several papers collected from various online databases. The overview of social media crime, factors contributing to social media crime among the young generation, impacts of social media crime on young generations, and the strategy of social media for young generations from diverse parties on social media are covered in these research findings.

4.1 Overview of social media crime

Khoury, G. (2019) has concluded online threats, stalks, cyberbullying, hacking and fraud, illegal purchasing, vacation robberies, and fake online friendships as examples of social media crime. Harness, J. (2023) also stated that some common types of social media are bullying, false impersonation, stalking, hacking, phishing and fraud, sex crimes, illegal business, vacation robberies, illegal media sharing, and getting caught in social media. As reported by the India National Crime Reporting Bureau, statistics on crime cases on social media show that it has elevated by 43% in 2018, from 27,248 cases to 44,546 cases in 2019 (Agrawal, S., 2021).

A study conducted by a research agency in Europe has found that YouTube, Instagram, WhatsApp, TikTok, and Snapchat are the most common social media downloaded by teenagers and it is found that approximately most teenagers spend 4 to 7 hours a day on phone (Milmo, D., 2022). A survey conducted for 40,000 respondents worldwide by RR Author (2022) justified that 68.44% of teenagers agreed that they are more engaged in social media than any other age group, 37% agreed that Facebook is the most popular social media platform and 39.5% agreed that an average of teenagers will have more than 5 social accounts each. Moyer, M. W. (2022) explained based on a survey published by Common-Sense Media, a non-profit research organization, in the year 2021 has shown an increment of 17% from 2019 the cumulative screen time among teens and tweens and the increment is still growing for the next four years. On average, the tweens had spent 5 hours and 33 minutes daily and teens had spent 7 hours and 22 minutes daily.

4.2 Factors contributing to social media crime among the young generation

The younger generation, tweens, and teenagers are active users of social media nowadays. Today's youngsters spend a lot of time on social media rather than on productive activities (Rani & Padmalosani, 2019). In simple words, they are the direct product of the world of digitization at this point. Among the factors of social media crime towards the young generation is the anonymity of the Internet, lack of validation of social media content, and lack of parental control. These social media crimes range from cyberbullying, online fraud, online harassment, identity theft, and so forth.

All these crimes are often caused by the anonymity of the Internet which makes the social media users act without fear of what the consequences will be. The unrestricted expansion of anonymous identities, on the other hand, has weaponized the Internet, transforming it into a real orgy of hatred, violence, vitriol, and intimidation (Tewari, 2022). This factor is extremely serious since anonymity encourages anti-social behavior, and the use of fake names, fake identification (ID), and unverified user accounts allow people to disguise their identity when they post inappropriate messages and comments. In addition, the validation of social media content, most of which are established companies handling social media are constantly struggling to constantly monitor activities, censor content and remove such harmful content by use of users of different ages. Next is the lack of parental control over children’s social media use. Nevertheless, things posted to social media that are deemed unsuitable or constitute a risk to users must be checked and deleted, even if this takes time. Live-stream footage of mass shootings and viral social media "challenges" that inspire young people to commit risky acts like holding their breath until they pass out are examples of content that might be restricted under the new rules (Kurohi & Low, 2022). Dorasamy et al. (2021) also highlighted the need for parental involvement in children’s Internet safety. Parents are unable to spend time with their children since they are preoccupied with their daily responsibilities. Social Internet allows youngsters of today to escape boredom (Rani & Padmalosani, 2019). Therefore, parents may not be aware of the harmful risks associated with social media and their children’s social media monitoring activities are not carried out. Nevertheless, parental control, however limited and indirect, has a protective impact against cyber victimization (Álvarez-García et al., 2019).

Thus, it can be seen that all of these factors not only contribute to the exposure of children and adolescents to online predators but also indirectly engage them with other types of social media crimes. According to Rashidah Abdul Rahman & Normah Omar (2015) as well, educating young people about cybercrime will assist to raise awareness and perceptions of cybercrime.

4.3 Impact of social media crime on young generations

Social media crime toward teenagers has shown several negative impacts. Unethical use of social media will lead to youth crime. Online crime in young generations such as stalking and intimate partner violence, human trafficking, online pornography, minor abuse imagery, and online hate and harassment are targeting female teenagers as their victims (Bailey and Shayan, 2021).

For the long-term effect, these victims will suffer from mental illnesses such as depression and social anxiety. Normally these patients are scared to seek for help, and it is suggested to develop a new approach to improve their help-seeking behaviors (Goodwin and Behan, 2023). RR Author (2022) claims that the youth tend to suffer from poor mental conditions, resulting in fewer physical activities and interactions with people. Social media crime affects the teen's emotional, mental, and physical health as they can suffer from FOMO (fear of missing out) problems, depression, and anxiety also includes intentional physical harm towards the victim, (Agrawal, S., 2021). Glazzard, J. & Stones, S. (2019) summarize that social media bullying and body image concerns have a significant effect on mental health among young people. It brings negative development as it can influence anxiety, stress, and depression. Social media bully can also be in the form of humiliating messages and media which leads to embarrassment and confidence loss.

Social media crime also leads to violence in human rights and privacy rights. Human right is recognized by protecting one's dignity and privacy from abuse, discrimination, and potentially dangerous activities. Social media infringement such as stalking and illegal monitoring will against the human rights of teenagers (Coombs, 2021). Privacy rights cases can relate to identity theft and cyberstalking. The perpetrator may have collected the identifiable information with improper use for their purpose. The perpetrator also acts in the form of stalking the victim's social media which produces discomfort or abuse (Thukral, P. & Kainya, V., 2022). Identity theft is also threatening in social networking as it can utilize a person's person personal data illegally such as mobile numbers and addresses to demand confidential information. Profile cloning attack is one of the new crimes that exist as the assaulter creates a cloned social media profile to build trust and connections to attack silently through cyberstalking and blackmailing (Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021).

4.4 The strategy of social media for young generations

The use of social media to draw young people's attention is known as a social media strategy for the younger generation. The social media algorithm, advertisements, and the demands of young people on social media are three of them.

A social media algorithm is a system of guidelines and cues that automatically classifies content on a social network by the likelihood that each particular social media user would engage and enjoy it (Newberry, 2022). The content that news readers are exposed to more frequently is stuff that has been chosen using an algorithm. in particular, the younger generations, who depend on social media websites like Facebook, YouTube, and Instagram for individualized news. 2019 (Kalogeropoulos). Therefore, algorithms are beginning to affect how young people learn about their environment more and more. However, little is known about how people see and engage with automated news selection. Numerous conceptual studies (e.g., Beer, 2017; Diakopoulos, 2015; Willson, 2017) have investigated how algorithms impact daily life, but these often adopt a technological approach to ascertain how algorithms wield power.

The social network, a cutting-edge new media, is currently helping marketers and consumers increase their communication. This is the most recent development in product advertising and customer outreach. Facebook is one of the social networking sites with the fastest growth. It takes a lot of spontaneous brainstorming among the network's participants for an opinion to emerge in the media (Akar & Topcu, 2011; Kim & Ko, 2012). In actuality, this complete social media platform has made it feasible for any brand to sell its goods through exposure, attention, and perception, as well as to create opinions and establish values (Kim & Ko, 2010).

Moreover, since social media is utilized for amusement and self-expression, young people who use it must employ this strategy. Furthermore, the platform may enlighten children about current events, facilitate cross-border dialogue, and transmit information on several issues, including healthy behaviors. Teenagers may also benefit from significant connections with peers and a big social network, as well as from hilarious or disturbing social media (Mayo, 2022).

5. DISCUSSION

First, studies on people's fear of crime were created and advanced by researchers. Due to its distinct features and the current growth in user numbers, social media was the researcher's primary platform of choice (Greenwood et al., 2016; Perrin, 2015). examined the impact of social media use on society’s perceptions of victimization and criminal fear. The findings imply that young individuals' total use of social media has a significant impact on how miserable they feel. This result backs up the claims made in the cultivation research.

The findings suggest that using social media more frequently may amplify the psychological and social factors that cause fear, which is consistent with earlier studies (Kross et al., 2013; Martin et al., 2012; O'Keeffe & Clarke-Pearson, 2011) that linked frequent social media use to negative effects like anxiety and social withdrawal. Fear of crime was not associated with any aspects of traditional or entertainment media, with the possible exception of watching national television news, which was only weakly associated. Despite the possibility that this contradicts earlier efforts, social media is eventually a more significant and effective media source (Callanan, 2012; Chiricos et al., 2000, 1997; Dowler, 2003; Eschholz et al., 2003; Jamieson & Romer, 2014; Kohm et al., 2012). This is true because it has a higher likelihood of being used by young people than mainstream media that focuses on amusement. A sample of college students who claimed to use social media more regularly than any other kind of conventional media on average serves as evidence of this.

Not only that, youth can share their writing, writing-related content, and other works via social media (Mesch, 2009; Shewmaker, 2012). This demonstrates how social media can simultaneously meet young people's demands for relationship development and provide them with a special chance to participate in the media actively (Mesch, 2009)

Furthermore, there are benefits to using social media, although it is not always all positive. Keeping in touch with friends and family is one of them. You can maintain contact with far-flung friends and family members by using social media. You can use social media to organize parties and get-togethers as well as to share pictures, videos, and updates about your life. Besides that, developing relationships can connect with people who share your interests through social media. You may interact with people you might not otherwise meet on social media by connecting with them in groups and communities. The next positive is acquiring new knowledge. Social networking may be a fantastic resource for knowledge and education. On several subjects, you can find articles, videos, and other resources.

Additionally, receiving support is another positive. Social networking may be a terrific resource for finding comfort through trying times. You can make connections with other individuals who have gone through similar things, and you can find tools and knowledge to make it through. And finally, doing good. An excellent method to give back to your community is through social media. You can donate your time to causes that matter to you, and you can utilize social media to spread the word about significant concerns. The use of social media, of course, also has certain drawbacks. It's critical to be informed of these dangers and to utilize social media responsibly and safely.

6. CONCLUSION

In modern days, social media is one of the essential things, especially for young generations as they can gain a lot of knowledge and information. Thukral, P. & Kainya, V. (2022) states that social networking sites help the young generations to keep updated with the information worldwide limitless and help them in term of educational purpose. Social networking also helps the young generations to express their thoughts and ideas to the world resulting in a convenient and pleasurable space in social media.

According to several studies, while young people are typically aware of the hazards of social media crime, they may not always be aware of the exact types of crimes that can occur or how to defend themselves. These findings show that young people need more education and knowledge regarding social media crime. Parents, schools, and social media corporations may all play a part in educating young people about the dangers of social media and how to protect themselves. There is some advice for parents and educators on how to talk to their children about cybercrime on social media. To begin, talk to your youngster about the various sorts of social media crimes that might occur. Make it clear that cyberbullying, online predators, and other forms of social media crime can have serious consequences in people’s life. After that, assist your child in developing safe Internet behaviors. This includes things like creating secure passwords, exercising caution when sharing information online, and not responding to messages from strangers. Next, encourage your youngster to alert a trusted adult to any unusual behavior. This could be a parent, teacher, counselor, or another trusted adult.

Acknowledgments: In the name of Allah, the Most Gracious and the Most Merciful. Alhamdulillah, first we would like to thank Allah, All praises to Allah and His blessing for the completion of this paper. We thank Allah for all the opportunities, trials, and strengths that have been showered on us. This task had been done through the efforts and cooperation of our team authors, Amirah Batrisyia Mohamad, Nur Athirah Zulriadi, and Nur Malihah Zailani even though we faced many challenges while accomplishing this paper. A thousand thanks are also expressed to the administration of UiTM Machang, Kelantan, for the monetary donation and all funding provided to the finances for the publication of this research article, as well as the fee required to participate in the Glocal Symposium on Information and Social Science (GSISS) program for the year 2023. Biggest thanks we address to the co-author, Mr. Meer Zhar Farouk Amir Razli for his guidance and advice to help us prepare and complete this paper. Besides, the biggest thanks we address to our lecturer, Madam Salliza Md Radzi due to her guidance and encouragement, our paper cannot be done successfully. She always gives support, guidance, and motivation in purpose to produce a good outcome. We are also grateful that we managed to complete this paper within the time given. Not forgotten, our deepest gratitude goes to all our peers, classmates, family members, and friends for trying their best to give their support by giving us a lot of supportive ideas, mental support, and understanding from the beginning until the end of this paper. It would not be possible to write this paper without the support from them. The need for their moral support, kindness, and prayers is real. Our heartfelt thanks.

References

Agrawal, S. (2021, September 27). Social media and crimes: An entangled relationship. *The Daily Guardian.* https://thedailyguardian.com/social-media-and-crimes-an-entangled-relationship/#:~:text=Fraud%20cases%20on%20social%20media,by%20National%20Crime%20Reporting%20Bureau.

Alotaibi, N. B. (2019). Cyberbullying and the expected consequences on the student's academic achievement. *IEEE Access,* 7, 153417–153431. https://doi.org/10.1109/access.2019.2947163

Al-Samarraie, H., Bello, K.-A., Alzahrani, A.I., Smith, A.P. and Emele, C. (2022), "Young users' social media addiction: causes, consequences and preventions". *Information Technology & People*, 35(7), 2314-2343. https://doi.org/10.1108/ITP-11-2020-0753

Álvarez-García, D., Núñez, J. C., González-Castro, P., Rodríguez, C., & Cerezo, R. (2019). The effect of parental control on cyber-victimization in adolescence: The mediating role of impulsivity and high-risk behaviors. *Frontiers in Psychology*, *10*. https://doi.org/10.3389/fpsyg.2019.01159

Amini, M., & Pashootanizadeh, M. (2019). Assessing the satisfaction of teenagers at risk and vulnerable to social damages of young adults' publications in Iran based on the CSI model. *Collection and Curation,* 38(1), 1–8. https://doi.org/10.1108/cc-03-2018-0003

Apoorva, A., Chaudhuri, R., Hussain, Z. and Chatterjee, S. (2022). Social media usage and its impact on users' mental health: A longitudinal study and inputs to policymakers. *International Journal of Law and Management*, 64(5), 441- 465. https://doi.org/10.1108/IJLMA-08-2022-0179

Asongu, S., Nwachukwu, J., Orim, S.-M., & Pyke, C. (2019). *Crime and social media. Information Technology & People,* 32(5), 1215–1233. https://doi.org/10.1108/itp-06-2018-0280

Bailey, J. and Shayan, S. (2021). The missing and murdered indigenous women crisis: Technological dimensions. *The Emerald International Handbook of Technology-Facilitated Violence and Abuse (Emerald Studies in Digital Crime, Technology, and Social Harms),* 125-144. https://doi.org/10.1108/978-1-83982-848-520211007

Baker-Eveleth, L., Stone, R. and Eveleth, D. (2022), "Understanding social media users' privacy-protection behaviors", *Information and Computer Security,* 30(3), 324-345. https://doi.org/10.1108/ICS-07-2021-0099

Bare, C. (2020). The undisclosed dangers of parental sharing on social media: A content analysis of sharing images on Instagram. *ProQuest Dissertations & Theses Global.* https://ezaccess.library.uitm.edu.my/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdissertations-theses%2Fundisclosed-dangers-parental-sharing-on-social%2Fdocview%2F2570139500%2Fse-2%3Faccountid%3D42518

Cama, E. (2021). Understanding experiences of sexual harm facilitated through dating and hook-up apps among women and girls. *The International Handbook of Technology-Facilitated Violence and Abuse*. 333-350. https://doi.org/10.1108/978-1-83982-848-520211025

Coombs, E. (2021). Human rights, privacy rights, and technology-facilitated violence. *The Emerald International Handbook of Technology-Facilitated Violence and Abuse (Emerald Studies in Digital Crime, Technology, and Social Harms),* 475-491. https://doi.org/10.1108/978-1-83982-848-520211036

Dorasamy, M., Kaliannan, M., Jambulingam, M., Iqbal Ramadhan, & Sivaji, A. S. (2021). Parents' awareness on online predators: Cyber grooming deterrence. *Qualitative Report*, *26*(11), 3685–3723. https://doi.org/10.46743/2160-3715/2021.4914

Friedman, L. (2014, April 22). *5 Benefits of Using Social Media*. Linkedin.com. https://www.linkedin.com/pulse/20140422162738-44670464-5-benefits-of-using-social-media

Gjika, A. (2020). Going viral: Youth and sexual assault in the digital age. *ProQuest Dissertations & Theses Global.* https://ezaccess.library.uitm.edu.my/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdissertations-theses%2Fgoing-viral-youth-sexual-assault-digital-age%2Fdocview%2F2419331884%2Fse-2%3Faccountid%3D42518

Glazzard, J. & Stones, S. (2019). *Technology and Child Mental Health.* ResearchGate. 335549577_Social_Media_and_Young_People's_Mental_Health

Goodwin, J. and Behan, L. (2023). Does media content have an impact on help-seeking behaviors for mental illness? A systematic review. *Mental Health Review Journal,* 126-144. https://doi.org/10.1108/MHRJ-06-2022-0038

H€allgren, C. & Bj€ork, A. (2022). Young people's identities in digital worlds. *The International Journal of Information and Learning Technology*, 40(1), 49-61. https://doi.org/10.1108/IJILT-06-2022-0135

Harness, J. & Liss, P. (2021, January 18). The most common crimes committed on social media. *Vista Criminal Law.* https://vistacriminallaw.com/common-social-media-crimes/

Intravia, J., Wolff, K. T., Paez, R., & Gibbs, B. R. (2017). Investigating the relationship between social media consumption and fear of crime: A partial analysis of mostly young adults. *Computers in Human Behavior*, *77*(77), 158–168. https://doi.org/10.1016/j.chb.2017.08.047

Kang, H., Shin, W. and Huang, J. (2022), "Teens' privacy management on video-sharing social media: the roles of perceived privacy risk and parental mediation". *Internet Research*, 32(1), 312-334. https://doi.org/10.1108/INTR-01-2021-0005

Kurohi, R., & Low, D. (2022, June 20). Social media platforms remove harmful content and add safeguards under S'pore's proposed rules. *The Straits Times*.

Li, Y., Li, J., Fan, Q. and Wang, Z. (2022), "Cybercrime's tendencies of the teenagers in the COVID-19 era: assessing the influence of mobile games, social networks and religious attitudes", *Kybernetes*, https://doi.org/10.1108/K-07-2021-0582

Macmillan Dictionary. (n.d.). The younger generation. In *Macmillan Dictionary.co*m. Retrieved June 10, 2023m from https://www.macmillandictionary.com/dictionary/british/the-younger-generation#:~:text=the%20youngest%20adults%20in%20a%20society.

Merriam-Webster. (n.d.). Crime. In the *Merriam-Webster.com dictionary.* Retrieved June 10, 2023, from https://www.merriam-webster.com/dictionary/crime

Merriam-Webster. (n.d.). Social media. In the *Merriam-Webster.com dictionary.* Retrieved June 10, 2023., from https://www.merriam-webster.com/dictionary/social%20media

Milmo, D. (2022, December 5). Risky behavior 'almost normalized' among young people, says study. *The Guardian.* https://www.theguardian.com/technology/2022/dec/05/risky-online-behaviour-almost-normalised-among-young-people-says-study

Moyer, M. W. (2022, March 24). Kids as young as 8 are using social media more than ever, a study finds. *The New York Times.* https://www.nytimes.com/2022/03/24/well/family/child-social-media-use.html

Moyer, M. W. (2022, March 24). Kids as Young as 8 Are Using Social Media More Than Ever, Study Finds. *New York Times*.

Murthy, N. and Gopalakrishnan, S. (2022), "Does openness increase vulnerability to digital frauds? Observing social media digital footprints to analyze risk and legal factors for banks*". International Journal of Law and Management,* 64(4), 368-387. https://doi.org/10.1108/IJLMA-04-2022-0081

Nalaka, S., & Diunugala, H. (2020). Factors associating with social media related crime victimization: Evidence from the undergraduates at a public university in Sri Lanka*. International Journal of Cyber Criminology,* 14(1), 174-184. https://ezaccess.library.uitm.edu.my/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Ffactors-associating-with-social-media-related%2Fdocview%2F2404395436%2Fse-2%3Faccountid%3D42518

Newberry, C. (2022). *Social Media Algorithms: A 2023 Guide for Every Network*. Social Media Marketing & Management Dashboard. https://blog.hootsuite.com/social-media-algorithm/#:~:text=strategy%20in%202023.-

Norwood, M. (2022). Social media experience of young people. *ProQuest Dissertations & Theses Global.* https://ezaccess.library.uitm.edu.my/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdissertations-theses%2Fsocial-media-experience-young-people%2Fdocview%2F2796963889%2Fse-2%3Faccountid%3D42518

Rani, P. U., & Padmalosani. (2019). Impact of social media on youth. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, *8*(11 Special Issue), 786–787. https://doi.org/10.35940/ijitee.K1138.09811S19

Rashidah Abdul Rahman, & Normah Omar. (2015). Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia Compliance and Effectiveness Analysis of the Mutual Evaluation Reports of

Financial Action Task Force Member Countries View Project Financial Statement Fraud View project. *Article in Journal of the Social Sciences*. https://doi.org/10.3844/jssp.2015

RR Author. (2022, August 18). Over 38% say teenagers spend more than 8 hours on social media daily. *Real Research Media.* https://realresearcher.com/media/over-38-percent-say-teenagers-spend-more-than-8-hours-on-social-media-daily/

Shareef, M. A., Mukerji, B., Dwivedi, Y. K., Rana, N. P., & Islam, R. (2019). Social media marketing: Comparative effect of advertisement sources. *Journal of Retailing and Consumer Services*, *46*(1), 58–69. https://doi.org/10.1016/j.jretconser.2017.11.001

Swart, J. (2021). Experiencing Algorithms: How Young People Understand, Feel About, and Engage with Algorithmic News Selection on social media. *Social Media + Society*, *7*(2), 1–11. https://doi.org/10.1177/20563051211008828

Teens and social media use: What's the impact? (2022, February 26). Mayo Clinic. https://www.mayoclinic.org/healthy-lifestyle/tween-and-teen-health/in-depth/teens-and-social-media-use/art-20474437#:~:text=Social%20media%20allows%20teens%20to

Tewari, M. (2022, June 11). Manish Tewari | Behind all social media ills: Not privacy, but anonymity. *Deccan Chronicle*.

The Economic Times. (2023, June 9). What is 'social media'? *The Economic Times.* https://economictimes.indiatimes.com/definition/social-media

Thukral, P & Kainya, V. (2022). *How social media influence crime.* ResearchGate. https://www.researchgate.net/publication/360540601_How_Social_Media_Influence_Crimes

Trninić, D., Vukelić, A., & Bokan, J. (2021). Perception of "Fake News" and Potentially Manipulative Content in Digital Media—A Generational Approach. https://scite.ai/reports/10.3390/soc12010003

UNICEF. (2017). *Children in a Digital World*. www.unicef.org/SOWC2017

Research Article

The Application of Ethics in The Development of Cyber-Physical System

Siti Nur Ramadan Mohd Sahim[1], Siti Norafiqah Mohd Nasir[2], Muhammad Safdar Izzul Islam Mohd Yatim[3], and Zaila Idris[4*]

[1] Universiti Teknologi MARA; 2020456042@student.uitm.edu.my; 0009-0004-0554-9868

[2] Universiti Teknologi MARA; 2020602396@student.uitm.edu.my; 0009-0009-1790-2602

[3] Universiti Teknologi MARA; 2020456016@student.uitm.edu.my; 0009-0006-7569-757X

[4] Universiti Teknologi MARA; zaila267@uitm.edu.my; 0000-0002-8287-6430

[4] Correspondence: zaila267@uitm.edu.my; 012-9329530.

Abstract: *This article discusses the application of ethics in the development of cyber-physical systems. The impact of the development of cyber-physical systems has become a debate between philosophers and technologists today. This is because cyber-physical system technology has changed the thinking and landscape of modern society. This issue clearly has an impact on human relationships because humans are becoming more dependent and influential with the development of technology. This makes human values fade into themselves until they are completely dependent on technology. Humans will be distracted by technology until they forget about the real reality of human life, to the point of causing various mental illness problems such as depression, anxiety, and bipolar. Therefore, the purpose of this study is to discuss the development of cyber-physical systems that threaten the ethical values of society. Meanwhile, the objective of our study is to identify the influence of cyber-physical systems on ethical values in society and the challenges to the development of cyber-physical systems. This study uses the literature review method. This method is used to find accurate information in online databases and has credibility because most of the review articles are based on previous studies produced from 2017 to 2021 to see the difference of opinion between philosophers and technologists. According to the analysis of this article, numerous studies have been conducted to examine ethical changes in the development of cyber-physical systems. Researchers are taking this issue seriously and doing a thorough analysis of the changes in ethical values that are impacted by the advancement of cyber-physical systems due to this change in ethics.*

Keywords: cyber-physical system, CPS, ethics, cyber ethics, development

DOI: 10.5281/zenodo.8181104

1. INTRODUCTION

A new digitally networked embedded systems, known as "cyber-physical systems" (CPS), link the physical and digital worlds through sensors and actuators (Esterle & Grosu, 2016). The term "CPS" was first used in 2006 by Helen Gill of the US National Science Foundation (NSF). Since then, the system that connects the offline and online worlds has come to be called 'CPS' (Lee, 2015). Since then, the NSF has generously funded his studies on CPS (Shi et al., 2011). This is because it can have significant social, environmental, and economic impacts. Cyber-physical systems (CPS), a class of large-scale, interconnected systems composed of physical and computational elements, are currently of interest to academia, industry, and government (Xu et al., 2014; Gürdür et al., 2016). With the advent of Industry

4.0 and the Internet of Things (IoT), embedded systems have given way to CPSs in the manufacturing sector. By integrating cutting-edge capabilities through IoT and the Web of Things, enabling the connection of physical reality operations with computing and communication infrastructure, CPS is an excellent foundation for the development of advanced industrial systems and applications. (Xu et al., 2018; Lu 2017). Cyber-physical system “CPS” is a new generation digital system consisting of two main functional components such as intelligent data management, analysis, and computing power to create cyberspace and advanced connectivity to ensure real-time data collection from the physical world and information feedback from cyberspace (Lee et al., 2015). Connected CPS may be widely deployed in the coming decades to solve global needs in sectors such as energy, water, healthcare, and transportation (Satchidanandan & Kumar, 2016). This study is an overview of the literature on the theoretical foundations and applications of CPS. Due to their potential to have significant social, environmental, and economic impacts, CPS are currently of interest to scientists, businesses, and governments. According to several recent studies (Li et al., 2018; Lu 2017b; Xu & Duan, 2018), CPS has become a central part of 'Industry 4.0'. CPS aims to accelerate the deployment of large-scale systems by improving the adaptability, autonomy, efficiency, functionality, reliability, security, and availability of these systems. CPS applications cover many fields such as agriculture, energy, medical, industrial, transportation and smart environment. A few studies reveal the current state of Cyber Physical System research.

However, there is no thorough and systematic review of research on the application of ethics in the design of cyber-physical systems. This journal comprehensively discusses the definition, theoretical foundations, ethical applications, and applications of CPS. Next, the current state of his CPS applied research on ethical management of CPS is discussed. This journal examines the ethical concerns surrounding cyber-physical human systems (CPHS). Intelligent cyber-physical systems (CPS) are emerging due to the increasing integration of computers, communications, and controls into various physical systems with sensors and actuators and increasing levels of automation enabled by machine learning and artificial intelligence. being developed. The increasing use of such technologies in dynamic public environments is changing the way people interact with intelligent CPSs. The development of smart and connected cars, robotics in manufacturing, robotic surgery, precision agriculture and other technologies, transportation, manufacturing, energy, and healthcare are all undergoing this dramatic change. Such developments are likely to continue and accelerate over the next few years and decades. Considerable ethical challenges are expected in the development of such a revolutionary CPHS that impacts both individuals and society. This article presents a structure for analysing how the emergence of cyber-physical systems threatens society's ethical norms. The purpose of our research is to elucidate how ethical ideals in society are affected by cyber-physical systems and what difficulties arise in their growth.

2. LITERATURE REVIEW

For this literature review, we have taken various opinions and views done in previous studies related to our topic. We take information from various credible sources such as journal articles and additional sources such as information search results. Among the journal articles we use are "When Smart Systems Fail: The Ethics of Cyber–Physical Critical Infrastructure Risk (Grady et al., 2021)", "Applications of Cyber-Physical System: A Literature Review (Chen, 2017)" , "Human Digital Shadow: Data-based Modeling of Users and Usage in the Internet of Production (Mertens et al., 2021)", "A Framework for Ethics in Cyber-Physical-Human Systems (Sampath & Khargonekar, 2020)", "Ethics Aspects of Embedded and Cyber-Physical Systems (Thekkilakattil & Dodig-Crnkovic, 2015)", and "Designing Ethical Cyber-Physical Industrial Systems (Trentesaux & Rault, 2017)".

2.1 Ethics

In today's technological development, ethics is very important to make sure in control something, so it does not exceed certain limits. Based on Merriam-Webster, an online dictionary, ethics may be described as a set of moral principles that include: a moral value theory or system. Ethics and Morals are different from each other. Ethics is a guide about what is good and what is bad to do, it can also help us for decision making or making judgement. However, morality is a system used to modify and regulate our behavior. This system can create a moral person who has a high sense of justice and a high sense of humanity towards others. According to Trentesaux and Rault (2017), ethics was initially a field of philosophy. Ethical behavior is in line with the culture that has to do with morality and justice (Morahan, 2015). Ethics has different types based on its use in various fields. According to Trentesaux and Rault (2017) have discussed techno/engineering ethics in the literature review section of their article. From the review made, they discovered that in industry, techno/engineering ethics has been addressed mostly in the fields of information and communication technology (ICT) and robotic engineering. It focuses heavily on cyber security, data usage ethics, young people and the internet, privacy, and other topics in ICT (Capurro, 2000), (Bhadauria et al., 2010). The research done by them is more directed to the field of robotic engineering. According to the authors, the presence of the IEEE-RAS Technical Committee (TC) on Roboethics aided in the realization of various initiatives that had an influence on Roboethics. The "Euron Roboethics Atelier" project in 2005 aimed to draw the first Roboethics Roadmap as a guide for those in this field, there are also other projects such as European Union (EU) Project Ethicbots (2005-2008) and EU Project RoboLaw (Palmerini et al., 2016). There are two ethical theories presented in the study made by (Alsegier, 2016), namely rule utilitarianism theory and social contract theory. The authors also found that the main factor that encourages the use of techno ethics by researchers is often related to the idea of a charter to be signed through the Hippocratic oath (an oath of ethics historically taken by physicians).

In addition, the author (Trentesaux & Rault, 2017) also discussed machine ethics, it has complexity level 2 to 4. At complexity level 2, AI can be dealt with well by identifying and verifying or limiting (proof) all behaviors and conditions different research object which is the designed system. The authors state in this regard that the traditional and historical technique is a holistic way to create autonomous systems utilized by industrial R&D engineers. At level 3, the legal responsibility of the learning entity from a lawyer's point of view can be addressed with a set of very innovative works, there is a large corpus of law that is only human-centered and has nothing to do with artificial beings. This suggests the emergence of a new species other than humans, and it may also mean that the human rights constitution should be revised correspondingly. For example, the study made by (Dreier & Döhmann, 2012) has discussed service robot administrative control organization and legal liability regime, as well as the question of service robot autonomy. In addition, the study made by (Sampath & Khargonekar, 2020) also discusses artificial intelligence ethics. Automation, artificial intelligence, and machine learning are being integrated into the next-generation cyber-physical human system (CPHS), a type of variation of cyber-physical system. The authors take and focus on the latest IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems (A/IS) study "Ethically Aligned Designed (EAD)" (IEEE, 2019). This study provides an ethical analysis conceptual framework based on three pillars: universal human values, political self-determination and data agency, and technical dependability. These three pillars serve as the foundation for general principles critical to the ethical design of A/IS, such as human rights, well-being, data agency, efficacy, openness, accountability, misuse awareness, and competence. Detailed ideas on how to deal with this ethics issue can be supplied, with the main purpose of assisting A/IS developers in reducing to practice applicable principles in the goods or services they supply.

There are examples of ethics that are practiced in certain fields to achieve their goals, it is also known as a code of ethics which is a guide for an organization. According to Sampath and Khargonekar (2020), in the United States, the National Society of Professional Engineers, a group specifically for engineers, has a code of ethics for engineers that is organized for all professionals that work there. Engineers' services, according to this code of ethics, must be honest, unbiased, fair, and equitable, and must be committed to the preservation of public health, safety, and welfare. Furthermore, the Association for Computing Machinery (ACM), a US-based worldwide learned society for computing, has a Code of Ethics and Professional Conduct that asserts that "the actions of computing professionals change the world.". To act responsibly they need to always think about the impact on society rather than thinking about their work alone, consistently to support the public good. The Code of Ethics and Professional Conduct expresses the conscience of the profession". According to Thekkilakattil and Dodig-Crnkovic (2015), the European Union (EU) has made a proposal related to robotics and artificial intelligence at the parliamentary level (Delvaux, 2016). Aside from presenting the fundamental goals of human safety, integrity, safety, autonomy, and dignity, the EU Parliament's goals are to unite and stimulate European innovation in robotics and artificial intelligence (AI). The ethical framework is made up of the Robotics Charter, which includes the Code of Ethical Conduct for Robotics Engineers, and Licenses for Designers and Users, which are based on the principles of the EU Charter of Fundamental Rights and are dependent on the establishment of the European Agency for Robotics and AI.

2.2 Cyber-Physical System

Cyber-physical system (CPS) is now a topic that is hotly discussed in various fields such as industry, academia and government because of its potential to impact society, the environment and the economy. The definition of CPS changes according to various perspectives in the scientific community. According to Hong Chen (2017) in his study, CPS is a physical and engineering system monitored, coordinated, controlled, and integrated by a computational and communication core. CPS is also a new generation of integrated systems with computational capabilities and physical capabilities that can interact with humans through various modalities or ways. The author concludes that CPS is a combination of embedded systems, real-time systems, distributed sensor systems, and controls that focus on the complex interdependence and integration between the cyber and physical worlds and are made up of tightly integrated computation, communication, control, and physical elements. Although CPS has been used since the early 1970s, when the first microprocessors appeared, it began to alter in 2006, when Dr Helen Gill from the United States National Science Foundation's Program on Cyber-Physical Systems invented the phrase "cyber-physical system" (RMIT University, 2019). Cyber-physical systems are classified into two types: autonomous cyber-physical systems and closed-loop human machine systems. Autonomous cyber-physical systems are systems that can make decisions and operate "stand-alone". However, nowadays, the development of many cyber-physical systems in semi-autonomous systems, for example, semi-autonomous drones, users can set the flight path and real-time machine vision to allow the drone to avoid obstacles, this can reduce the dependence on the need for manual flight. The system is a cognitive system, it can learn from the environment, from the human itself to make decisions in real-time, but it is not completely dependent on this system, humans remain part of the decision-making process in this system (Roberto, 2019).

Cyber-physical system (CPS) can be applied to various fields involving computing and technology. According to Sampath & Khargonekar (2020) who studied the computer-physical-human system (CPHS), CPS allows basic control system knowledge to be used and incorporated into new technological systems. Applications in fields such as manufacturing, energy, transportation, aerospace, and military are all examples of industries, it can also be applied to biomedical and healthcare fields and may be many more in the future. For example, an autonomous system that can control the driving of a vehicle that can decide what road to take. Industry 4.0 and smart manufacturing can also happen by applying CPS. The integration of renewable electricity from solar and wind turbines is key to a smart electric grid (Annaswamy & Amin, (2013) enabled with CPS. In addition, smart CPHS is an integrated combination of machine learning (ML) and artificial intelligence (AI). CPHS with AI and ML is applied to e-commerce, information processing and computer vision. Smart electric grid, smart manufacturing and smart health has become a topic for research and development, and we can expect a wider commercial development of smart CPHS in the future with the development of current technology. According to Chen (2017) taking from (Wang et al., 2007; Li et al., 2008, 2014; Tan et al., 2010), CPS applications include many fields and disciplines such as agriculture, energy, health care, manufacturing, transportation, and smart environment. CPS also deals with physical systems such as transportation, energy, medical, and defense. Based on the research done, The author discovered that CPS is also used in agriculture, education, energy management, environmental monitoring, intelligent transportation, medical devices and systems, process control, security, smart city and smart home, and smart manufacturing.

Cyber-physical system (CPS) also has various types according to the field to be applied such as the production field, according to Mertens et al., (2021) CPS is used for the internet of production, it is known as cyber-physical production systems (CPPS). Because of the system's complexity, data generation is frequently heterogeneous, unstructured, and isolated. The first step in realizing the goal of the Internet of Production should be the connectivity of machines, people, and whole production sites throughout the world to enable interaction and information exchange with one another. information about all available sensors and systems is stored in the Data Lake, it refers to a large-scale storage place to store raw data to handle a high amount of unstructured real-time data. The digital shadow aims are then to link abstract and aggregate data from the Data Lake for specific activities and concerns, allowing knowledge-based and real-time decision making in manufacturing, development, and related disciplines. The interdisciplinary group of authors is persuaded that an extra anthropocentric perspective in the form of a Human Digital Shadow has enormous promise for addressing current and future CPPS concerns in a more sustainable and integrated manner. Despite amazing development in the field of automation, humans will continue to be the primary and most significant function in socio-technical production systems in the long term. The Human Digital Shadow encompasses all data that can be provided to human actors in a sociotechnical system as a source or sink. The Human Digital Shadow is similar to the Digital Shadow, but it aids in the examination of actual connections between individuals, technology, and organizations. Human Digital Shadows can include, for example, their behavior and movement patterns. To study this concept, the authors used different perspectives to apply Human Digital Shadows in the CPPS that was developed based on a Delphi Study and then used SWOT to make an analysis. In addition, there are also CPS used for machine learning and intelligence such as (Sampath & Khargonekar, 2020) cyber-physical-human systems (CPHS). Continuous integration of control, communication, and computing into various types of physical systems using sensors and actuators, in conjunction with rising levels of automation, enables machine learning and artificial intelligence to produce a smart system known as smart CPS. The effect of this CPHS innovation affects individuals and society, especially ethical issues. The study conducted by the authors provides a framework to assess current and possible future ethical issues in smart CPHS. In recent years, the term CPHS has been used to capture the entire CPS interacting and embedded in human society (IFAC, 2018).

3. METHODOLOGY

Literature reviews are one of the methods used by researchers to obtain information from past studies conducted by other researchers that have topics related to or similar to the one you are studying. Literature reviews can provide an overview of the topic being studied to allow you to study your topic in more depth and provide a good understanding. One of the processes to get good literature reviews is to search, evaluate, identify, and write.

For search, researchers look for suitable materials to be used as literature reviews. Researchers look for it in online database platforms such as Science Direct, IEEE, Emerald Insight and Google Scholar. All of these are online databases that provide materials that are credible and mostly accurate. Researchers use the keywords "cyber-physical", "cyber-physical system", "ethic", and "development" to find suitable material according to the topic under study. The researcher arranged the time of the article from 2017 to 2023 and set the category "journal article", to find information that is still relevant and accurate to the needs of this study. Researchers also use Boolean search techniques "AND", "OR" and "NOT" to find materials that are really related only to the topic under study. For example, "ethics" AND "cyber-physical system" AND "development". Search results with this search technique will produce materials that have those keywords and are related.

Next, evaluate. The researcher evaluates the material that has been searched for. A total of 15 journal articles were found by researchers that are related to the topic under study. After evaluating and appropriateness of the content reviewed in this journal article, the researcher decided to select 6 articles from the 15 articles because they fit the topic under study.

Next, identify. After the material was obtained and selected, the researcher began to read one by one the journal articles that were searched to identify what relevant content could be placed in the literature reviews. This looks at the relevance of the content to the topic being studied.

Finally, write. After identifying what content is appropriate. Researchers start writing literature reviews in the past tense because it is a past study. Content in the journal article will be read and paraphrased into its own sentences to avoid plagiarism.

Apart from searching for information in the online database, the researcher also used the search engine "Google Chrome" to find additional information to support or improve the written content.

4. RESULTS AND DISCUSSION

4.1 Influences of the cyber-physical system towards society ethics values.

A cyber-physical system (CPS) is a technical system that communicates with the physical world via networked computers, robots, and artificial intelligence. Other examples of CPS include smart grids, self-driving car systems, medical surveillance, industrial control systems, robotic systems, recycling, and autopilot avionics. Given that every type of system has advantages and disadvantages, developing human ethical standards should be given priority alongside the development of cyber-physical systems. To assist European legislators in foreseeing potential future issues associated with advancements in CPS, robots, and artificial intelligence, the Scientific and Technological Options Assessment Panel (STOA) has established a project titled "Ethical Aspects of CPS." Health care, agriculture and the provision of food, manufacturing, energy and essential infrastructure, logistics and transportation, and the safety and protection of human communities are among the subjects addressed by the CPS. The system should therefore emphasize a variety of elements, such as those pertaining to the social, technological, environmental, economic, political, ethical, and demographic aspects of CPS use. This is because the CPS could have an impact and result in issues down the road. As a result, the development of this CPS has made it possible for social scientists and technological specialists to collaborate on an in-depth investigation of probable CPS-related ethical dilemmas in the future.

When the potential future effects of CPS are examined, it becomes clear that many aspects of our personal and professional lives may be significantly impacted. Many legal difficulties, such as accountability, liability, data ownership, and privacy, are raised by the deployment of autonomous work robots connected to complex data environments. When constructing CPSs for activities involving humans, current safety laws must be updated to guarantee that no one is hurt and that the anticipated advantages outweigh any potential unintended consequences. These standalone policy briefs may be suitable for actual usage by the following congressional committees: Ethical issues and soft repercussions are translated into legal and regulatory considerations for cyber-physical systems. First, the STOA report might serve as a useful "tool" for the relevant committees as they formulate their opinions on the draught DELVAUX report on robot civil legislation. If the report is approved, it is hoped that it will serve as the foundation for upcoming EU legislative efforts.

These systems, which combine computer, networking, and physical operations, have the potential to significantly increase productivity, security, and comfort. To make sure that these systems are created and utilized properly, CPS development and implementation also involve significant ethical issues, just like with any technological innovation. The possibility of greater surveillance and privacy invasion is one of the most urgent ethical issues concerning CPS. These technologies will probably gather enormous volumes of information about people and their behaviors as they spread throughout society. There are many potential uses for this knowledge, both good and bad. For instance, CPS data could be used to enhance municipal traffic flow, but it could also be used to track people's activities for sinister purposes. Strong privacy safeguards must be incorporated into the design of CPS in order to solve this issue, and there must be clear standards for the use of the data gathered by these systems. According to privacyinternational.org resource, massive surveillance involves the collection, processing, creation, analysis, use, or storage of data about a large number of individuals, whether or not they have been accused of wrongdoing. In democratic societies, comprehensive surveillance is neither essential nor proportional, thus creating challenges from a legal perspective. There are often less-invasive alternatives. We also question whether democratic societies can exist under constant scrutiny, especially if they do not. Mass surveillance creates the potential for unlimited state power and control over people through daily life surveillance. Fundamental values and principles of democratic societies aim to limit the information states know about their citizens to limit their power, but the assumption that all information helps counter hypothetical threats incompatible with mass surveillance undermines the separation of powers by giving the executive freedom of action without strict legislative or judicial regulation. Due to the fact that oversight powers are not granted in connection with every wrongdoing but collectively, mass oversight powers lack effective independent powers. In the eyes of the state, everyone is guilty until proven innocent, but this is incompatible with democratic ideals and principles. It fosters a climate of danger and mistrust. Finally, mass surveillance adversely affects other freedoms and rights. Unjustifiable invasions of privacy interfere with the enjoyment of other freedoms and often open floodgates to violations of other rights such as freedom of assembly, freedom of expression, and freedom of movement. Prohibition of discrimination and political participation.

The prospect of job displacement is another ethical problem associated with CPS. As these systems progress, they might be able to conduct jobs that formerly required human personnel. In some industries, especially those that entail manual labour or repetitive tasks, this could result in large employment losses. It has historically been the case that the development of new technologies has resulted in the creation of new jobs, but given the rapid improvements in CPS, it is uncertain whether this trend will continue. It is vital that governments and businesses invest in education and training programs to support workers' adaptation to the shifting labour market in order to lessen the possible negative effects of job displacement. Discussions regarding artificial intelligence's (AI) potential effects on the labour market have been spurred by the technology's rapid advancement. Concerns about intelligent machines replacing humans as workers grow as AI technology progresses. Automation of normal and repetitive tasks across numerous industries by AI has the potential to replace some job functions. Automation is more likely to occur with tasks that are simply specified, characterized, and conducted algorithmically. For instance, AI-powered robots on assembly lines can replace human labour in the manufacturing industry. Chatbots are getting better at answering simple questions in customer service. It is vital to understand that technical developments have traditionally changed the nature of employment rather than completely destroying occupations, even though job displacement due to AI is a threat. As regular jobs are automated, new career opportunities arise that call for aptitudes that are only possessed by people, including adaptability, emotional intelligence, creativity, and problem-solving. Additionally, AI can supplement human abilities, allowing employees to concentrate on more difficult jobs that call for complex decision-making and critical thinking. AI has the potential to replace certain occupations while simultaneously creating new ones. AI engineers, data scientists, ethical experts, and policy analysts are just a few of the trained individuals needed for the creation, implementation, and maintenance of AI systems. AI can also stimulate economic growth by boosting productivity, encouraging innovation, and enabling companies to provide novel services and goods. Employment prospects in linked industries may result from this in turn. Retraining and upskilling programs are essential to reducing the possible negative effects of job relocation. Individuals can develop new talents that are in demand in the AI-driven job market by making investments in lifelong learning projects. Governments, educational institutions, and organizations must work together to offer easily accessible training programs at reasonable costs so that people can move into burgeoning professions. For managing the shifting work landscape, it will be crucial to place an emphasis on adaptation and lifelong learning. Even though losing a job may have economic repercussions, it's important to think about how it will affect society as a whole. To help displaced workers move on to new careers, there needs to be enough support mechanisms in place. Policies and rules should also address potential problems, including wage disparity, job polarization, and protecting employees' rights in the age of AI. It is essential to make sure that society as a whole receives the advantages of AI in an equitable manner.

Another moral issue that needs to be resolved is the possibility that CPS could be used as an instrument of social control. This technology has the potential to monitor and suppress opposition under an authoritarian system, enhancing the authority of a repressive administration. There is a chance that CPS will be employed to unfairly target particular groups or people according to their political opinions or other qualities, even in a democratic country. It is crucial that a solid legal framework be in place to safeguard people's rights and freedoms in order to prevent the exploitation of CPS for social control. The PiMind paper is an illustration of how CPS is used as a social control tool. Although it is currently feasible to make certain predictions about its implementation, Terziyan et al. (2018) believed that the digital twinning of human decision-making behavior required more advances in order to be validated. Pi-Mind Technology can be defined as a process where the world's most brilliant brains' decision-making processes are trademarked for use in high-tech machines. To enable the proper operation of the patented clones' decision-making behaviors, corporations must have incorporated sufficient technology. More than technology, it is essential that employees of the companies have a strong enough digital culture to inspire a desire for adaptability to new technologies. The advancement of technology and the use of CPSs in manufacturing facilities will significantly affect human employment. Companies will need to inspire employees and help them see the future in order to avoid issues like the inability to coordinate operations across various organizational divisions or a lack of employee enthusiasm and technical proficiency. In actuality, people will play a crucial role in the transition to the adoption of CPSs in businesses. In this situation, the development of decision-making clones acknowledges the existence of great minds that ensure the transformational process's success. The deployment of CPSs therefore necessitates the most skilled agents of the company because this process is dependent on the knowledge of individual employees. Additionally, it is asserted that this approach can capture cognitive elements of creative human decision-making based on individualized values and preferences. When applied to CPSs, this will have an effect since, despite the automatic decision-making approach, a human is still involved in the process. The so-called "Smart consultants," whose goal is to make recommendations to the human workers since they may not yet be able to replicate the human decision-making process, can be used to further integrate Pi-Mind technology into production. A decision maker needs to feel confident in the accuracy and completeness of the data in order to make a choice, and these "smart consultants" are equipped with the ability to gather data via the integrated CPS sensors in order to warn humans about potential problems. Pi-Mind agents can be structured as a single expert or as groups of autonomous Pi-Mind agents, forming a multi-agent system where the Pi-Mind robots communicate with one another. This interaction must be taken into account. Finally, the incorporation of legal considerations constitutes a crucial requirement for the execution of this method to ensure that Pi-Mind agents' objectives and actions are consistent with and supportive of human values in all facets of their employment.

Accountability issues also pose serious ethical challenges in the context of CPSs, and as these systems become more autonomous, finding accountability for their activities may become more difficult. For example, if a self-driving car is involved in an accident, it can be difficult to determine whether the car's manufacturer, software developer, or owner is at fault. This lack of clarity can make it difficult for victims to seek financial compensation and for authorities to enforce safety regulations. According to Gruel & Stanford (2016) and Pernestl & Kristoffersson (2018), self-driving cars are predicted to fundamentally change the way we travel and use transportation. It will take a long time, require significant investments in infrastructure and vehicles, and require changes in behaviour and mindset. Full self-driving road vehicles are likely to be phased in over decades, perhaps only in limited locations such as parking lots and designated highways and highway lanes where speeds are minimized. This is a fundamental technical change. It takes a lot of effort to predict and evaluate all possible social changes caused by the introduction of the latest technology. As part of this effort, the ethical and political implications of the technology itself and possible deployment scenarios should be considered (Palm & Hansson, 2006). Much of the discussion about self-driving cars is about liability. Current tests on public roads always have a 'safety driver' or 'steward' at the wheel who is required to monitor traffic and take immediate control if necessary. Even without the advent of self-driving cars, traditional notions of who is responsible for what on the road have changed in recent decades. Historically, drivers and other road users have been primarily blamed (Melcher et al., 2015, p. 2868). Currently, our tolerance is very high when it comes to large differences in the hazards that different cars pose to other road users due to differences in equipment, driver skill, and actual attitude. To ensure a minimum level of technical safety, it is common in many countries to require monthly inspections of vehicles, including brake tests and other basic standard inspections. However, there are still significant differences between driver monitoring systems and anti-lock braking systems between car makes and models. Newer cars are generally held to higher standards than older ones. To our knowledge, there is no practice anywhere in the world to bring old vehicles up to the technical safety standards of new vehicles. Updating software in older vehicles can be a difficult problem, especially for vehicles beyond the manufacturer's lifetime (Smith, 2014).

4.2 Challenges against the development of cyber physical systems.

The Internet of Things, also known as IoT, has created this new ecosystem known as cyber-physical systems. Creation of new technologies and cutting-edge technical systems using computation, communication, and control in cyber-physical systems. A few decades ago, there was a lot of research on cyber-physical systems that society could not have foreseen. The development of this new ecosystem poses many risks and difficulties that raise questions about how human ethics will change. Therefore, this document also covers his CPS security issues. Security by design is one of the common problems in CPS. Most CPSSs are not designed with security in mind because they are not connected to any other network, such as the Internet. Most CPSS are not connected to any other network, so security is not a consideration in their design. Physical security is therefore paramount to ensuring personal safety. Physical security is the best way to keep people safe. Addressing both cyber and physical aspects of security requires CPS designers to redefine the way security is viewed. In the future, this could allow us to predict and stop cyberattacks that cause physical damage more accurately. We need to create a framework for both components of the cyber-physical solution that have been neglected so far. Inconsistent change is another difficulty facing CPS. There are many people working at CPS. This includes both those who work for them and those who produce, consume, own, and operate goods. Even if the roles and rights are different, it is important to manage them properly. Many people and various CPS departments have to deal with issues that cannot be overlooked during the transition. Community collaboration among her members involved in the CPS department will be very important at some point. Improvement methods include introducing new features, updating, or modifying software, and upgrading hardware. Please keep in mind that unexpected changes to CPS security, such as new vulnerabilities, can compromise system security and cause serious national problems.

4.3 Smart grids challenges

Change management is a difficulty in the development of the smart grid. Change management in a smart grid is not any simpler than it is with ICS, but it is also not any more difficult. Smart grids are more sophisticated and involve more people, yet they struggle to adapt to change. As a result, change management is essential for a robust smart grid. Advanced Metering Infrastructure (AMI) enables two-way communication in smart grids. AMI enables smart meters to communicate with utility providers near customers' houses, unlike the power grid, making it simpler for physical assailants to flee. In the smart grid, where there are more gadgets than ever before, it is getting harder to keep these devices secure. A strong access control system is necessary for smart grids because of their extensive reach and large investor base. It's crucial to keep an eye on and restrict any access that may be granted to network, data, or smart grid devices. Giving the individual or organization that is intended to assist enough power in an emergency is always the wisest course of action. Additionally, they are concerned about the use of their data. This has grown to be a significant issue for people as smart grids become more widespread. In addition to encrypting customer data, it's critical to provide anonymization procedures to stop hackers from deducing patterns from encrypted data to reveal sensitive information. We refer to this as "anonymization." Therefore, we must be sure that the systems we create can safely gather and encrypt data. There should not appear to be any trust placed in the delivered information and instructions in this situation. Alternately, new strategies to spot unauthorized false data and instructions must be developed. Due to the complexity of the smart grid, it may be challenging to employ specific algorithms that solely check for issues, making FDI attacks difficult to detect. Therefore, having elevated levels of security in a smart grid is beneficial. It's terrible at lower levels (since devices at lower levels have fewer capabilities). As a result, each level's required level of security might not be the same. To do this, numerous research teams must provide simple solutions. To keep data private and secure, encryption is crucial at all levels of the smart grid. To prevent any security breaches, do this.

4.4 *Smart Vehicles challenges*

There are contradictory security assumptions at the edge of integration when manufacturers integrate commercial-off-the-shelf (COTS) and third-party modules into smart automobiles. According to the automakers, the COTS integration must be dependable, and other components must function well. It should guarantee that automakers do not compromise on safety in any way. If the Electronic Control Unit (ECU) of the gateway can be circumvented, then several attack methods, such as bypassing it and gaining access to constrained bandwidth, can be employed against it. Our cars can operate more efficiently by separating critical and non-critical ECUs, utilizing Ethernet or IP connections, and swapping out gateway ECUs for expert ECUs. Other partners in the automotive industry produce, buy, or import car spare parts and components. Both vendors and purchasers should focus more on security criteria, evaluation, and testing to make sure there are no security flaws or patches. Safety must be a consideration for manufacturers from the start of the design process. The CAN network is exposed due to the presumption that it is isolated. A new protocol that takes potential malevolent attackers into account is required. In the coming years, communication between vehicles (V2V) and infrastructure (V2I) will encounter a number of new security issues. It takes this danger to put an effective solution on hold and allow it to function.

4.5 Challenges in medical cyber-physical system.

Medical devices use technology to automate some functions, including hardware features such as security keys. However, given the importance of software development, it is generally accepted that the Machine Copyright Protection Society's (MCPS) security cannot be guaranteed. Therefore, it is important to ensure that medical devices are certified, safe, accurate, efficient, and protected. Patient information provided during system contact can help diagnose illness earlier, alert emergency personnel, and provide a clearer picture of the patient's overall health. By enabling this device to be used to treat patients in the most effective manner, MCPS' analytical expertise can be leveraged to increase the flexibility of the device. In this way, the circuit should be closed quickly and safely. MCPS collects medical data and maintains the collected data, so security and privacy are paramount. Therefore, it is important to protect your data from being accessed or modified by anyone. As a result of such behaviour, patients may lose their privacy and be exposed to discrimination, abuse, and even physical violence from others. Additionally, most medical devices are designed to work for groups of people with similar medical conditions. Patients can react very differently to the same drug, so it can be very confusing and take a lot of time on MCPS. For example, most medical devices can simultaneously trigger an alarm when a potentially dangerous condition occurs. Medical devices can also cause false alarms. Parents do not do that. To effectively treat patients and collect information for electronic health records (EHRs), medical devices are now establishing robust network connections. In this case, studies should be conducted using flexible algorithms that can be adapted to the individual needs of patients. To reduce false alarms, it is planned to modify the alarm thresholds and display the patient's training history in her EHR. Future medical devices may integrate "smart alarm services" to reduce false alarms. Currently, it is the only company working on medical device integration and decentralized interoperability infrastructure, facilitating regulatory approval while reducing the benefits of device-to-device communication. The cornerstone of medical device interoperability is one of many open connectivity standards shared by MCPS. However, it would be more effective if this standard could be applied to a platform that is easy to build and use. To get the most out of their products and to ensure that they work together and integrate with each other, medical device manufacturers must follow a set of standards when developing their products.

5. CONCLUSION

In summary, wide embedded device deployment by CPS enables seamless real-world and virtual world integration, opening novel and intriguing business and research opportunities. It has a significant impact on our society and represents a brand-new paradigm for intelligent systems. CPS has been effectively used in several industries, including agriculture, manufacturing, transportation, healthcare, and more. However, the interaction between the dynamics of the cyber world, networking, and physical systems necessitates the use of fundamentally new advanced design technologies. Humans learn their values and expectations for moral behavior through experiences in their families, communities, schools, churches, and workplaces. Fundamental ethical principles have been upheld by a variety of societies and civilizations for centuries, and despite their strong foundation in human prosocial nature, social technology accelerates in a globally connected world. These changes are creating new situations such as: We can be more adaptive and future oriented. Smart CPHS will play a big role in driving these improvements. In order to fulfill our ethical obligations in many of our roles, we believe that the literature suggested in this article will serve as a basis for his discussion and development of CPHS ethics.

Acknowledgments: The authors would like to express deepest and most sincere gratitude to the corresponding author and lead researcher, Ms. Zaila Binti Idris, for giving the opportunity to conduct the study and for her valuable assistance during this study. Her dynamism, vision, integrity, and motivation have inspired us deeply. She gave us a methodology for conducting research and presenting the results as clearly as possible.

References

Chen, H. (2017). Applications of cyber-physical system: A literature review. *Journal of Industrial Integration and Management, 2*(3), 1750012 (28 pages). https://doi.org/10.1142/S2424862217500129

Grady, C., Rajmajet, S., & Dennis, L. (2021). When smart systems fail: The ethics of cyber–physical critical infrastructure risk. *IEEE Transactions on Technology and Society*, *2*(1), 6-14. http://doi. 10.1109/TTS.2021.3058605.

Hansson, S.O., Belin, M. Å., & Lundgren, B. (2020). Self-driving vehicles: An ethical overview. *Philosophy & Technology*, *34*(1), 1383–1408. https://doi.org/10.1007/s13347-021-00464-5

Liang, X., & Chen, H. (2020). The application of CPS in library management: A survey. *Library Hi Tech*, *38*(1), 117-131. https://doi.org/10.1108/LHT-11-2017-0234

Mertens, A. et al. (2021). Human digital shadow: Data-based modelling of users and usage in the Internet of production. *14th International Conference on Human System Interaction (HSI)*, 1-8. http://doi. 10.1109/HSI52170.2021.9538729.

RMIT University. (2015). *What are cyber-physical systems*? https://www.rmit.edu.au/news/c4de/what-are-cyber-physical-systems

Sampath, M., & Khargonekar, P. P. (2020). A framework for ethics in cyber-physical-human systems. *IFAC PapersOnLine*, *53*(2), 17008–17015. https://doi.org/10.1016/j.ifacol.2020.12.1251

The BlackBerry Cylance Team. (2020). *Using COTS Products to Visualize Vehicle Data and More*. Blackberry Blogs. https://blogs.blackberry.com/en/2020/01/using-cots-products-to-visualize-vehicle-data-and-more

Thekkilakattil, A., & Dodig-Crnkovic, G. (2015). Ethics aspects of embedded and cyber-physical systems. *IEEE 39th Annual Computer Software and Applications Conference*, 39-44. http://doi. 10.1109/COMPSAC.2015.41.

Törngren, M., & Sellgren, U. (2018). Complexity challenges in development of cyber-physical systems. *Lecture Notes in Computer Science*, 10760, 478–503. https://doi.org/10.1007/978-3-319-95246-8_27

Trentesaux, D., & Rault, R. (2017). Designing ethical cyber-physical industrial systems. *IFAC PapersOnLine*, *50*(1), 14934–14939. https://doi.org/10.1016/j.ifacol.2017.08.2543

Tyagi, A. K., & Sreenath, N. (2021). Cyber physical systems: Analyses, challenges and possible solutions. *Internet of Things and Cyber-Physical Systems*, *1*, 22-33. https://doi.org/10.1016/j.iotcps.2021.12.002.

Zhang, C., Xu, X., & Chen, H. (2020). Theoretical foundations and applications of cyber-physical systems: A literature review. *Library Hi Tech*, *38*(1), 95-104. https://doi.org/10.1108/LHT-11-2017-0230

Research Article

The Impact of Cybersecurity in Public and Private Sectors

Syahida Fara Najwa Sulaimi[1, *], Nur Asyikin Saidi[2], Nur Shafiqah Asmawi[3], and Noor Arina Md Arifin[4]

[1] UiTM Kelantan Branch; 2020492376@student.uitm.edu.my; 0009-0005-9430-6311
[2] UiTM Kelantan Branch; 2020834016@student.uitm.edu.my; 0009-0005-7425-2352
[3] UiTM Kelantan Branch; 2020859268@student.uitm.edu.my; 0009-0005-9035-2724
[4] UiTM Kelantan Branch; arina848@uitm.edu.my; 0000-0002-2900-0026
[*] Correspondence: 2020492376@student.uitm.edu.my; 01131601606

Abstract: *This paper is about cybersecurity in today's world. Cybersecurity is the area of information security that focuses on safeguarding the availability, confidentiality, and integrity (CIA) of digital information assets from dangers that could result from those assets being compromised online. Cyberattacks have arguably garnered more regular media coverage in recent years. The objective of this paper is to give knowledge to all private and public sectors about the importance of cybersecurity care and to spread awareness to all private and public sectors about security. The problem statement of this paper is lack of knowledge from public and private sectors about importance of cybersecurity care and lack of awareness about cybersecurity in public and private sectors. The cybersecurity environment includes high-profile data breaches, hacks, and cyberattacks. Cybersecurity is crucial for all organisations, not just business and government organisations. The growing number of people using the internet worldwide is the primary factor behind changes in cyberattacks. The growth, frequency, and sophistication of cybersecurity assaults, particularly those utilising social engineering techniques like phishing and malware, make it difficult to establish a strong cybersecurity defence. Many organisations think that the IT and security teams are the only ones with responsibility for managing cybersecurity risk. An organisations-wide understanding of cybersecurity issues is actually necessary for an effective strategy.*

Keywords: cybersecuirty; private sector; public sector, applying law, cyberattacks

DOI: 10.5281/zenodo.8181140

1. INTRODUCTION

Newspaper articles, academic papers, security-related conference proceedings, and many other studies make it evident that cyberspace, and particularly cybersecurity, is a subject that is currently attracting considerable interest and attention from a wide range of stakeholders. The objective of this paper is to give knowledge to all private and public sectors about the importance of cybersecurity care and to spread awareness about cybersecurity among all private and public sectors. Month by month, the significance and importance of this subject grow, along with the implications and impact that it has. From the average person using their online banking account to the boards of directors (BoDs) of corporations, stakeholders span the entire spectrum. These boards are becoming increasingly aware that safeguarding their respective companies in cyberspace is a clear corporate governance obligation, and as a result, they are responsible for the related cyber risks in their organisations and the ensuing legal repercussions for any potential negligence or ignorance. However, because of these worries about cyber-related risks, a lot of people including security solution providers looking to market their products—have turned the term "cybersecurity" into a buzzword because of the problem such as lack of knowledge from public and private sectors about importance of cybersecurity care and lack of awareness about cybersecurity in public and private sectors. In doing so, they often capitalise on the "cyber fears" of users and executive management by using it as an umbrella term for all security-related concepts. Depending on the circumstance, various definitions and explanations of cybersecurity are given, and phrases like the following are frequently used in connection with the cyber field.

Cybersecurity is the area of information security that focuses on safeguarding the availability, confidentiality, and integrity (CIA) of digital information assets from dangers that could result from those assets being compromised online. Information security includes cybersecurity. Cybersecurity is concerned with safeguarding the CIA's digital information assets against threats and attacks that in some way include the internet, which serves as the primary application domain for cybersecurity. This illustration may help further clarify the meaning. Let's say a worker sells a USB drive to an unauthorised person after copying private company data onto it. Information security has undoubtedly been compromised, but cybersecurity has not occurred because the internet is not involved. However, if an employee uploads data from within the organisation to a cloud-based storage system (over the internet) and the unauthorised party is given access to this cloud storage, then this becomes a cybersecurity and information security breach. The cybersecurity environment includes high-profile data breaches, hacks, and cyberattacks. Attacks on computers and information networks, both public and private, are disclosed in the news daily. Most recently, Apple, Facebook, and Twitter acknowledged that they were attacked and were now taking additional measures to secure their networks. As a result, both the public and private sectors now view cybersecurity as a top issue. Cybersecurity is becoming increasingly crucial due to the increased reliance on computer systems, the Internet, and wireless network technologies like Bluetooth and Wi-Fi, as well as the expansion of smart gadgets and the myriad devices that make up the "Internet of Things." Cybersecurity is one of the biggest problems in the modern world because of its complexity in terms of politics and technology.

Cybersecurity began in the 1970s when researcher Bob Thomas developed the computer programme Creeper, which marked its path by leaving a breadcrumb trail as it moved throughout the ARPANET network. The programme Reaper was created by email's creator, Ray Tomlinson, and it chased and removed Creeper. Reaper, the first computer worm ever, was also the first instance of antivirus software and the first self-replicating application. Commercial antivirus initially appeared in 1987, despite conflicting claims over who invented the first antivirus product. In 1987, Andreas Lüning and Kai Figge launched Ultimate Virus Killer, their first antivirus programme for the Atari ST. The original version of the NOD antivirus was developed by three Czechoslovaks in the same year that John McAfee launched McAfee in the US and made VirusScan available. More people started posting their personal information online as the internet became more widely used. As a possible source of income, organised crime groups began stealing data from citizens and governments online. By the middle of the 1990s, network security threats had grown tremendously, necessitating the mass production of firewalls and antivirus software to safeguard users. Beginning in the early 2000s, organised crime groups began to heavily invest in funding professional cyberattacks, while governments started to crack down on the illegality of hacking by handing out increasingly harsher punishments to those responsible. Sadly, viruses also grew in number as the internet expanded, despite the fact that information security continued to progress. The cybersecurity market is still expanding at a breakneck pace. According to Statista, the size of the worldwide cybersecurity market is expected to increase to $345.4 billion by 2026. One of the most frequent dangers to the data security of any company is ransomware, and its prevalence is expected to rise.

2. LITERATURE REVIEW

2.1 Cybersecurity

The most recent security technologies may be expensive to implement and may not be very helpful if users are not properly instructed or trained (Singer and Friedman, 2014). An IBM report from 2014 states that 80–90% of recent cybersecurity failures are the result of organisational and human failings. Users must be taught to adopt safe online habits and security precautions as security incidents continue to increase in cost and frequency. The best cybersecurity investment a company can make, according to Disparte and Furlow (2017), is in better training. The strategic management of organisational knowledge and intellectual capital can benefit from including a cybersecurity awareness training programme. According to Nerdrum and Erikson (2001), either formal education or informal on-the-job training produces intellectual capital. Organisations must regularly provide cybersecurity awareness training for all staff in order to stop further data breaches to intellectual property (Anwar et al., 2017). According to Al-Awadi and Renaud (2007), awareness training is a crucial component of a successful information security implementation in an organisation.

To change the attitudes and behaviours of their employees and to instill in them a sense of responsibility for security, numerous organisations have put in place security awareness and training programmes (Thomson and von Solms, 1998). Many of these security awareness and training programmes have given staff members information on security standards, regulations, and policies for protecting data. Employees who receive cybersecurity awareness training are better equipped to recognise different security risks and threats. People who have received training, for instance, are less likely to abuse the resources of information systems (D'Arcy et al., 2009). Nevertheless, Rhee et al. (2005) found that merely being aware of the risks and threats does not appear to be enough to spur users to alter their current behaviour.

The chief information security officers are interested in learning how to improve cybersecurity education. According to Rhee et al. (2005), one's awareness of the personal risk of becoming involved in a bad security event is what really motivates one to take a precautionary and/or preventive action. People frequently underestimate the risks, so there is a difference between knowing a threat and responding to it (Schwarzer, 1994). Therefore, they believe that in order to encourage staff to take preventive and precautionary measures, an effective cybersecurity training programme needs to focus on how people perceive risk. They discuss a study they conducted to find out how different evidence-based cybersecurity training techniques affected employees' behaviour and perceptions of cybersecurity risk.

2.2 Cyberattacks

A number of institutions around the world have recently reported experiencing cybercrimes. Daily, there are over 20 significant cyberattacks. The Wannacry incident serves as a good illustration. Several people, public organisations, and private institutions could be harmed by a single cyberattack. Due to our dependence on technology, the threat environment is currently growing alarmingly. New strategic opportunities and threats brought about by the emergence of cyberspace have prompted a rush to establish dominant positions. Building an organization's competitive advantage in the private sector and fostering trust in both the public and private sectors both depend on its online reputation. The term "online reputation" is becoming more common, according to studies that are currently available. In order to define online reputation, Barnett, Jermier, and Lafferty (2006) took into account three different factors: stakeholder opinions and beliefs, intangible financial resources, and in-depth institutional knowledge. In their 2015 paper, Dijkmans, Kerkhof, and Beukeboom defined cyber reputation management as "the process of positioning, monitoring, measuring, talking, and listening as the organisation engages in a transparent and ethical dialogue with its various online stakeholders." As well as focusing on various facets of cyberspace, other researchers have. Anderson (2013) used secondary data to investigate the financial costs of cybercrime for the UK economy. The study excluded computer-integrity crimes and calculated costs for cybercrime actions for which data were available, which were primarily frauds. A national information security breaches survey that had been repeatedly conducted since 2004 was built upon, according to Klahr (2017), by conducting an annual cybersecurity breaches survey for the UK government. Less than half of the businesses, according to the study, experienced at least one cybersecurity breach. By outlining a conceptual framework and applying it to Belgium, Paoli, Visschers, and Verstraete (2018) investigated how cybercrime affects businesses. For cybersecurity services, Kilinc and Cagal (2016) proposed a reputation-based trust centre model to identify both malicious and insufficient information sources. Furthermore, if there is only unique information about the target, the attack benefits a firm's industry rivals.

Cybercrime is on the rise as a result of more advanced technology (Soumyo, 2004; Sabillon, 2016; Kennedy et al., 2019; Chandra and Snowe, 2020; Buil-Gil et al., 2021), and it has a daily impact on international trade (Zheng and Albert, 2019; Hassija et al., 2020). In order to reduce the risks associated with it, governments, organisations, and companies of all sizes must prioritise protections against it (Bambauer, 2014; Brookson et al., 2016; Pandey et al., 2019; Simon and Omar, 2019; Li and Xu, 2021). Cybercrime is a more comprehensive term defined as "illegal acts that target or use computers, computer networks, or networked devices" (Dashora, 2011; Choo et al., 2021). Cyberattacks, a subset of cybercrime, are more targeted and refer to specific attacks performed using new technology. They are an intentional and hostile attempt by a person or organisation to access another person's or organisation's information system. According to Lindsay (2015) and the Cisco Annual Cybersecurity Report (2020), 53% of hacks result in damages and other negative repercussions totaling more than US$500,000. Technology is used in cybersecurity to safeguard data (Darko and Boris, 2017; Colajanni et al., 2018; Li and Xu, 2021).

Cyberattacks continue to garner a lot of attention globally. A Google search for "cyberattacks" in July 2021 produced 19 million results. The author, citing Fosso Wamba et al. (2018), describes a rise in interest in the subject, which is shown by Google Trends, which lists Singapore, the United States, Canada, the United Arab Emirates, and the Philippines as the top five nations with more interest in the issue between 2010 and 2021. In recent years, a number of researchers have concentrated on cyberattacks. Urquhart and McAuley (2018) focused on the security of industrial objects from internet threats, whereas Ariffin (2021) concentrated on cyberattacks leveraging internet access. Levy (2021) discussed how cyberattacks are concentrating on people or small businesses that are components of larger businesses.

There is increasing pressure on organisations to protect the security of their intellectual property as a result of the introduction of revolutionary technologies like artificial intelligence, machine learning, cloud computing, big data, and IoT. Cyberattacks and data breaches are reported almost daily, so organisations are under more pressure than ever to ensure the security of their intellectual property. The actions taken by an organization's staff to avoid or reduce information security incidents determine how effectively it can manage intellectual capital. Though it is not an easy task, creating a strong cybersecurity defence. Every employee has a responsibility to do their part in protecting the company because people are the weakest link in a cybersecurity chain, so they need to be provided with the necessary security training and resources.

3. DISCUSSION

Cyberattacks have arguably garnered more regular media coverage in recent years. The Office of Personnel Management was the target of a significant hack in 2015 that exposed the personal data of 21.5 million people. According to David (2015), his incident exposed significant data breaches in the USA and raised the issue of cybersecurity in the public eye. Even more recently, at least 200,000 people across 150 countries were affected by a severe cyberattack on healthcare organisations. As more cybersecurity problems emerge in both public and commercial organisations, worries are growing. According to Fouad (2021), he extent of the harm that cyber security risks can have on the operation of education has been demonstrated in recent years by a number of malicious cyber incidents against educational institutions, whether in the form of monetary losses, the cancellation of classes and exams, or significant breaches of student and staff data. Financial institutions, shops, hotels, restaurants, transportation, and a number of other businesses are now common targets for cyberattacks. According to research, cybercrime has significantly increased since 2014, and each incidence results in damages of at least $2 million (Walters, 2015). A Rosen Hotels and Resorts data breach event in 2016 cost the business more than $2.4 million in damages and legal claims from credit card issuers and clients (Hertzfeld, 2017). As a result, concerns about cyber risks and information security have grown among consumers and commercial organisations alike.

The growth, frequency, and sophistication of cybersecurity assaults, particularly those utilising social engineering techniques like phishing and malware, make it difficult to establish a strong cybersecurity defence. However, the solution to the problem is according to Chatterjee (2019), organisations should not only provide their employees with adequate security training and resources, they should also establish and uphold a culture of security awareness as people are frequently the weakest link in an organisation's cybersecurity chain. Without continuing human training, the most recent security technologies are unable to prevent or mitigate cyberattacks. As more employees fall for phishing scams and improperly set up servers, a recent IBM (2019) analysis reaffirmed that human errors continue to facilitate security breaches. Adequate staff training addressing safe online behaviour and security countermeasures remains the cornerstone of businesses' cybersecurity strategies as security events continue to increase in number, sophistication, and expense. Stronger security training for staff is suggested as the optimal cybersecurity investment by Disparte and Furlow (2017). To increase staff readiness and awareness, businesses must invest in cybersecurity awareness training (CSAT).

According to Aldawood and Geoff (2020), the majority of businesses have weak cybersecurity procedures in place and unprotected data, which leaves them open to security breaches. The issues could be addressed with the aid of cybersecurity awareness programmes, prevention measures, and the creation of a cybersecurity culture. Binwal (2015) argued in favour of a framework for cybersecurity governance that emphasises the essential elements of a governance structure. A cybersecurity framework actually includes a complete set of management tools, an all-encompassing risk management strategy, and a security awareness programme that applies to every employee in the organisation. In order to educate and train teleworkers to be able to recognise potential threats, Abukari and Bankas (2020) agreed that security awareness programmes are essential. In order to combat cybercrime, teleworkers, businesses, and governmental organisations must be extremely watchful and collaborate.

3.1 Cybersecurity training methods

3.1.1 Malware Report

According to Etsebeth (2007), malware is defined by Grimes (2001) as "any software programme designed to move from computer to computer and network to network in order to disrupt, damage, or obtain unauthorised access to a computer system. The term can refer to viruses, Trojan horses, worms, script attacks, and malicious internet programming. Previously, the term "malicious mobile code" had a limited meaning that included just viruses, Trojan horses, and worms. However, as technology has advanced and the sophistication of current malicious mobile code has increased, the definition and use of the term has been widened to cover "all harmful programmes developed through scripting language and powered by internet technologies." As previously stated, malware poses a very serious threat to corporate information assets, resources, and systems due to its ability to infiltrate firewalls, hijack Virtual Private Networks (VPNs), and bypass digital signatures (Tipton and Krause, 2000). Malware is currently the most prevalent form of security failures, and it can cause organisations to incur and suffer the following sorts of damages and losses: direct harm, indirect damage, and psychological damage.

The most prevalent malware types on the network and a variety of malware that had been attacking two university campuses' networks for two years were found using industry-leading anti-malware tools from FireEye and Wedge Networks. In order to identify the most frequent malware attacks on the networks, malware frequency and type were tracked. Further details about these malwares were then gathered from online sources. The reports on the most frequent malware attacks were created using the findings. The most frequent malware attacks on campus networks are described in the report for the readers' information.

3.1.2 *Training Videos*

To help staff members improve their cybersecurity-related knowledge and self-efficacy in handling malware attacks that are relevant to their organisations, over 30 e-learning malware videos and reports based on the key types of malware attacks identified have been created. As a result, they were able to recognise typical malware that affects their employees' computers. We then produced some e-learning videos along with pertinent reports for the malware that was chosen, such as Trojan, malicious URL, SQL injection attack, ransomware, and Win Adware Agent. The malware videos and reports for each attack explain what the malware is, how it affects the computer or network, how it is transmitted, what the consequences are, how to remove the malware, and how to prevent it. The e-learning video provides an overview of each attack, explaining the malware, how it affects the computer or network, how it is transmitted, what the consequences are, how to get rid of the malware, and how to prevent it.

3.2 *Applying laws and adopting policies*

The difficulty of applying laws and adopting policies to support and implement security principles is comparable to the technical struggle to protect information and computer systems from an attack or compromise. Governments have a responsibility to defend their citizens against harm in the real world, and the military and police carry out this duty. The civil law offers a remedy if there is harm between people, including corporations. The obligations and remedies, however, are not always clear-cut in the cyberspace environment. Proactive prevention, rather than capture or remedy, is also becoming more crucial. Governments and private organisations are required to work together in order to prevent intrusions before they happen and to assist the police in apprehending suspects when necessary because of the interconnected network of public and private networks and the private ownership of critical infrastructure in many countries. Cyberspace threats arise in a networked environment where an attack may be launched from one nation while still causing significant harm to systems, people, and property in other locations; as a result, it is challenging to attribute blame, and obstacles are created by national boundaries when trying to hold the offenders personally accountable. As a result, choosing prevention over dread and treatment becomes much better.

4. CONCLUSION

Cybersecurity and the prevention of cyberattacks are ongoing problems that demand ongoing attention from both the public and private sectors. However, recent voluntary and mandatory legislation to fight cybercrime and maintain a safe electronic environment prioritises the significance of private sector security. Private sector businesses must remain aware since both their own interests and the interests of the networked environment depend on it. It is no longer enough for them to wait for the enforcement of laws against cybercrime and computer intrusions while remaining passive. Moreover, cyberattacks and breach of security at the national and business levels are becoming more severe and widespread. In the cyber arena, the traditional method of a government defending its population, including businesses, against unlawful and criminal actions is insufficient. The cost of cyberattacks, attribution, and worldwide enforcement challenges make prevention more vital than law enforcement and remedies. Cybersecurity and cyber threat defence are ongoing issues that demand constant concern from both the public and the private sectors. However, the relevance of private sector security is at the forefront of current voluntary and required policies aimed at combating cybercrime and ensuring a trustworthy electronic environment. It is no longer adequate for private sector enterprises to sit on the side-lines and wait for cybercrime and computer intrusion laws to be enforced; their own self-interest, as well as the interest of the networked environment, requires their vigilance.

Acknowledgments: This research was partially supported by University Technology MARA Kelantan Branch, Malaysia

References

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (smes). Information & Computer Security, 27(3), 393–410. https://doi.org/10.1108/ics-07-2018-0080

Chandna, V., & Tiwari, P. (2021). Cybersecurity and the New Firm: Surviving Online Threats. *Journal of Business Strategy*, *44*(1), 3–12. https://doi.org/10.1108/jbs-08-2021-0146

Chigada, J., & Madzinga, R. (2021a). Cyberattacks and threats during COVID-19: A systematic literature review. *SA Journal of Information Management*, *23*(1). https://doi.org/10.4102/sajim.v23i1.1277

Etsebeth, V. (2007). Malware: the new legal risk. *The Electronic Library, 25(5)*, 534-542. https://doi-org.ezaccess.library.uitm.edu.my/10.1108/02640470710829523

He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2019). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital*, *21*(2), 203–213. https://doi.org/10.1108/jic-05-2019-0112

Malatji, M., Marnewick, A. L., & Von Solms, S. (2021). Cybersecurity capabilities for Critical Infrastructure Resilience. *Information & Computer Security*, *30*(2), 255–279. https://doi.org/10.1108/ics-06-2021-0091

McCarthy, D. R. (2018). Privatizing Political Authority: Cybersecurity, public-private partnerships, and the reproduction of liberal political order. *Politics and Governance*, *6*(2), 5–12. https://doi.org/10.17645/pag.v6i2.1335

Perera, S., Jin, X., Maurushat, A., & Opoku, D.-G. J. (2022). Factors affecting reputational damage to organisations due to cyberattacks. *Informatics*, *9*(1), 28. https://doi.org/10.3390/informatics9010028

Pérez-Morón, J. (2021). Eleven years of cyberattacks on Chinese supply chains in an era of cyber warfare, a review and future research agenda. *Journal of Asia Business Studies*, *16*(2), 371–395. https://doi.org/10.1108/jabs-11-2020-0444

Rahim, N. H., Hamid, S., Mat Kiah, M. L., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. Kybernetes, 44(4), 606–622. https://doi.org/10.1108/k-12-2014-0283

Von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information & Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ics-04-2017-0025

Xu, H., & Mahenthiran, S. (2021). Users' perception of cybersecurity, Trust and Cloud Computing Providers' performance. Information & Computer Security, 29(5), 816–835. https://doi.org/10.1108/ics-09-2020-0153

Yang, A., Kwon, Y. J., & Lee, S.-Y. T. (2020). The impact of information sharing legislation on cybersecurity industry. *Industrial Management & Data Systems*, *120*(9), 1777–1794. https://doi.org/10.1108/imds-10-2019-0536

Zhang, Z. (Justin), He, W., Li, W., & Abdous, M. (2021). Cybersecurity Awareness Training Programs: A COST–benefit analysis framework. Industrial Management & Data Systems, 121(3), 613–636. https://doi.org/10.1108/imds-08-2020-0462

Research Article

Business Information Ethics Disclosure

Noorauni Nabilah Ridzuan[1], Aifa Nabila Mohd Rahman[2], Nur Aina Natasya Mohd Zambri[3] and Nur Ainatul Mardiah Mat Nawi[4,*]

[1] Universiti Teknologi Mara Kelantan Branch; 2020834968@student.uitm.edu.my; 0009-0004-7621-941X

[2] Universiti Teknologi Mara Kelantan Branch; 2020496206@student.uitm.edu.my; 0009-0004-4366-8518

[3] Universiti Teknologi Mara Kelantan Branch; nurainanatasya.mz@gmail.com; 0009-0001-9279-8018

[4] Universiti Teknologi Mara Kelantan Branch; ainatulmardiah@uitm.edu.my; 0000-0002-5868-4535

[*] Correspondence: ainatulmardiah@uitm.edu.my; 014-5142921.

Abstract: *Ethics is crucial for businesses to employ since it can come in handy in decision-making processes about what is right or wrong, it educates about how to act in a particular situation and creates a judgment to indicate better choices. Given that ethics appears as a code of conduct, it is intended to be agreed upon and adopted by all businesses. The issue that seeks to be addressed in the paper is to conceal the business's concern with the set of principles that determines the bounds of acceptable action (ethics). The paper aims in disclosing the issues from real cases and strategies to gain outstanding ethics in managing business policies and practices. Impacts towards the paper could lead to better awareness for the business in applying appropriate ethical aspects to their practices. The study discovered that social entrepreneurs, employment contracts, and corporate governance all encounter ethical issues while carrying out their duties. The researchers give solutions that can assist businesses in implementing effective ethics.*

Keywords: ethics; business; social entrepreneur; employment contract; corporate governance.

DOI: 10.5281/zenodo.8181201

1. Introduction

Ethics instructs people how to behave in certain circumstances and helps them make decisions that have advantages for them personally. Not to be mistaken with laws, a society's moral code is made up of a number of interconnected laws that together convey the ethical principles that underlie society. Moreover, ethics comprises guidelines and principles that inform people to behave properly. The breach of ethics may result in unclear or no punishment or penalty since no restrictions to it. Over the past 10 years, businesses have paid increasingly more attention to encouraging moral and responsible digital design (Truax, C., Orchard, A. & Love, H. A., 2021).

In contrast to information technology, ethical concerns have had a positive and negative impact on business. First and foremost, spam email marketing offers the business the opportunity to communicate with millions of partners, organisations, and stakeholders globally at a very low cost. Employees, representing an important resource of any organization (Mehrotra,A. & Mariam, S., 2020), may also be observed at work while having access to their email and the Internet. The benefits make it possible for staff to balance their need for privacy and autonomy with the management of key corporate resources and working hours. On the other hand, the bad side of complying with ethical issues in information technology could include the case where the hackers could break into databases of financial and retail institutions to steal customer information, then use it to commit theft by opening new accounts and charging purchase to unsuspecting victims. Students around the world have been caught downloading materials from the Web and plagiarizing content for their term papers. After all, only industries with core competences can effectively govern ethical and legal decision-making processes in their environment (Dhirani, L. L., Noorain Mukhtiar, Chowdhry, B. S., & Newe, T, 2023).

2. Method & Material

The researcher is using the literature review method for this study. Research papers were observed and analysed. The research papers being referred to were precisely and strictly filtered according to the narrower aspect of ethics relating to business whereby the issues and strategies that appear to course from real cases. Moreover, in getting a more accurate journal to refer to, the researcher applies the Boolean research method. In delivering the arguments on the case, the researcher conceptualized the different parties to issues related to ethics on business including social entrepreneurs, contract employees and corporate governance. Then, there are strategies that could lead to better ethical development for business.

.

3. Findings

3.1 Ethical challenges that businesses are facing with examples from actual cases

The researchers came across the fact that the implied ethical practices of various businesses varied. The significance of indicating them in the first place could enhance the business' working environment, as employees would feel more at ease accomplishing their duties in such a controllable ethical setting. Recently, the need for job seekers is more focused on a positive and healthy work environment, which implies the necessity for ethical procedures. Employees, on top of that, have the right to demand an exceptional business for putting their efforts and attention, spending daylight and night in, since choices are always accessible. Businesses are responsible for managing their employees' satisfaction with the ethical sides of their work environment in order to create excellent outcomes for the business and, most importantly, to secure their success. Employees in one business surely differ and sort in a variety of manners depending on their work of expertise. However, the remainder of this section aims for three parties with their own challenges faced in regard to ethical issues which include, social entrepreneurs, employment contracts and corporate governance.

3.1.1 Dilemmas faced by social entrepreneurs in addressing social and commercial missions

For the first challenge, it seems that many perceive social enterprises as a moral alternative to businesses (Bhatt, 2022). To support their operations, social entrepreneurs engage in economic activities to address difficult societal challenges. Since the interference demand from top management, stakeholders, and partners might flip everything completely upside down, the commercial department's scope of work is heavier than anyone could ever assume. The employee in charge was required to construct appropriate, efficient, and effective commercial procedures in response to the demands of today's customers and technology diversions. With so many rivals, being inventive alone will not suffice to win the market. Platforms for commercials are also necessary for reaching the proper target market.

In order to accomplish their social and economic goals, social entrepreneurs must overcome obstacles such as those linked to community engagement and juggling a variety of stakeholders. The study by Hota P.K. et. al (2023), with the aim of explicating, refining, and complementing the emerging theory of ethics in social entrepreneurship using 36 months of an ongoing qualitative and inductive study, of a SE (Alpha), those businesses in Uttarakhand, a rural area of India, provided the arguments for the challenges mentioned. The study's arguments will be outlined and suggested for better instances of business challenges involving the ethical component. In this specific case, the researchers aim to validate the moral conundrums that the study team, Alpha, known also as the social entrepreneur, has with respect to the rural Indian community.

a) Challenges in engaging the community

Entrepreneurs are expected to be prominent in the community since they can produce and invent new ideas, services, and business procedures, plan and establish a business based on their new ideas, and identify market possibilities. The Alpha team, as the social entrepreneur, had challenges involving the community in their full collaboration in managing social-commercial conflicts in this setting. First and foremost, in selecting beneficiaries, it was assumed that the community studied had limited and varying levels of access to resources. In comparison to small farmers, large farmers appear to enjoy higher revenue and assistance from other beneficiaries. Furthermore, if the Alpha team included women, sustainable development goals may be accomplished. However, due to gender inequality and patriarchal traditions, women are excluded from decision-making processes linked to farming and are either landless or own a small plot of land. Second, the absence of livelihood options in the communities where they were operating presented the Alpha team with moral conundrums in their scaling choice, which prevented them from fulfilling their social purpose or resolving their social-commercial goal.

The lesson learned from the findings obtained for the social entrepreneurs' first challenge in engaging the community in achieving their goals includes the limitations for the business in achieving their goals due to humanity's struggles, the culture they implied, and the environment they are exposed to. The business must identify more accurate ethical practices that are appropriate for its corporate goals. The rules followed by their target market will also have an impact on the business's ethics. After all, business ethics should be beneficial to the community in the geographical areas.

b) Challenges in balancing diverse stakeholders

In the context of the Alpha team trying to get the trust of a variety of stakeholders, there are some challenges they went through and most of them seem as if they could not be solved. The thinking between businesses or teams with their stakeholders definitely differs since the concept consists of many thinkers. It forms a combination of ideas from many experts. On top of that, knowing the importance of stakeholders to the business, mainly are increasing the chances of project success and broadening the pool of people who care about the well-being of your company.

According to the real case research, the Alpha team, known as a group of social entrepreneurs once again highlighted the challenges they faced while balancing social-commercial tensions which is in balancing diverse stakeholders. In summary, community members, angel investors, and government policymakers, as their stakeholders, are the ones that decided on providing resources and support to Alpha. On the other hand, the report said they were only interested in social impact stories, and less concerned about Alpha’s data-driven approaches in the first place. It is best to conclude that the study thought about the importance of knowing the differences between ethics of justice and ethics of care. The differences are as follows;

Table 1. The difference between ethics of justice and ethics of care.

Ethics of justice	**Ethics of care**
Suggests that while making decisions, an organization should depend on formal logic and unbiased judgement.	Suggests that ethical decision-making is influenced by the narrative and contextual intricacies of interpersonal interactions.

3.1.2 Legal issues relating to employment contracts.

Work done for another person that is expected to be done just for remuneration under the conditions of an employment contract is known as "conducted within the terms of an employment contract." Both parties' interests are protected by the employment contract. An agreement not to compete may be included in the employment contract by the employer to prevent the employee from using sensitive information for personal gain. In actuality, a strong work ethic triumphed over knowledge, training, and effort. This demonstrates the growing significance of work ethic in the employment process. The Bureau of Labour Statistics (2019) listed the activities of a human resource professional as recruit, screen, interview, and place workers.

The leadership of the workforce shifted as mills and factories expanded quickly from focusing on craftsmanship to maximising productivity. Cycles of long, uninterrupted workdays and feverish activity were countered by economic downturns and an increase in unemployment. There are moral requirements for all government contracting activity in the procurement regulations. When asked to sign a non-compete or non-disclosure agreement on the "take it or leave it" premise, employees may assume this is unethical because they aren't given any negotiating leverage. An organization's reputational value is taken into account while estimating its worth. Non-compete and confidentiality agreements' worth.

Most employment agreements aren't intended to be long-term. Even if an employment contract only lasts for a short time, there may be circumstances when both parties need to end their job connection.

Problems arise from employment contracts is lack of willingness. This problem is typically caused by higher-ranking workers abusing their power. In one of the real-life instances, Ms. Druyun, a Key Administrator, recruited the Boeing Company by giving the maker of aeroplanes significant contracts in order to secure work for herself, her daughter, and her daughter's fiancé (later son-in-law). She sent Boeing sensitive information from other companies in an effort to obtain a new job after she retired, and Boeing utilised it in their offers. Due to her acts, her accomplice was also imprisoned, and the president of Boeing resigned as a result. Boeing-related contracts are still being looked into. Actually, a $615 million deal with the US Government on ethical complaints, in major part, For the second quarter of 2006, Boeing recorded a loss of $160 million. She was the team member who understood the rules for the government contracting game the best. When faced with hiring someone who also offers a serious hazard due to unethical behaviour, Michael Sears, a former criminal who donated his knowledge and experience to the business, became the private sector example of what not to do.

3.1.3 Bribery and Corruption in business ethics

Offering, giving, receiving, or soliciting something of value in order to influence the behaviour of a person in a position of power constitutes bribery and corruption, both of which are immoral acts. Individuals, businesses, and society may suffer significantly as a result of these activities. In terms of corporate ethics, bribery and corruption damage trust, impair fair competition, and impede economic growth. These were considered to be the largest corporate governance scandals. Decision-makers, according to Petrick and Scherer (2003), had disregarded integrity's importance, nature, and potential.

Most nations consider bribery and corruption to be crimes, and they frequently have laws specifically prohibiting them. In Malaysia, The Malaysian Anti-Corruption Commission Act 2009 (the "MACC Act"), which was passed to establish the Malaysian Anti-Corruption Commission and to make additional and improved provisions for the prevention of corruption as well as for matters necessary and related thereto, is the main piece of legislation that governs bribery and corruption in Malaysia. The Anti-Corruption Act of 1997 has been replaced with the MACC Act. Its purpose is to encourage the honesty and decency of public and private sector management and to inform the public, public officials, and public authorities about corruption and its negative repercussions.

Rest (1986) defined moral awareness as an interpretive process through which people can identify difficulties that are real and related to specific situations. It is strongly tied to how one's conduct is formed. Religions or beliefs that place a great emphasis on morality will have a stronger moral foundation than others (Ward and King, 2018). There are various forms of bribery and corruption in business. Here are some examples of bribery that involves in business such as petty bribery.it involves small-scale payments to people in low-ranking positions to hasten the completion of routine activities or obtain essential services. Next is Grand corruption: Involves widespread acts of bribery at the top of the political or business food chain to sway crucial choices, agreements, or policies. Next is facilitation payments. It is when payments are paid informally to speed up or guarantee the completion of mundane tasks, frequently in nations with excessive bureaucracy. Another thing is when a person in a position of authority demands a bribe under the fear of negative repercussions, this is called extortion. Last is kickbacks. It is an unlawful payment or perks offered in exchange for preferential treatment, such as choosing to award contracts or make purchases.

There are actual examples of corruption and bribery. The 2009 accounting fraud by the founder of Satyam provides evidence that such conduct is motivated by greed, ambition, and a desire for fame, money, power, and glory. The situation shows that it is urgently necessary to strengthen corporate governance, ethics, accounting standards, and audits. Next, White-collar crime is on the rise, which calls for strong and exemplary punishment as well as efficient law enforcement conducted with the proper attitude (Bhasin, 2013). Based on these issues, ethics plays a significant role in determining how a person behaves as a result of accounting. Systems can be purposefully created by accountants to change people's behavior. They also more often represent the idea that accountability includes factors like attitudes and how other people utilize information, in addition to straightforward measurement and aggregation (Hofstedt and Kinard, 1970). Therefore, it is crucial to investigate accounting conduct and lessen deviant attitudes that influence subsequent behavior.

Bribery will also have consequences and an impact on business ethics. First, bribery gives those who are ready to pay an unfair advantage, undermining honest and open competition. Second is the impact on economic costs. Corruption can drain resources away from profitable endeavours, preventing investment and economic growth. Third is lack of legitimacy and trust. Public trust in institutions, both public and private, is eroded by widespread bribery, which also calls into question their authority. Apart from that it also causes a Social inequality. Resources meant for the general welfare may be exploited or diverted to benefit a select few people or organizations, which can worsen social inequities. Next is impaired development. Poverty, poor governance, and insufficient access to critical services such as education, healthcare, and other services are frequent problems in nations with high levels of corruption. It is crucial for people, companies, and governments to take a proactive approach against bribery and corruption in order to encourage ethical business practices. We can all work together to promote openness, responsibility, and a culture of honesty in order to promote equitable and long-term economic growth.

4. DISCUSSION

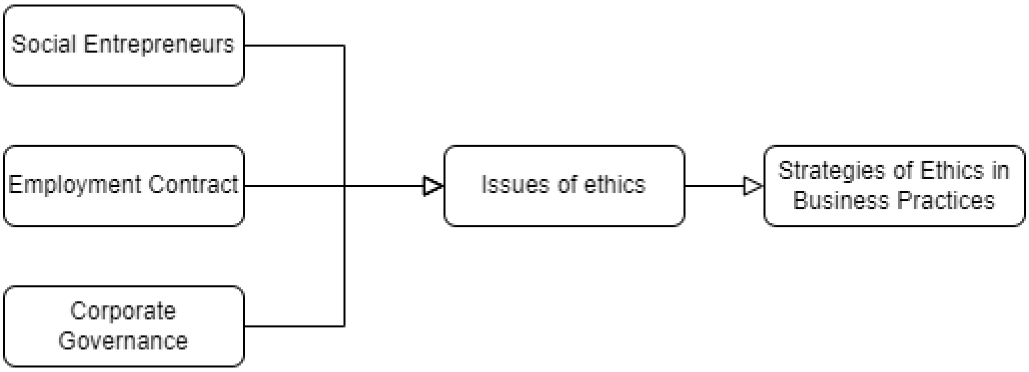


Figure 1. Conceptual Model

4.1 Strategies in applying ethics in managing business policies and practices

4.1.1 Applying idiosyncratic deals (i-deals)

In particular, everyone in the company, starting with the management, is required to devote great attention to ethical instruments aligned with the business in order to create influential and appropriate practices to operate the business. Employee satisfaction and organisational drive have an impact on the processes and viability of the business, consequently, customers could benefit from the strategic initiatives and customer service offered. Bal and Boehm, 2019, found a positive relationship between i-deals and customer satisfaction.

Effective and efficient ethics should be used to improve business performance. By using idiosyncratic (i-deals), voluntary, unique contracts of a nonstandard character are established with specific employees and their employers on terms that are advantageous to each side. According to Vizcaíno, F. V. et. al. (2023), when the workplace has a high ethical standard, employees are prone to believe that negotiates were given to those that deserved and earned special treatment. I-deals include schedule and task agreements, which can benefit both the employee and the business at large (Rosen et al., 2013). This explains why different sorts of arrangements are used in i-deals. Task i-deals are agreements formed between employees and their employers relating to changing the job's content or avoiding certain job responsibilities, whereas schedule i-deals refer to an employee's flexible daily work hours and focus on the employee's capacity to negotiate a flexible work schedule. After all, schedule i-deals and task i-deals may be advantageous to both the employee and the business in general.

4.1.2 Using code ethics in business organizations

A code of ethics defined as a distinct and formal document containing a set of prescriptions developed by and for a company to guide present and future behaviour on multiple issues for at least its managers and employees toward one another, the company, external stakeholders, and or society in general. (Kaptein and Schwartz, 2008, p. 113). When the company has a stated code of ethics, everyone is able to work the same rules in the organization, from the people at the top of the organisation, those in the executive suite, to the lowest member of the team. That also applies to consultants and contractors. A code of ethics helps in defining the company's identity and supports every aspect of its mission. The points of view from different stakeholders can be used to investigate the CE quality, as well as the employees of those stakeholders. As an example, an organisation that applies a code of ethics will be aware of the value of the document as a source of ethical culture and will be able to assess its potential impact on employees' ethical thinking and behaviour.

When employees are faced with a dilemma regarding ethics, it is their duty to Respond. The following decision-making model can be used to determine whether or not a specific course of action is "the right thing to do." Remember that doing nothing is an action in and of itself, and that action can have a negative impact on the Company and its personnel. Keep in mind that rushed decisions and work stress often have an ethical influence.

One of the factors affecting changes in corporate codes of ethics, may be seen in the coming together ability in the contents of codes of ethics (Berenbeim, 2000). The establishment of corporate subsidiaries throughout the world has forced the contents to be responsive to ethical issues on a more global scale.

A code of ethics established by professional licensing organisations must be followed by professionals like engineers, architects, and others. Licences may be cancelled by the giving organisation if someone does not follow the code, even though violations of these codes are not enforceable in court. As a result, professionals in many fields are held to standards of professional accountability in addition to the contracts they sign. The level of disclosure is another element of ethical standards that has been studied by researchers. In other words, an organization's attention to ethics and ethical issues can be judged by the accessibility its code of ethics is to all of its (Bondy et al., 2004).

4.1.3 Strong legal framework

Governments should pass comprehensive legislation that makes bribery and corruption illegal and guarantees that it is properly enforced. The legislation should apply to both the public and private sectors, and violators should face harsh consequences. A comprehensive set of laws, rules, and policies that control businesses' ethical behaviour and advance ethical and sustainable business practices is referred to as a solid legal structure in business ethics. It sets out a set of guidelines and requirements that companies must follow in order to ensure fairness, openness, and accountability in their operations.

Next is strong anti-corruption regulations and enforcement procedures should be a part of the legal structure in order to combat corruption in business. Along with whistleblower protections and procedures for reporting and looking into allegations of corruption, these laws might contain clauses that penalize bribery, embezzlement, money laundering, and other corrupt practices.

5. CONCLUSION

Business ethics encourages transparency, honesty, fairness, and integrity in all business interactions, both internal and external. It involves observing and maintaining the rights and well-being of all stakeholders, including employees, clients, suppliers, and other stakeholders. Businesses can develop strong relationships with their stakeholders and earn their trust by acting ethically, which will improve their reputation and increase customer loyalty.

In summary, businesses that are sustainable and profitable must stick to business ethics. Businesses can create trust, promote good connections, give back to society, abide by the law, and ensure their long-term success in an ever-changing business environment by respecting ethical standards.

Acknowledgements: We would like to express our profound gratitude to Madam Salliza Binti Md Radzi**,** our lecturer and Miss Nur Ainatul Mardhiah Mat Nawi, our supervisor and correspondence author for their guidance and contributions to the completion of our paper. In providing the budget to publish this paper, we are blessed by our institution, Universiti Teknologi MARA (UiTM) for their contribution. We are also grateful to all of those with whom we have had the pleasure to work during this and other related projects, our group members counting Noorauni Nabilah, Aifa Nabila and Nur Aina Natasya. Each of the members of our group has provided extensive cooperation to make this research paper a success.

References

Ahmad Sharbatoghlie., Mohsen Mosleh., & Taha Shokatian. (2013). Exploring trends in the codes of ethics of the Fortune 100 and Global 100 corporations. *Journal of Management Development, 32*(7), 675-689. https://doi.org/10.1108/JMD-04-2011-0044

Caniago, I., Yuliansyah, Y., Dewi, F. G., & Komalasari, A. (2023). Islamic work ethic in Behavioral Accounting. *Journal of Islamic Accounting and Business Research*. https://doi.org/10.1108/jiabr-05-2021-0152

Dhirani, L. L., Noorain Mukhtiar, Chowdhry, B. S. & Newe, T. (2023). Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. *Sensors, 23*(3), 1151. https://doi.org/10.3390/s23031151

Furlotti, K., & Mazza, T. (2020). Quality of code of ethics: an empirical analysis on the stakeholder employee. *Social Responsibility Journal,*16.(8), 1377-1402. https://doi.org/10.1108/SRJ-03-2019-0113

Gayton, M. C., & Lastname, F. M. (2008). Business ethics, restriction on employment and knowledge management. Legal Aspects Of Knowledge Management, 38.(2), 174-183. https://doi.org/10.1108/03055720810889815

Hatami, A., Hermes, J., & Firoozi, N. (2023). Moral laxity – the cognitive gap between true and pseudo corporate social responsibility. *Critical Perspectives on International Business*. https://doi.org/10.1108/cpoib-03-2021-0029

Hota, P. K., Bhatt, B. & Qureshi, I. (2023). Institutional work to navigate ethical dilemmas: Evidence from a social enterprise. *Journal of Business Venturing, 38*(1). https://doi.org/10.1016/j.jbusvent.2022.106269

Kumar, V., & Srivastava, A. (2021). Mapping the evolution of research themes in business ethics: A co-word network analysis. *VINE Journal of Information and Knowledge Management Systems*, *53*(3), 491–522. https://doi.org/10.1108/vjikms-10-2020-0199

Mehrotra,A. & Mariam, S. (2020). Leveraging of Social Media by Employers: Balancing Efficacy Against Ethics. *8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 442-446. https://doi.org/10.1109/ICRITO48877.2020.9197822

Mohammed T.Nuseir., & Ahmad Ghandour. (2019). Ethical issues in modern business management. Int. J. Procurement Management, 12.(5), 592-604.

Porter, G. M. (2005). A "career" work ethic versus just a job. Journal of European Industrial Training, 29.(4), 336-352. https://doi.org/10.1108/03090590510597160

Sahil Sholla, Roohie Naaz Mir &Mohammad Ahsan Chishti. (2020). Towards the design of ethics aware systems for the Internet of Things. *China Communications, 16*(9), 209-221. https://doi.org/10.23919/JCC.2019.09.016

Truax, C., Orchard, A. & Love, H. A. (2021). The influence of curriculum and internship culture on developing ethical technologists: A case study of the University of Waterloo. *IEEE International Symposium on Technology and Society (ISTAS),* 1-8. https://doi.org/10.1109/ISTAS52410.2021.9629124

Vizcaíno, F. V., Martin, S. L. & Jaramillo, F. (2023). The role of i-deals negotiated by small business managers in job satisfaction and firm performance: Do company ethics matter?. *Journal of Business Research, 158.* https://doi.org/10.1016/j.jbusres.2023.113697

Research Article

Emerging Trends in Cybersecurity: Issues in Cybersecurity During Covid-19 Pandemic

Siti Ubaidah [1], NorNadia Faqiani [2], Muhammad Iqbal Afiq [3], and Nor Erlissa Abd Aziz [4,*]

[1] Universiti Teknologi MARA; 2020862702@student.uitm.edu.my; 0009-0005-2062-7534

[2] Universiti Teknologi MARA; 2020862728@student.uitm.edu.my; 0009-0007-2190-3662

[3] Universiti Teknologi MARA; 2020459108@student.uitm.edu.my; 0009-0008-6795-1165

[4] Universiti Teknologi MARA; erlissa@uitm.edu.my; 0000-0001-9722-0947

[*] Correspondence: erlissa@uitm.edu.my; +447392832154.

Abstract: *The world is currently facing the COVID-19 pandemic, which is one of the most devastating global health crises of this century. It has affected approximately 10.7 million people worldwide and has caused significant disruption. One notable consequence is the rapid increase in remote work. Organizations also need to adapt to the new reality. However, this shift has exposed a critical concern that employees who work from home often have limited cybersecurity resources compared to organizations with dedicated security teams. This creates vulnerabilities, leaving employees far more vulnerable to potential cyber-attacks. Organizations need to prioritize the security of their dispersed workforce and implement robust cybersecurity measures to protect against these threats. Cybersecurity attacks have become a serious problem. The common types of cyber security attacks are Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, Man in the Middle (MitM), Phishing and Spear Phishing attacks, and Malware. Attackers have a clear motive when they target victims with obtaining their credentials or financial rewards. People who engage in online activities are exposed to numerous cyber dangers. This vulnerability arises from the network's inherent insecurity. Attackers possess the skills to exploit the flaws in the Internet's infrastructure, utilizing their coding expertise to their advantage. This research paper focuses more on discussions related to cybersecurity issues during the Covid-19 Pandemic.*

Keywords: Cyber security, Covid-19, Cyberattack, Cyber threats

DOI: 10.5281/zenodo.8181232

1. INTRODUCTION

The geography of the globe was promptly altered by the Internet, which first appeared as a platform for communication and exchange. Particularly, the 21st century has been and still is the century in which global geography and the Internet network are interconnected. As a result, the Internet allows for rapid global communication between people, and crucial commercial, political, economic, and cultural ties have been established between states. Computers, users, and networks are the three essential components of the Internet. It has been noted that network technologies have advanced because of the continually evolving computer industry and user segments that have begun to hold a variety of skills. However, the advancement and widespread application of network technologies has also resulted in serious problems with security. To secure the assets of institutions, organizations, and people, efforts have been undertaken to create a cyber security environment.

Networks with infrastructure information systems are referred to as "virtual reality" and are referred to as "cyber" in this context. Communication, life, integration, tangible and intangible assets, and data are all protected by cyber security measures in an electronic setting created by institutions, organizations, and people in information systems. In summary, cyber security guarantees the safety of digital existence on digital networks. Under the general heading of cyber security, the fundamentals of information systems' data integrity and confidentiality are protected. Securing personal and organizational data on the Internet is the main goal of cyber security. Ignorance of this crucial issue may pose major risks. (Omar, Semih, Merve, et al; 2023). Data theft, network, and computer interruptions, and other effects are caused by the attack. Attacks have also increased because of several other issues, such as the improper use of unmanned aerial vehicles. Attacks can be launched using techniques including phishing, ransomware, Denial-of-Services (DoS), and malicious software. An attacker's particular skills and the quantity of information they have about their victim both affect how successful their attack will be. (Mah Hui, Alya, Carin, et al; 2020).

2. LITERATURE REVIEW

2.1 Cybersecurity

Cybersecurity, also known as information technology security or electronic information security, is all about protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. Its ultimate goal is to safeguard these crucial components from unauthorized access, data breaches, and a wide range of cyber threats. To ensure the integrity, confidentiality, and availability of digital assets, cybersecurity relies on the implementation of preventive measures like robust security protocols, encryption, firewalls, and intrusion detection systems. (Kaspersky, 2023).

In today's rapidly evolving digital landscape, cybersecurity plays an important role in protecting the security, integrity, and confidentiality of various elements in the electronic environment. It serves as an important defense mechanism that protects communication, life, integration, tangible or intangible assets, and data in information systems. Institutions, organizations, and individuals rely on cyber security to create a robust and secure framework that effectively mitigates the risks posed by cyber threats. By implementing comprehensive cyber security measures, they ensure the smooth functioning and protection of their digital infrastructure. Protecting these critical components is essential to fostering trust, preserving privacy, and promoting the overall well-being of individuals and organizations in our interconnected world (Omar, Semih, Merve, et al; 2023).

Another definition of Cybersecurity is Cybersecurity is the protection of internet-connected systems such as hardware, software, and data from cyber threats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems (Sharon Shea, Alexander; Casey Clark, 2022).

2.2 Cyber Threats

In the digital world, cyber threats or also known as cyber security threats are malicious actions that aim to steal or damage data or disrupt the digital well-being and stability of an enterprise. Cyber threats include a wide variety of attacks from data breaches, to computer viruses, denial of service, and many other attack vectors (Raj Joy, 2023).

Another definition of cyber threat is that it refers to anything that has the potential to cause serious harm to a computer system. Also, a Cyber threat may or may not happen, but can potentially cause serious damage (Margaret Rouse, 2022).

2.3 Denial of Services (DoS)

A Denial-of-Service (DoS) assault could be a cyberattack that disturbs arrange frameworks with untrue demands for the reason of disturbing trade operations. The creator states that as a result of the assault, clients are incapable to perform scheduled assignments, such as getting to e-mail, websites, online accounts, or other assets worked by the influenced computer or arrange (Bart Lenaerts, 2023). In addition, this type of attack bombards target systems to intercept customer service requests, and it happened during the pandemic to slow down response to coronavirus cases. It can be launched from multiple malware-infected servers allowing attackers to take control of them (Khalid Hussain, Syed Jawad Hussain, et al., 2019).

2.4 Man in Middle (MitM)

A Man in The Middle (MITM) assault may be a general term when the culprit places himself within the discussion between the client and the application. The point of the assault is to take individual data, such as login accreditations, account points of interest, and credit card numbers. The target is as a rule clients of monetary applications, e-commerce locales, and other websites that require a login (Erez Hason, 2023). Next, this type of attack happens to be a threat to those who are working from home especially those without security guidance from their companies.

2.5 Phishing and Spear Phishing

Phishing is sending malicious emails designed to trick people into falling for a scam. Typically, the intent is to trick users into disclosing financial information, system credentials, or other sensitive data (Proofpoint, 2020). In addition, another definition of Phishing attack is phishing is a type of cybercrime where the targets are lured or tricked into giving up sensitive information, such as their Social Security Number and personally identifiable information and passwords (Alyssa Anne, Syukrina, Azween, et al., 2019). Phishing assaults imitate emails or social media joins from genuine sources in arrange to get individual data from a target. This sort of assault includes the naivety of human interest and specialized guile. Shapes of conveyance of phishing assaults are through emails that contain malware or join to ill-conceived websites or downloads.

Spear phishing is a type of targeted phishing attack that involves identifying the target and generating personalized messages tailored to the target. This makes education scams difficult to identify, combat, and prevent. Spear phishing can be done with cloned websites to get social media credentials or spoof emails by spoofing the source of the email (Alyssa Anne, Syukrina, Azween, et al., 2019).

2.6 Malicious Software (Malware)

Next is Malware. The short name for Malware is malicious software. Malware is an umbrella term for viruses, worms, trojans, and other malicious computer programs that hackers use to destroy and gain access to sensitive information (Josh Fruhlinger, 2019).

Malware is any undesirable computer program introduced onto a target gadget without the user's consent. Malware can utilize the gadget to spread to other gadgets by reproducing itself and covering up invaluable applications. There are numerous shapes of malware assaults counting, including large-scale infections, record infectors, ransomware, trojans, rationale bombs, etc (Jeff Melnick, 2023).

3. FINDINGS

3.1 Issues and Challenges

Cybercriminals are always developing their methods to accomplish their objectives as technology does. Human causes are the main cause of cyberattacks. individuals share knowledge online and with other individuals and organizations, making the most of their time to be as productive as possible. During the COVID-19 pandemic, people are susceptible to cyber security due to there is an increase in online activities including e-learning, working from home, online shopping, and others. It might be challenging for everyone to stay updated on new information regarding devices and internet safety in this highly technological digital environment. Additionally, users must make sure that all their devices, including PCs, i-Pads, and mobile phones, are up to date. However, most individuals prefer to ignore the message asking them to upgrade their device because they believe the updating process will be difficult and take up a lot of memory. The ease with which hackers can access their gadgets makes them vulnerable to cyber security (Home Instead, 2021).

Additionally, other issues in cyber security are there are many security bugs in software applications. During the COVID-19 pandemic, people are likely to download more software applications such as Zoom, Microsoft Teams, and Google Meetings. This is because hackers can create code based on weaknesses in software applications. Devices can be easily attacked if software applications have many unknown security features and bugs. Hackers wrap your code in malware and install it on your device. This makes their respective devices vulnerable and puts them at risk by using malware to attack software vulnerabilities. The device can then be compromised, and hackers gain unauthorized control of the device. They can access anything and steal the victim's information (Norton, 2019).

Another is cloud computing services ended up vulnerable to cybersecurity. It is because people depend on technology as well. The modern tech trend in computer systems is cloud computing. More companies than ever resort to this effective computing system and the amount of data facilitated on these cloud services is amazing. (Chandana, 2022). These days, users store their records on cloud services. Be that as it may, cyberattacks on cloud services have multiplied in 2019, making cloud services the third most focused on stage by cybercriminals right now. Users just not store records on cloud services but also passwords on their browsers for convenience. This facilitates users amid logins by auto-filling the accreditations after the user's confirmation. For case, Google Chrome allows users to save their passwords in his/her Google account. Upon successful login, all the passwords can be read. Thus, if the user's Google account is gotten by an unauthorized user, the unauthorized user will have to get to all his/her other accounts. Having a weak password and utilizing the same password over stages and applications are moreover exceptionally unsafe. Weak passwords can be effectively hacked in minutes. Typically, too why websites have made it compulsory for users to have a strong password that incorporates alphanumeric, special characters, and capitalization. These systems are a few of the juicier targets for modern-day hackers, as indeed a little breach of security can demonstrate sadly. To avoid any issues, businesses utilizing this system must continually discuss and request the finest security systems from their cloud service suppliers (Mah Hui, Alya, Carin, et al; 2020).

In addition, misleading data moreover makes people vulnerable to cyber security during the COVID-19 widespread. Attackers will attempt to trap an individual into giving them a few important data or their accreditations such as username, password, and credit card number so that the attacker can enter the victim's device and download malware in their device. The most common sort of phishing attack uses mail as its essential tool. Victims will get fake emails and on the off chance that they press on malicious joins, ransomware or malware can be installed in their devices. Phishing attacks are usually utilized to target individuals or organizations so that attackers can take advantage of them. This strategy will cause theft of individual information such as personality card numbers, addresses, account bank data, and so on.

3.2 Types of Cybersecurity Threats

One of the foremost common types of cyber-attacks is phishing and spear phishing attacks. Phishing attacks imitate emails or social media links from legitimate sources to get individual data from a target. This type of attack includes the naivety of human interest and technical deceit. Forms of conveyance of phishing attacks are through emails that contain malware or join to ill-conceived websites or downloads. Spear phishing could be a focused-on type of phishing attack, which includes surveillance of the target and making personalized messages that are significant to the target. This makes spear phishing troublesome to identify, protect and avoid. Spear phishing can be done with website cloning to get social media logins or mail spoofing by forging the root of the mail or sender's mail address. For example, we found phishing attacks generally centered around Personal Protective Equipment (PPE) and testing kits in March 2020, government jolt programs from April through the summer of 2020 counting a fake U.S. Exchanging Commission website that postured as the U.S. Of note, that from December 2020 to February 2021, vaccine-related phishing attempts increased by 530%, while those targeting pharmacies and hospitals increased by 189% during the same period. (Lucas Hu, 2021).

Another type of cybersecurity threat is Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. This type of attack is a target system to block service demands from clients, and it has happened during the pandemic to slow down response to coronavirus cases. It can be propelled from numerous machines that have been infected with malware that allows the attacker control over them. DoS attacks do not deliver the attacker a direct advantage unless the attack was propelled by a competitor or propelled to execute another type of attack. There are numerous ways to execute a DoS attack, such as an SYN flood attack, tear attack, smurf attack, ping of death assault, and botnets. For case, the cybersecurity attack scene in 2020 was caused by the COVID-19 widespread. The report states that DDoS attacks proceed to be the biggest disturbance during the COVID-19 pandemic and within the predictable future. Also, the high volume of online shopping occasioned by the COVID-19 widespread led to expanded DDoS attacks during the Movement Control Order (MCO). (Alicia Hope, 2021).

4. DISCUSSION

Among the cyber security issues listed in the findings section are Phishing and Spear Phishing attacks and the next issue is A Denial-of-Service (DoS). But Phishing attacks are more and are the main issue that will be discussed. Phishing occurs when fraudsters try to obtain sensitive information or data from you by portraying themselves as a reliable source. Phishers use a variety of places to carry out their cyberattacks, including email, SMS, and phone calls. According to Security Magazine (2022), in the magazine's writing titled "More than 255m phishing attacks in 2022 so far". In the magazine, the authors stated that 23.6% was the rate of total phishing attacks recorded in the first quarter of 2022. The financial industry was the most targeted industry at that time. Furthermore, the magazine also stated that as many as 255 million phishing cases were recorded throughout the six months of 2022 (Nivedita James, 2023). In addition, there is a study conducted by the AICPA in 2018 stating that it is reported that almost 60% of Americans have been victims of fraud schemes and 26% have been exposed to email phishing scams (Clare Stouffer, 2022). According to a report made by Verizon, 2022 phishing is one of the main causes of data breaches which is often a major problem (Verizon, 2022). According to a report issued by the FBI, 2020 states that they received the highest number of internet crime phishing reports in 2020, with a total of 241,342 victims (Clare Stouffers, 2022).

In 2019, which is the middle of December 2019, the world was shocked by the news of the emergence of a new virus. The Covid-19 virus is the name given to this virus. According to sources from the World Health Organization (WHO), this virus started in the city of Wuhan, Hubei, China. So, the World Health Organization has decided to recognize that Covid-19 started on March 11, 2020 (WHO, 2020). Since Covid-19 is spreading all over the world and this also indirectly causes cases to increase from time to time. Governments all across the world have taken various measures to halt the spread of the virus. The example of Malaysia, which is no exception in facing this crisis, has taken steps by implementing the Movement Control Order (MCO). According to a source from Berita Harian, Tan Sri Muhyiddin Yassin, who was the Prime Minister at the time, had implemented the order to curb the spread of this epidemic from continuing to spread among Malaysians. The Prime Minister issued a Movement Control Order from March 18 to March 31, 2020. This Movement Control Order applies to the entire state and no one is exempt (Berita Harian, 2021).

After the emergence of the epidemic, we can witness the emergence of many cases of fraud, cases of phishing attacks involving individuals, organizations, or businesses. Next, according to the author, a study conducted by the NCSC (National Cyber Security Center), it was stated that they had received 350 cases of attacks involving phishing, online fraud, and more (Swissinfo, 2020). This case occurred in Switzerland in April 2020. The NCSC also compared the number before Covid-19 existed, which is on a normal day when only 100 to 150 cases were reported. As a result, Covid-19 has been labeled as the main factor in the increase in the number of cases in Switzerland (Cedric Nabe, 2022). This situation occurs because the work pattern during the Covid-19 pandemic has changed significantly where the government has ordered workers to work from home only and a person's movement is limited due to restrictions that have been ordered by the government (Cedric Nabe, 2022). Working remotely has a very low level of internet security and it's not like in the workplace which definitely has a high level of cyber security. Evidence can be seen through a study obtained by Swissinfo, 2020 in which it recorded as many as 47% of individuals who have been involved in phishing fraud syndicates while working at home. Phishers take the opportunity to further expand their reach by exploiting the weaknesses of workers who work from home. For example spreading fake news related to Coronovirus (Cedric Nabe, 2022).

5. CONCLUSION

To conclude the research, it is observed that cybersecurity is a field of study that should not be disregarded as we are moving towards an age of digital technology, such as Artificial Intelligence (AI), Blockchain, the Internet of Things (IoT), and the like. Nonetheless, some cybercriminals are more frequent and sophisticated. Cybercriminals are instilling fear into the population, becoming more assertive and fearless as cybersecurity is not enforced, maintained, and enhanced. E-mail phishing threats (Alawida, Omolara, Abiodun, and Al-Rajab, 2022) and vulnerability to cybersecurity threats (Chgada and Madzinga, 2021) are the most common example of cybersecurity attacks that occur every day and night during the COVID-19 pandemic. It is probably due to hackers being so busy launching different variants of cybersecurity attacks that can harm economic transactions and computer-based systems.

Even though many business owners, companies, and organizations have turned to digital security to ensure the longevity of their business, it is believed that many businesses ignore the threats of cybersecurity attacks, or cyberattacks during the COVID-19 pandemic and the total lockdown. Cyberattacks can be dynamic and affect all computer-based systems and the Internet environment by manipulating the attack format and target audience. The increase in cyberattacks is usually caused by different factors such as technical and non-technical reasons, the transfer of social life to the Internet environment, errors and vulnerabilities in software, and so on.

To efficiently and effectively protect computer-based systems from cyberattacks, extensive protection is required, such as technical solutions that significantly improve the ability to scan for data breaches, find vulnerabilities in computer systems and communication networks, and enhance the accuracy of attack detection systems, Although, there are still some issues and challenges to effectively detecting new and complex cyber-attacks. Meanwhile, overcoming the issues and challenges of cybersecurity attacks is especially important to enhance people's security in the future. Also, when experiencing the attacks firsthand, most business owners should take action on countering cybersecurity attacks, by owning a security policy, purchasing equipment or software required to maintain the security, hiring security professionals such as ethical hackers to perform penetration testing, and allowing administrators to modify sensitive information.

Acknowledgments: We would like to thank our lecturer for this assignment Mrs. Salliza Binti Radzi for providing us with useful information and guiding us until this project was completed. Thanks also for handling and giving invaluable guidance on how to write a report. We would also like to thank Mrs. Erlissa Binti Aziz our correspondent in our group.

References

Ahmad Kamal, A.H.; Yi Yen, C.C.; Ping, M.H.; Zahra, F. Cybersecurity Issues and Challenges during Covid-19 Pandemic. *Preprints.org 2020*, 2020090249. https://doi.org/10.20944/preprints202009.0249.v1

Eian, I.C.; Yong, L.K.; Li, M..Y.X.; Qi, Y.H.; Z, F. Cyber Attacks in the Era of COVID-19 and Possible Solution Domains. *Preprints.org 2020*, 2020090630. https://doi.org/10.20944/preprints202009.0630.v1

Aslan, Ö.; Aktu ˘g, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics 2023*, 12, 1333. https://doi.org/10.3390/electronics12061333

Ubing, A. A., Jasmi, S. Z. A., Abdullah, A., Zaman, N., & Supramaniam, M. (2019). Phishing Website Detection: An Improved Accuracy through Feature Selection and Ensemble Learning. *International Journal of Advanced Computer Science and Applications*, *10*(1). https://doi.org/10.14569/ijacsa.2019.0100133

Hu, L. (2021, March 24). Fake Websites Used in COVID-19-Themed Phishing Attacks, Impersonating Brands Like Pfizer and BioNTech. *Unit 42*. https://unit42.paloaltonetworks.com/covid-19-themed-phishing-attacks/#:~:text=We%20found%20phishing%20attacks%20largely,to%20steal%20user%20credentials)%20and

Hope, A. (2021, January 29). DDoS Attacks Increased Rapidly During the COVID-19 Pandemic as Hackers Exploited New Tools and Techniques. *CPO Magazine*. https://www.cpomagazine.com/cyber-security/ddos-attacks-increased-rapidly-during-the-covid-19-pandemic-as-hackers-exploited-new-tools-and-techniques/

Chandana. (2022). Cyber Security Risks in the todays Era of Digitalization. *Simplilearn.com*. https://www.simplilearn.com/cyber-security-8-vulnerable-risks-article#2_cloud_computing_services

James, N. (2023, April 3). *Phishing attack statistics 2023: The ultimate insight*. Astra Security Blog. https://www.getastra.com/blog/security-audit/phishing-attack-statistics/?utm_feeditemid=&utm_device=c&utm_term=&utm_source=google&utm_medium=cpc&utm_campaign=Dynamic%2Bads%2B-%2BCampaign%2B-%2BPentest&hsa_cam=17272935963&hsa_grp=153763431830&hsa_mt=&hsa_src=g&hsa_ad=660848984559&hsa_acc=8352936176&hsa_net=adwords&hsa_kw=&hsa_tgt=dsa-2082491362765&hsa_ver=3&gclid=CjwKCAjwsvujBhAXEiwA_UXnADzU9ak7Dm7uiv1WLJM809ZD11u7NTDIjNo9dc2N4HwiYJQMTLdQmxoCZN8QAvD_BwE

Cost of a data breach 2022. IBM. (n.d.). https://www.ibm.com/reports/data-breach

Cassetto, O. (2023, May 1). *Cybersecurity threats: Types and challenges*. Exabeam. https://www.exabeam.com/information-security/cyber-security-threat/

Shea, S., Gillis, A. S., & Clark, C. (2023, January 11). *What is cybersecurity? everything you need to know: TechTarget*. Security. https://www.techtarget.com/searchsecurity/definition/cybersecurity

Tessian. (2023, April 12). *Why we click on phishing scams - how to avoid being hacked*. Tessian. https://www.tessian.com/blog/why-we-click-on-phishing-scams/#:~:text=In%20a%20recent%20survey%20conducted,a%20phishing%20email%20at%20work

Roy, R., 23, L. U. A., Raj Roy opens a new window opens a new window Raj leads the editorial sponsorship, Raj Roy opens a new window, & opens a new window Raj leads the editorial sponsorship and premium content program at ToolBox. With over 8 years of experience in 360 digital marketing. (2021, August 23). *What is a cyber threat? What Definition, types, hunting, best practices, and examples*? Spiceworks. https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-cyber-threat/#_001

Margaret Rouse Margaret Rouse is an award-winning technical writer and teacher known for her ability to explain complex technical subjects simply to a non-technical, Rouse, M., Margaret Rouse is an award-winning technical writer and teacher known for her ability to explain complex technical subjects simply to a non-technical, Editor, April, L. updated: 25, & updated: L. (2022, April 25). *Cyberthreat*. Techopedia. https://www.techopedia.com/definition/25263/cyberthreat

What is a denial of service (dos) attack? – crowd strike. crowdstrike.com. (2023, April 21). https://www.crowdstrike.com/cybersecurity-101/denial-of-service-dos-attacks/

What is phishing? - definition, types of attacks & more: Proofpoint us. Proofpoint. (2023, May 29). https://www.proofpoint.com/us/threat-reference/phishing

Fruhlinger, J. (2019, May 17). *What is malware: Definition, examples, detection, and recovery*. CSO Online. https://www.csoonline.com/article/3295877/what-is-malware-viruses-worms-trojans-and-beyond.html

Alawida, M., Omolara, A.E., Abiodun, O.I., Al-Rajab, M. (2022). *A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University* - Computer and Information Sciences. Vol. 34 (10), pp 8176–206. doi: 10.1016/j.jksuci.2022.08.003. Epub 2022 Aug 11. PMCID: PMC9367180.

Chigada, J. & Madzinga, R. (2021). *Cyberattacks and threats during COVID-19: A systematic literature review.* SA Journal of Information Management, Vol. 23 (1). 10.4102/sajim.v23i1.1277.

Zerlang, J. (2022, July 20). *The Pandemic's Lasting Effects: Are Cyber Attacks One of Them? Forbes*. https://www.forbes.com/sites/forbestechcouncil/2022/07/20/the-pandemics-lasting-effects-are-cyber-attacks-one-of-them/?sh=9def68f2b76c

Lohrmann, D. (2022, August 21). *Hacktivism and DDOS attacks rise dramatically in 2022*. GovTech. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/hacktivism-and-ddos-attacks-rise-dramatically-in-2022

Author Cedric Nabe Partner cnabe@deloitte.ch +41 58 279 8090 . (2020, December 15). *Impact of covid-19 on Cybersecurity*. Deloitte Switzerland. https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

Kronologi Pelaksanaan FASA PKP | Nasional | Berita Harian - BH Online. (n.d.). https://api.bharian.com.my/berita/nasional/2021/01/775155/kronologi-pelaksanaan-fasa-pkp

Research Article

Protecting Against Cyber Threats: Strategies & Best Practices for Effective Cyber Security

Nor Zalikha Marzukaini[1], Nur Izatul Asma Abd Ghani[2], Nur Syamimi Zulkefli[3] and Meer Zhar Farouk Amir Razli[4, *]

[1] Universiti Teknologi MARA; 2020459034@student.uitm.edu.my; 0009-0007-9574-6233

[2] Universiti Teknologi MARA; 2020819166@student.uitm.edu.my; 0009-0004-0961-4743

[3] Universiti Teknologi MARA; 2020830748@student.uitm.edu.my; 0009-0000-4671-1316

[4] Universiti Teknologi MARA; farouk955@uitm.edu.my; 0009-0008-8849-336X

* Correspondence: farouk955@uitm.edu.my; 019-9846868.

Abstract: *This research article is titled Protecting against cyber threats: strategies & best practices for effective cyber security. This topic was chosen to be studied because the writer is aware that many people do not care about cybercrime and cyber security which is becoming more and more worrying today. The objective of the study in this research article is to examine the level of public awareness, especially those involved in the business field, of cybercrime and cyber security. In addition, the research of this article also aims to identify what types of cybercrime often occur as well as the correct steps or strategies to prevent yourself and your company from becoming a victim of cybercrime. This research method is implemented by searching for several reference articles in online databases such as Emerald Insight, EzAccess, Science Direct and also Google search engine. A literature review is a survey of academic books, journals, and other materials pertinent to a specific problem, field of study, or theory, and it offers a description, synopsis, and critical assessment of these works. The purpose of literature reviews is to show readers how your research fits into the greater body of knowledge and to give an overview of the sources you used to investigate a particular topic. This research article discusses the true meaning of cybercrime from the point of view of research analysts, as well as systematic ways to prevent this cybercrime from occurring. This writing is more directed to business practitioners which companies or industries will be more at risk of experiencing cybercrime cases. Today, hackers or criminals are smarter and more forward-thinking in their tactics to steal customer's personal data and make money with each stolen data. Furthermore, the type of cybercrime not only involves large industries, but ordinary Internet users are also likely to become victims of cybercrime. As a result, this research paper has a positive impact because it contains research findings that cover all aspects of cyber security and cybercrime.*

Keywords: Cyber security; cybercrime; business; Internet; aware.

DOI: 10.5281/zenodo.8181246

1. INTRODUCTION

In today's digitally-driven world, cybersecurity is a critical concern for individuals and organizations alike and has become a critical aspect of our lives. Cyber threats come in many forms, from phishing scams and malware attacks to ransomware and data breaches. The consequences of a successful cyber attack can be devastating, ranging from financial losses and reputational damage to legal liabilities and compromised personal information. It is essential to have strategies and best practices in place to protect against cyber threats effectively. This essay will also explore some of the most effective cyber security strategies and best practices, providing insights into how individuals and organizations can minimize their risks and better protect themselves against cyber threats.

2. METHOD & MATERIAL

This study uses the manner of a literature review. This type of research method is used to ensure the writer can complete this research article carefully because the previous study is used as a reference. The author uses scientific materials such as articles and information from relevant websites. All these materials are obtained from online database and Internet platforms such as Emerald Insight, EzAccess, Science Direct and Google search engine. The author used a total of 4 materials including articles and websites that are closely related to the topic studied by the author. This allows researchers to make comparisons and use these materials as a reference to complete their studies. Furthermore, this online content article and webpage has important content related to cyber security and cybercrime which gives researchers the opportunity to complete this study more easily and provide comprehensive understanding to researchers.

3.0 LITERATURE REVIEW

No matter what the discipline, the foundation of all academic research activity is developing research and connecting it to existing knowledge. Therefore, getting it right is crucial for all academics. This is the reason that using a literature review as a research approach is more pertinent than using earlier studies. This evaluation of the literature can be seen of as a more or less organised method of compiling and combining earlier studies (Baumeister and Leary, 1997; Tranfield, Denyer, and Smart, 2003). According to Webster and Watson (2002), studies and research techniques that are well-executed and efficient lay a strong foundation for knowledge advancement and the facilitation of theory building. A literature review will be used to address the research topic since it combines empirical data and viewpoints from numerous sources. The claim made by Tranfield et al. (2003) that a literature review is the best method for combining study results to demonstrate evidence at a meta level and tries to uncover Areas where more research is required is used to support this argument. This is important for developing the conceptual model and creating the theoretical framework. The conventional method of describing the literature is also less detailed and won't be applied consistently (Tranfield et al., 2003).

As researchers, we have conducted a literature review to help us better understand and add knowledge to this study. Cybercrime, according to Norton Security Symantec Corporation, is any crime that involves computers or the internet in some way (Norton, 2016). Deshmukh and Chaudary (2014) stated that the phenomenal growth in the use of trained people also increased the global spam rate, malware rate and phishing rate rapidly, bank account fraud as a cybercrime also increased at a higher rate. This is supported by Wavefront (2016) when the first account of cybercrime occurred in 1970 involving a teller at the New York Dime Savings Bank who used a computer to embezzle over $2 million in money. Julien (2016) also stated that the first spam email was sent through ARPAnet, the United States Department of Defense Network by a Digital Equipment Corporation marketing executive after 8 years had passed. Since the usage of computers has grown quickly over time, cybercrime has dramatically expanded. Threats from cybercrime to computer security can take many different forms, from quick attacks to extensive criminal activity.

Cybercrime has many incentives for hackers. A hacker is usually defined as a person who uses a computer "to gain unauthorized access to data" (Oxford Dictionary, 2018). According to Smith et al. (2011), cybercriminals are motivated by economic, personal, ideological, and structural factors. Hackers might see a chance to further their own interests or carry out personal revenge. Selling information that has been taken on the black market is another way that cybercriminals can benefit. Governments have engaged in cybercrime on a global scale. Cybercriminals frequently pick their victims carefully and scan the target for weak points. The eight cybercrimes listed above have one thing in common: most of the time, the victim must take part in some way for the crime to happen and to be effective. The victim is exposed to such attacks because they either comply with the request, engage with the perpetrator, or lack proper defences like anti-virus or anti-intrusion software. The importance of human behavioural aspects in preventing cybercrime is acknowledged in the literature (Hadlington and Chivers, 2018).

Conclusions made by Sarre et al. (2018) that the aspect of education is one of the best responses to cybercrime, especially education that provides exposure about victimization to them. This is supported by Cornish and Clarke (2003) because it is argued in their study a further understanding of crime prevention approaches that focus on self-protection by potential victims and help reduce the chances of crime that will occur. Sherizen (1991) states that there is an important socio-technical approach to the problem of computer crime. It needs to determine where the social and psychological line is drawn between normal and deviant and split into two poles of groups between them that cause mutual misunderstandings and perform unethical tasks. To build crime prevention activities based on evidence, effective and efficient actions in countering these cybercrime activities, it is necessary to understand the numerous hazards of online victimisation and crime prevention in the online context. Grabosky, 2001; Renys, 2010; Drew and Farrell, 2018).

4.0 FINDINGS

The findings of the study show that several reference articles use different content where each researcher has a different view on the definition of cybercrime, types of cybercrime and how to protect against cybercrime. Explanations related to other study findings are discussed in the paragraphs below.

4.1 Definition of cybercrime

Cybercrime is the term used to describe illicit behaviours carried out using digital technology or the Internet, according to the paper "The Effect of Cybercrime on Open Innovation Policies in Technology Firms." Data theft, hacking, identity theft, and the dissemination of malware or viruses are a few examples of these actions. Cybercrime can have major negative consequences for both persons and companies, including financial loss, harm to one's reputation, and disruptions of essential infrastructure and services. In order to defend themselves from cyber dangers, it is crucial for both individuals and businesses to employ appropriate cybersecurity measures. (Raten, 2019).

According to the article "A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies", cybercrime is any criminal action that is carried out through the internet or other digital communication technology (Jacqueline, 2019). This covers a wide range of unlawful actions, including cyberstalking, online fraud, identity theft, and hacking, among others. In the current digital era, cybercrime is a severe threat to everyone, including people, corporations, and governments.

Cybercrime is any criminal conduct involving the use of computers, networks, or the internet, according to the article "Examination of Cybercrime and its Effects on Corporate Stock Value". Cybercriminals may infiltrate computer systems to inflict harm or disruption, or they may steal sensitive information such as trade secrets, financial data, or personal information. The financial performance and reputation of businesses, as well as the people who are victims, can be significantly impacted by cybercrime (Smith, Johnson, Jones & Lawrence, 2018).

Cybercrime is defined as criminal activity carried out utilising digital technology including computers, smartphones, and the internet, according to the paper "Awareness towards cybercrime among secondary school students: the role of gender and school management." These actions could include, among others, online harassment, phishing, hacking, and identity theft. The essay also emphasises how critical it is to educate people about cybercrime, especially secondary school children, in order to safeguard them from harm and provide them the tools they need to make wise decisions online (Mudit Kumar Verma & Shyam Sundar Kushwaha, 2020).

4.2 Types of cybercrime

There are numerous forms of cybercrime that the general public may be aware of. Website fraud is one of the cybercrimes that are prevalent today and are frequently reported. Spoof is interchangeable with the words deceive, hoax, and trick. Website spoofing is the practise of creating a website that imitates another one in order to deceive users into thinking it is the real deal. This criminal behaviour is carried out to propagate harmful and malicious software, get access to user computers, steal data, or steal money. This dishonest practise is copying authentic websites and exploiting corporate branding, user faces, domain names, and corporate style to deceive people into entering usernames and passwords in a website without any scepticism or hesitation. This gives dishonest people a way to steal the data of every user, use it for nefarious purposes, and install malicious software on users' machines.

Ransomware is another typical form of cybercrime. Modern cybercrime known as ransomware occurs when hackers steal important data and demand a hefty ransom in return. It is sometimes referred to as the long-standing crime of extortion. This crime generally involves the encryption of a company's data and happens in the majority of enterprises. If this ransomware crime takes place, a company's business will be restricted or abruptly stopped, which will have several negative impacts including preventing people from performing their tasks and costing them their livelihood. In this case, without recoverable backup data, the business companies involved are generally at the mercy of attackers or criminals who will hold high-value data as hostages in exchange for currency and so on. Ransomware is becoming a criminal activity and should be a major concern in all organizations whether in the business industry or any type of industry. Based on recent research, ransomware breaches have increased by 13% over the past five years combined. For instance, are people more likely to use virus protection but less likely to utilise other cybercrime preventative measures if they have personally encountered a specific type of cybercrime, such as ransomware? Social media privacy settings that are relevant to their earlier victimisation should be kept in tact. What impact does the diversity of reported cybercrimes have on the application of crime prevention techniques? 2020 (Jacqueline).

The last type of cybercrime is IOT hacking. It is common knowledge that the Internet of Things is a brand-new era that bravely offers insights into the daily activities and commercial activities conducted by users online. All devices that have access to the Internet are gathering and exchanging data with one another whether the user allows this update or not. Data is valuable in this context, thus hackers and other cybercriminals would try to take advantage of any equipment that gathers it. If more users link objects to the Internet, hackers and other cybercriminals will have better opportunities and rewards. Thus, it's crucial that every user adopt security measures by enforcing passwords, whether they're for personal or professional use. Due to carelessness in failing to make the password more secure and other connected issues, it frequently happens that the user will lose all the crucial data kept on the device.

4.3 Strategies and best practices for cybercrime

One strategy for situational crime prevention that focuses on lowering the possibility of these crimes occurring is self-defence. Because the fast growth and progress of technology have opened various fields, new opportunities, and efficient resources for organisations of all sizes, we frequently hear that cybercrime may occur at any time and from any location, regardless of rank, age, or gender. Furthermore, the presence of the internet aided in the development of this technology. The truth is that the internet is a vital asset for the country, and national security is dependent on it. Self-defence, on the other hand, is one of the wisest techniques for avoiding being a victim of this crime. One of the best ways to protect oneself from this crime is to be cautious when using public Wi-Fi. We already know that internet users are extremely glad and delighted if wi-fi is available everywhere for the convenience of using the internet, but consumers are frequently dissatisfied because public wi-fi is one of the chances for thieves to steal our personal data without our knowledge or consent. Users should also encrypt and recover essential data. This is because hackers can carry out illegal objectives by copying vital information if users encrypt data stored on smartphones and laptops. The answer is to save as a copy and keep locally on an external hard drive that is only intermittently connected to a computer, such as in a cloud storage system, if the data is vital, such as medical information, or irreplaceable, such as family photographs.

According to Leukfelft (2014) and Miethe and Meier (1994), this is important to investigate the function of self-protection in reducing the harm of victimization because it provides an alternative that may be more effective to reduce the incidence of cybercrime. Among the strategies that are so effective in reducing the crime rate is to focus on these 25 strategies, Cornish and Clarke's situational crime prevention model can be used to fight this crime. Among the main tactics is to "increase efforts" surrounding crime. The strategy is to harden targets, control access to facilities, handicap offenders and controls/weapons. While to "reduce the reward" for committing this crime is to extend care, help natural supervision, reduce anonymity, use place managers and strengthen formal supervision. This risk-increasing strategy opens up opportunities for criminals to continue committing crimes. Then, this "diminishing reward" can hide targets, remove targets, identify assets, disrupt markets and deny benefits. The themes of "reducing provocation" and "eliminating excuses" can lessen anger and stress, prevent arguments, lessen lust and temptation, fend off peer pressure, and discourage imitation. In order to reduce target conformance in a number of classics like aggressive and sexual sorts, 25 strategies have previously been recognised in earlier work as one of the most effective approaches.

Furthermore, this cybercrime is one of the ones that is also at the top of the list. The authorities should collaborate with other federal departments and organisations, such as the Department of Homeland Security, to address this criminal issue. Aside from the Criminal Complaints Centre, the public is also informed of the presence of a number of procedures designed to make it easier for individuals to report any suspicious conduct to authorities. This is because the authorities are organisations that are extremely dedicated to combating cybercrime. Next, improving security, including employing personal data prevention methods to secure electronic devices such as user computers in terms of identification and transaction protection, is how to protect against cybercrime. One method is to always install or update antivirus and antispyware software and to be wary of downloaded files and fraudulent email attachments. To secure the firm's personal data, each company must have the best backup plan to protect the company's name by having a strategy to manage publicity and prepare comments for the media, and they must also be prepared to spend large sums of money during the repair and recovery phases. The corporation must, among other things, adopt strategic steps to protect the interests of the business and its many stakeholders, such as the owners of each share, customers, and the general public. Furthermore, if a firm encounters or is involved in cybercrime, it will have an influence through rumours that intend to tarnish the company's name.

Next, a wise user can avoid becoming a victim of the situation by participating in some way, i.e., either asking for something from the offender during a conversation or by being vulnerable to attacks and harassment due to a lack of protection, such as anti-virus or anti-intrusion software. If a victim does not react to a phishing email, for example, the fraudster cannot access their personal information. The virus cannot be installed on the victim's machine if they do not click on the offered link. Given this, it is important to comprehend the role of victims in cybercrime and, in particular, to look into the role of victims as a crucial component of stopping and preventing cybercrime.

5. DISCUSSION

The study carried out covers the awareness that needs to be taken into consideration regarding cyber security and cybercrime. This paper discusses what cybercrime is, the type of cybercrime that always occurs in today's society and also how to take good steps or strategies to prevent the occurrence of cybercrime that is becoming increasingly worrying today. Based on the findings, it can be known that a large number of people do not know about the dangers of cybercrime which is becoming more prevalent today. Studies conducted in business organizations show that they carry out open innovative activities which provide space and opportunity for cybercriminals to steal data or hack the organization's website easily. This is a concern for researchers because perhaps more business organizations will experience high losses due to uncontrollable internal technical problems. As a result, there is an urgent need to develop new strategies to combat cybercrime and shift much more towards a crime prevention approach that focuses on preventing victimisation from happening (Webster and Drew, 2017).

In addition, as expected when so many objects are connected to the Internet, the number of cybercrime cases increases. This is said because, the majority of society today depends on the Internet and every activity carried out will be related to the Internet. Therefore, every personal data stored will be easily stolen by cybercriminals for their immoral purposes. Previous studies have also shown that there is still a lack of awareness among the world community to be more careful in the use of the Internet and do not care to be more alert with something that causes doubts or misgivings. Cyber Crime is a serious crime, it breaches someone's privacy and confidential data and also exposes to financial losses. It involves infringement of human rights as well as of governmental laws. Therefore, one must consistently follow all the precautions discussed earlier, because 'Prevention is better than cure', as the well-known saying states" (Sonika Bharati, 2019).

6. CONCLUSION

As a result, cybercrime is a widespread problem that all users encounter, regardless of age or gender, demonstrating that men and women are equally vulnerable to being targeted and becoming victims of this criminal issue. Furthermore, this crime occurs without our knowledge in every act we perform. Through four publications that are closely relevant to the author's field of study. Furthermore, we can observe from this study that each publication has distinct study outcomes owing to the diverse scope of the investigation. The breadth of each author's research implies that each author investigates the same issue but in a different way. Following that, various writers generate a diversity of thoughts and discoveries that are intriguing despite their diverse backgrounds and writing styles. This is because the variety of these concepts might generate highly fascinating ideas for the researcher to gather information. Not only that, but the time of study causes each of these articles to have their own unique features because it is possible that the author studied this topic at a different time because each of these articles does not have the same continuity. For example, the author of this article studies in a year that is not serious and worrying, which will result in a finding as an issue of this crime can still be saved, whereas the author who studies in a year of such increased cases will not.

Acknowledgments: First and foremost, we would like to sincerely thank our corresponding author Sir Meer Zhar Farouk Amir Razli for his guidance, understanding, patience and most importantly, he has provided positive encouragement and a warm spirit to finish this research article. Thank you and our deepest appreciation to Universiti Teknologi MARA Machang, Kelantan for financing this writing with approval from KW3P.

References

Bandakkanavar, R. (2023, March 14). Causes of CyberCrime and Preventive Measures. Krazytech. Retrieved June 8, 2023, from https://krazytech.com/technical-papers/cyber-crime

Bharati, S. (2019). Cyber crime – awareness and security. Tax Guru. https://taxguru.in/corporate-law/cyber-crime-awareness-security.html#:~:text=Avoid%20using%20friend's%20phone%2C%20public,track%20of%20their%20online%20activities

BlueVoyant. (2022, October 3). What is cybercrime? Types and prevention. BlueVoyant. https://www.bluevoyant.com/blog/cybercrime-types-and-prevention

Cyber Crime Essay for Students and Children | 500 Words Essay. (n.d.). Toppr. Retrieved June 8, 2023, from https://www.toppr.com/guides/essays/cyber-crime-essay/

Cybercrime summary. (n.d.). Britannica. Retrieved June 8, 2023, from https://www.britannica.com/summary/cybercrime

Dakota. (2020, January 13). 7 Types of Cyber Security Threats. University of North Dakota Online. https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/

Jacqueline, M, D. (2019). A study of cybercrime victimization and prevention: exploring the use of online crime prevention behaviours and strategies. Journal of Criminological Research and Practice, 6(1), 17-33. https://doi.org/10.1108/JCRPP-12-2019-0070

Johansen, A. G. (n.d.). 11 Ways to Help Protect Yourself From Cybercrime. Norton. Retrieved June 8, 2023, from https://us.norton.com/blog/how-to/how-to-recognize-and-protect-yourself-from-cybercrime

Kaspersky. (2023, June 9). What is cybercrime? How to protect yourself from cybercrime. Www.kaspersky.com. https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

Raten, V. (2019). The effect of cybercrime on open innovation policies in technology firms. Information Technology & People, 32(5), 1301-1317. https://doi.org/10.1108/ITP-03-2018-0119

Situational Crime Prevention Theory, Elements & Examples | What is SCP? Video. (2022). Situational Crime Prevention Theory, Elements & Examples | What is SCP? - Video & Lesson Transcript | Study.com. Study.com. https://study.com/learn/lesson/situational-crime-prevention-theory-elements-examples-scp.html

Smith, K, T., Johnson, L., Jones, A., & Smith, L, M. (2019). Examination of cybercrime and its effects on corporate stock value. Journal of Information, Communication and Ethics in Society, 17(1), 42-60. https://doi.org/10.1108/JICES-02-2018-0010

Steve, U, JR., & Arnold, C. (2019, November 4). Cybersecurity is critical for all organizations – large and small. International Federation of Accountants. https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small

Synder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104.*(2019), 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039

Threatcop. (2022, December 5). Increase in Cybercrime Worldwide - Threatcop. Threatcop. https://threatcop.com/blog/increase-in-cybercrime/

Verma, M, K., & Kushwaha, S, S. (2021). Awareness towards cybercrime among secondary school students: the role of gender and school management. Safer Communities, 20(3), 150-158. https://doi.org/10.1108/SC-07-2020-0026

Wiktionary. Retrieved June 8, 2023, from https://www.hcltechsw.com/enterprise-security?utm_source=google&utm_medium=cpc&utm_campaign=BrandON_search_Home-Evergreen-Enterprise-Security-Page--CA_May2023_Malaysia_APAC&utm_content=RSA-660463640391&utm_term=cyber%20security&gad=1&gclid=CjwKCAjw1YCkBhAO

93 Must-Know Ransomware Statistics [2023]. (2023). Antivirusguide.com. https://www.antivirusguide.com/cybersecurity/ransomware-statistics/?gclid=EAIaIQobChMI2Jeypa64_wIVWB8rCh094wBQEAAYAiAAEgIfGPD_BwE

Research Article

Cyber-attacks and Cyber Security: Emerging Trends and Recent Developments

Muhammad Muhaimin Nizar Mohamad Sukri[1], Nur Aina Fazlina Muhamat Padli [2], Siti Syalwanie Roslan[3], and Nur Ainatul Mardiah Mat Nawi [4,*]

[1] Universiti Teknologi Mara Kelantan Branch; 2020818906@student.uitm.edu.my; 0009-0002-2264-5128
[2] Universiti Teknologi Mara Kelantan Branch; 2020822116@student.uitm.edu.my; 0009-0007-1548-8837
[3] Universiti Teknologi Mara Kelantan Branch; 2020621438@student.uitm.edu.my; 0009-0007-6883-0333
[4] Universiti Teknologi Mara Kelantan Branch; ainatulmardiah@uitm.edu.my; 0000-0002-5868-4535
* Correspondence: ainatulmardiah@uitm.edu.my; +60145142921.

Abstract: *Cybersecurity is an important field that deals with the protection of computer systems, networks, and data from unauthorized access, misuse, and attack. As technology evolves, the issue of cybersecurity and cybercrime is also increasing in today's environment. The impacts and phenomenon of cyberattacks and cybersecurity is widely discussed within the body of knowledge, lead for further exploration of the topic. Therefore, this study is being conducted in order to explore the issues on cyberattacks and cybercrimes. This study involves designing, collecting and analyzing data from the previous studies to find the evidence. The study was then narrowed down using Boolean search in order to get more in-depth information about cyberattacks and cybercrimes, which are becoming more common nowadays, before interpreting and subjecting them to serious analysis. Based on the other studies, this paper discusses the impact of cyberattacks and the importance of cybersecurity, trends that are changing in cybersecurity nowadays, and cybersecurity techniques such as access control and password security, authentication of data and firewall, and the role of social media. In addition, the discussion also discusses the value of cybersecurity, which refers to the benefits when this cybersecurity is used to protect data.*

Keywords: Attacks, Cyber-attacks, Cyber security, Cybercrime.

DOI: 10.5281/zenodo.8182721

1. INTRODUCTION

Sensitive data is progressively being stored as a result of the digitization process in every element of human life, including healthcare, education, business, etc. As technology develops, cybercrimes also grow in quantity and complexity. Security is the act of preventing digital information from being stolen or physically damaged while retaining the confidentiality and accessibility of information. The poor use of software, out-of-date security measures, design flaws, programming mistakes, readily accessible internet hacking tools, a lack of public knowledge, high rates of financial gain, etc., are some of the factors contributing to the tremendous expansion of cybercrime. Technical attackers create more potent attack tools to take advantage of the target's vulnerabilities and attack the victim. As a result, new, challenging-to-detect threats are emerging in various versions. Effective security algorithms have been developed because of the growing reliance on the internet in all spheres of life, the nature of digital data in enormous quantities gathered through online transactions, and the decentralization of data repositories. Cybercrime's dynamic nature makes it challenging to manage and stop new dangers from appearing. The most difficult duty is protecting cyberspace since sophisticated attacks are so prevalent.

2. METHOD & MATERIAL

Research methodology is a method and technique of designing, collecting, and analyzing data in order to produce evidence that can support a study. The study's methodology was based on the previous literature. The researcher reviewed and analyzed previous studies and articles. The searching process was being narrowed down using the Boolean search in order to get more in-depth information about cyberattack and cybercrime which is becoming more widespread nowadays before interpreting and making a serious analysis discussion.

3. FINDINGS

3.1 Definition of Cyberattack.

A cyberattack is an assault on infrastructure, personal computers, mobile devices, networks, or other electronic devices that use computers. A person or entity that makes an unauthorized, potentially harmful, effort to access data, functions, or other restricted areas of a system is called an attacker. Cyber-attacks may be a component of cyber terrorism or cyber warfare, depending on the situation. Sovereign nations, private persons, social groupings, organizations, and communities all can deploy cyberattacks, and they can also come from unidentified sources. Cyber weapons are occasionally used to refer to products that aid in cyberattacks. In recent years, cyberattacks have escalated. Distributed denial of service (DDoS) attacks is an extremely common type of cyberattack. Hacking into private networks or susceptible systems allows cyberattacks to steal from, change, or kill specified targets. Cyberattacks can involve anything from the placement of spyware on individual computers to attempts to compromise the infrastructure of a whole nation. Legal professionals are seeking to confine the term's usage to instances that result in bodily harm, separating it from more commonplace data breaches and extensive hacker activities. While cybersecurity is the protection of computer systems and networks from attacks by malicious actors that may result in unauthorized disclosure of information, theft or damage to hardware, software, or data, as well as from interruption or misdirection of the services they provide, cybersecurity is computer security, cyber security, digital security, or information technology security (IT security). Privacy and information protection can be key security behavior and one that any company and individual should constantly be concerned about.

3.2 Definition Cybercrime

The phrase "cybercrime" refers to theft and other crimes committed via personal computers. The United States department of justice has broadened the definition of cybercrime to include any crime that makes use of technology to store evidence. Cybercrimes are crimes committed using computers, such as the dissemination of network intrusions and computer viruses, as well as computer-based variations of legal crimes including stealing, stalking, threats, and coercion. In other words, cybercrime is sometimes characterized as crimes done using computers and the internet to steal identities, sell people to victims of human trafficking, stalk, or disrupt operations using destructive software. Additionally, (Julian Jang-Jaccard) asserts that any nation's security and economic health depend on enhancing cyber security and safeguarding crucial information infrastructure. An essential component of the development of new services and public policy is a safer internet. Additionally, (Veenoo Upadhyay Wizard) solicits people to "label" certain friends on social networking platforms as private.

The author then utilizes this information to build classifiers using machine learning patterns that may be used to automatically grant certain users' friend's access. The design's inspiration came from the fact that actual users are aware of their privacy practices and that, subject to a set of implicit restrictions, friends may view the details they use and duplicate them in other friends' settings. Because technology plays such a significant part in people's daily lives, cybercrime will rise as technology develops.

4. DISCUSSION

4.1 Impact of Cyber-attacks and The Importance of Cybersecurity

The growth of information technology, and the increasing reliance on digital systems, has created unprecedented prospects for creativity, efficiency, and connectedness. Along with these benefits, the world has seen an upsurge in cyber-attacks and security breaches. The intensity and frequency of cyber threats have increased in recent years, posing substantial risks to individuals, organizations, and even governments. Cyber-attacks have become a pressing concern due to their potential to cause significant economic, social, and political damage. With the advancement of technology, hackers and cybercriminals have developed sophisticated techniques to exploit vulnerabilities in computer systems and networks. They employ malware, phishing, ransomware, and Distributed Denial of Service (DDoS) assaults to jeopardize the confidentiality, integrity, and availability of sensitive data. These attacks can target individuals, corporations, governments, and critical infrastructure, leading to financial loss, reputational damage, and even loss of life in some cases.

Cyber-attacks have evolved as one of the contemporary era's most prevalent hazards, affecting individuals, corporations, and governments alike. These attacks can take various forms, including malware, ransomware, phishing, and distributed denial-of-service (DDoS) attacks. Cyber-attacks have enormous financial consequences. According to Smith and Jones (2019), cybercrime cost the global economy roughly $600 billion in 2018, with this figure expected to climb to $6 trillion yearly by 2023. Furthermore, the impact of cyber-attacks extends beyond financial losses. Organizations often face reputational damage due to data breaches, leading to a loss of trust from customers, partners, and stakeholders. In 2019, the Equifax data breach compromised the personal information of nearly 147 million individuals, resulting in a significant decline in the company's reputation (Johnson et al., 2020). Additionally, cyber-attacks have the potential to impair essential infrastructure such as electricity grids, transportation networks, and healthcare institutions. For instance, the WannaCry ransomware attack in 2017 paralyzed numerous National Health Service (NHS) hospitals in the United Kingdom, highlighting the potential dangers of cyber-attacks on public services (Brown et al., 2018).

Cyber-attacks have significant social implications, affecting individuals and society on various levels. One major source of concern is the compromise of personal information and privacy. According to a study conducted by Kshetri (2018), data breaches resulting from cyber-attacks can have far-reaching consequences for individuals, including identity theft, financial loss, and psychological distress. These incidents weaken people's trust in digital technologies and impede online service adoption, restricting social connectivity and economic prospects. Furthermore, Taddeo and Floridi's (2020) research emphasizes the social effects of cyber-attacks on important sectors such as healthcare and education. These attacks have the potential to disrupt critical services, compromising patient care and educational procedures. For example, ransomware assaults on hospitals can obstruct access to important medical documents, potentially endangering patient lives.

Other than that, the political impact of cyber-attacks has received considerable attention in recent years. State-sponsored cyberattacks have evolved as effective means of espionage, influence operations, and sabotage. According to Jevans (2018), these attacks have the potential to disrupt democratic processes such as elections and political campaigns. Cybercriminals or nation-states may undermine public trust in democratic institutions by meddling with voting systems or spreading disinformation, weakening the foundations of governance. Additionally, cyber-attacks on critical infrastructure might have serious geopolitical consequences. According to Ruggeri et al. (2022), state-sponsored attacks on power grids and communication networks can destabilize nations and have an impact on global security. During a conflict, such attacks can be used as a strategic weapon, causing power outages, disrupting key services, and potentially causing societal discontent.

Moreover, cyber-attacks have also significant economic impacts, affecting corporations, governments, and individuals alike. The financial industry is one of the primary areas of concern. Smith (2019) claims that the banking industry has suffered enormous losses as a result of cyber-attacks, including the theft of sensitive client data and financial fraud. These attacks not only affect financial organizations' reputations, but also undermine client trust, potentially resulting in revenue losses and increased operational expenses. In addition, Gonzalez-Padron et al. (2021) found that cyber-attacks on key infrastructure, such as power grids and transportation networks, might cause huge economic disruptions.

Furthermore, considering the pervasiveness and serious repercussions of cyber-attacks, robust cybersecurity measures are essential. Cybersecurity refers to a set of practices and technology aimed at preventing unauthorized access, damage, or interruption to computer systems, networks, and data. It includes preventive measures such as firewalls, encryption, and safe coding practices, as well as incident response strategies to mitigate the effect of successful attacks. Investing in comprehensive cybersecurity safeguards is both a defensive and a proactive strategy. Organizations can considerably lower the risk of cyber-attacks and their associated expenses by implementing appropriate cybersecurity policies. A study conducted by Anderson et al. (2021) found that companies that invested in advanced security technologies, employee training, and incident response plans experienced 95% fewer cyber incidents and saved an average of $1.5 million per year compared to those without adequate cybersecurity measures.

In addition, cybersecurity is essential for protecting individual privacy and safeguarding sensitive data. With the rising digitization of personal information, protecting privacy has become a top priority. Effective cybersecurity safeguards personal data against unauthorized access and misuse, maintaining its confidentiality and integrity. Organizations can comply with data protection rules while also instilling trust and confidence in their customers by deploying privacy-enhancing technologies (Sullivan et al., 2022).

4.2 Trends That Change Cybersecurity Nowadays.

Several developments have a big impact on cyber security, with web servers being one of them. A web server, which is hardware or server software created to run the world wide web, may be used to receive content. Incoming network requests are handled by web servers using the http protocol, along with a number of other related protocols. Still, there are still threats to target web programmes in order to steal data or spread malicious code. To disseminate their hazardous virus, cybercriminals hack onto legitimate web servers. However, assaults involving data theft, which regularly make the headlines, also provide a significant threat. The protection of web servers and online apps must now receive more attention. Web servers are these attackers' most efficient platform for data theft. Everyone must thus use a safer browser at all times, especially while doing important transactions, to prevent being a victim of this crime.

The services provided by cloud computing are discussed next. Right now, all small, medium, and large organizations are increasingly using cloud services. The planet is slowly making its way towards the cloud, to put it another way. This most recent trend offers a significant cybersecurity risk since traffic may already be getting past traditional controls. The number of cloud-based applications must increase together with the policy controls for online apps and cloud services in order to prevent the loss of crucial data. Security issues are always a top worry even if cloud businesses are developing their models. It's vital to keep in mind that as the cloud grows, so do its security concerns, despite the fact that it could provide a number of benefits.

Next is the wireless network. Mobile networks, which are also sometimes referred to as wireless networks, use radio waves to send and receive data between users. It consists of base stations that collectively provide large geographic radio coverage. Each base station covers a certain "cell," which is a geographic area. This allows connections to be made between many mobile transceivers, as well as between them and fixed transceivers and phones, from any place within the network, even if some transceivers transit across multiple cells while broadcasting. Because of this, communication between people is now feasible no matter where they are on the planet thanks to technological advancements. But one of the biggest concerns with these mobile networks is security. This is due to the fact that people utilize technology such as tablets, phones, computers, and other devices, all of which require greater security than what is offered by the programmes they are using. People should always take into account the security issues of these networks because mobile networks are so vulnerable to these cybercrimes. Therefore, considerable attention must be exercised to prevent safety issues.

Furthermore, one of the developments that is transforming cyber security is IPv6: the new internet protocol. This is because IPv6 is a new internet protocol that replaces IPv4 (the outdated version), which has evolved into the internet's and our networks' main structural pillar. Removing IPv4 support is not the only way to protect IPv6. Although IPv6 completely replaces IPv4 in terms of increasing the number of IP addresses, there are several extremely important modifications to the protocol that should be considered when developing security policies. To lower the dangers related to cybercrime, it is, therefore, preferable to transition to ipv6 as soon as feasible.

Finally, the code is encrypted. To prevent eavesdroppers or hackers from reading a message (or other piece of information), it must be encrypted. With the help of an encryption algorithm, a message or piece of data is transformed into an unintelligible ciphertext as part of an encryption system. Utilizing an encryption key, which controls the message's encoding, is typically how this is accomplished. Data integrity and privacy are safeguarded by encryption in the earliest stages. But as encryption is used more widely, cyber security issues get increasingly complex. Additionally, encryption is used to secure data in transit, including information sent across networks (such as the Internet or E-commerce), mobile devices, wireless microphones, wireless intercoms, and other devices. Therefore, one may determine whether there has been any information leaked by encrypting the code.

4.3 Techniques of Cybersecurity

Cyberattacks in cyberspace may change as a result of utilizing new methods. Most of the time, cybercriminals will alter existing malware signatures to exploit brand-new technological defects. In other cases, they are searching for specifics of cutting-edge technologies to identify malware injection flaws. The rapidly developing internet and its millions and billions of active users provide cybercriminals with easy and efficient access to a sizable population that is using this new technology.

i. Access control and password security

A quick and easy approach to protecting personal information and maintaining privacy is using usernames and passwords. One of the most important cybersecurity projects is this method of delivering security. It is common to use the terms "cyber security" and "knowledge security" interchangeably. The latter term examines the human element of security, whereas the former considered it to be an extra dimension.

ii. Authentication of data

Therefore, it is necessary to demonstrate that the information transmitted is accurate and that it originates from a reliable source. These papers are frequently validated using tools provided by the virus software program installed on the machine by the adversary. Sincerely speaking, anti-virus software is crucial for preventing infections on the system. An ethical discussion on cyber security, however, has significant ramifications since it speaks to society as a whole. To address issues with cyber security, several different methods and models have been created.

iii. Firewall

A firewall is a piece of hardware or software that assists in keeping out online hackers, viruses, and worms. All incoming communications are examined by the firewall, which then rejects those that don't adhere to the security standards that apply to all messages. To identify malware, firewalls are crucial.

iv. Role of social media

In today's modern world, businesses that are interactive and need to find new ways to collect client data in a more connected environment are needed. Social networking is essential for both individual cyberattacks and cyber security. Social media usage among employees is increasing, which increases the danger of assaults. Since the majority of them use social networking sites or social media almost every day, it has become common for hackers to access user accounts and steal important information there. Organizations must ensure that they detect any breach as fast as possible and take urgent measures to halt it because it is now rather simple to reveal personal information. Social networking platforms make it simple for users to share their personal information, which hackers may then use. Therefore, people must take appropriate safety measures to guard against misuse and loss of their personal information on these social media.

4.4 Value of Cybersecurity

First of all, cybersecurity is the practice of preventing unauthorized access, abuse, damage, and disruption to computer systems, networks, devices, and data. It involves implementing measures and adopting strategies to prevent, detect, respond to, and recover from cyber threats, attacks, and vulnerabilities. With the increased reliance on digital technology and the interconnection of systems and devices, the relevance of cybersecurity has expanded substantially. Malicious software (malware), phishing assaults, hacking, ransomware, denial-of-service (DoS) attacks, and social engineering are all examples of cyber dangers. Individuals, organizations, governments, or key infrastructure may be targeted by these threats, resulting in financial loss, data breaches, reputational damage, or even bodily violence. Cybersecurity refers to a collection of practices, technologies, and procedures used to safeguard digital assets and information. Among the primary areas of concentration in cybersecurity are network security is using techniques such as encryption, intrusion detection and prevention systems (ISD/IPS), and virtual private networks (VPNs), networks and their components (routers, switches, firewalls) are protected against unauthorized access and network traffic is secured. Next is endpoint security which is individual device security (computers, mobile devices) is achieved by deploying antivirus software, firewalls, and security patches to protect against malware, unauthorized access, and data theft. Other than that, this cyber security also includes application security. This area has been secure by ensuring the security of software applications by doing vulnerability assessments, code reviews, and penetration testing to detect and correct security issues and prevent exploitation. Last but not least is data security that is related by using encryption, access restrictions, data loss prevention (DLP) methods, and frequent backups to protect data throughout its lifespan, including data storage, transit, and processing.

Next is about the advantages that people can get when this cyber security is reliable in the community is protection of confidential information. This part briefs that personal information, financial records, commercial secrets, and intellectual property are all safeguarded by cybersecurity. Cybersecurity helps prevent unauthorized access, data breaches, and identity theft by establishing strong security measures such as encryption, access limits, and secure communication protocols. Next advantage that can be useful for people is prevention of financial loss. Cybersecurity measures aid in the protection of organizations and people from financial damage caused by cyber-attacks. Cybersecurity prohibits unauthorized access to financial systems, unauthorized transactions, and financial fraud by identifying and mitigating threats such as malicious software, phishing attacks, and fraud attempts. Other than that, is to maintain business continuity. Cybersecurity is critical to ensuring that corporate operations run smoothly. Organizations may recover fast from cyber assaults by using techniques such as frequent data backups, disaster recovery plans, and system redundancy. This reduces downtime and financial losses. This flexibility enables companies to preserve client confidence while meeting their duties. Safeguarding reputation and trust are also the advantages to cyber security because a successful cyber assault may significantly harm a company's brand and undermine consumer trust. Cybersecurity safeguards against data breaches by assuring the confidentiality, integrity, and availability of sensitive data. Organizations may establish trust and maintain a favorable reputation among their customers, partners, and stakeholders by demonstrating a commitment to data security. So, by this security it can help to avoid being hacked by hackers to steal the information. Not only that, many sectors and jurisdictions have their own cybersecurity legislation and standards that businesses must follow. Implementing cybersecurity safeguards guarantees that these criteria are met, hence avoiding legal and financial fines. It also displays a commitment to client data security and ethical business practices because it follows compliance with regulations and standards. Next is enhanced trust in digital transactions. With an increasing reliance on digital transactions, cybersecurity ensures and builds confidence in online activities such as e-commerce, online banking, and digital communication. Cybersecurity measures enable individuals and companies to engage in digital transactions with confidence by guarding against fraud, identity theft, and unauthorized access. The last point that can be advantageous to cyber security is in innovation and technological advancements. It relates because by providing a safe environment for research, development, and knowledge exchange, strong cybersecurity measures promote innovation and technical progress. Cybersecurity enables organizations to invest in new technologies and contributes to the expansion of digital economies by protecting intellectual property and sensitive research data.

The paper claims that now that the groundwork has been done, we may argue that IC is also a governance issue for cyber security. According to Chong et al. (2008), the network impact of using different intellectual, human, financial, and organizational resources results in IC. Choong carried out a comprehensive analysis of the terminologies and vocabularies used by academics to define and refer to IC. He notes and demonstrates how the term "intangible assets" (IAs) is frequently used as a synonym for IC. He presents the case for adding intellectual property (IP) in addition to human capital, structural capital, and relational capital, which according to his study may be represented by a "three-grouped framework" (p. 622) that includes all three. Others use the term "relational capital," while others use the term "social capital". The term "social capital/relational capital" was first used by Hussinki et al. (2017). Consequently, we will refer to the section of IC that is related to interactions between individuals and organizations and is a component of the IC of the organization by using both terms interchangeably. According to Reed et al. (2006), the various IC components are inter- and co-dependent in terms of how they affect the organization's financial performance; a weakness in one reduces the IC's ability to support the organization's success. In other words, both the network itself (relationships and organizational structure) and each individual node (personal knowledge and experiences) must be preserved if IC is to contribute to organizational success. This issue has a strong knowledge component to it; IC is almost like a galaxy of ideas revolving around the information that employees of an organization hold. However, according to Choong (2008) and Pike et al. (2005), it is also regarded as an "intangible asset". It may be considered that its security is not a cyber-related board issue due to its intangibility. When we examine the IC concept more closely, a compelling case can be made for including responsibility for its upkeep within the cyber security governance framework.

5. CONCLUSION

In conclusion, cyber-attacks and cyber security are constantly evolving fields with emerging trends and recent developments that have significant implications for individuals, organizations, and even nations. The digital landscape has become increasingly interconnected, and as a result, the threats and risks associated with cyber-attacks have grown in complexity and severity. Recent developments have also emphasized the necessity of international cooperation and information sharing in the fight against cyber threats. Cybercriminals operate across borders, hence it is critical for governments and organizations to collaborate and share intelligence in order to effectively identify and neutralize threats. Initiatives such as establishing international cyber security guidelines and exchanging best practices across stakeholders have shown promise in tackling the global character of cyber-attacks.

Furthermore, there is a rising skills gap in the sector of cyber security. The demand for highly qualified personnel in fields like threat intelligence, incident response, and safe software development is outstripping supply. To address this challenge, there is a need for increased investment in cyber security education and training, as well as efforts to attract diverse talent to the field. Additionally, automation and the deployment of sophisticated technology can also assist relieve the stress on human operators while also improving the effectiveness of cyber security operations. Overall, cyber-attacks and cyber security are growing rapidly, with rising trends and recent advancements impacting the digital security landscape. It is crucial for individuals, organizations, and governments to remain vigilant, proactive, and adaptable in their approach to cyber security. By staying informed about the latest threats and employing comprehensive security measures, we can mitigate the risks posed by cyber-attacks and protect the integrity, confidentiality, and availability of our digital systems and data.

Acknowledgments: We would like to extend our profound thanks to Miss Nur Ainatul Mardiah binti Mat Nawi, our research advisor, for her important guidance, support, and supervision during the duration of our research project.

References

Brauneck, A., Schmalhorst, L., Mahdi, M., Bakhtiari, M., Uwe Völker, Baumbach, J., Baumbach, L., & Buchholtz, G. (2023). Federated Machine Learning, Privacy-Enhancing Technologies, and Data Protection Laws in Medical Research: Scoping Review. 25, e41588–e41588. https://doi.org/10.2196/41588

Crawford, G. E., Maclean, F. M., Vasile, I., & Smyth, A. (2022, September 30). Privacy Enhancing Technologies — A Panacea for Data Protection Compliance? Lexology; Latham & Watkins LLP. https://www.lexology.com/library/detail.aspx?g=2372f94d-2df3-44ba-ae19-20eece28d728

Cremer, F., Sheehan, B., Fortmann, M., Kia, A., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. 47(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Dr. Yusuf Perwej, Abbas, Q., Jai Pratap Dixit, & Anurag Kumar Jaiswal. (2021, December 28). A Systematic Literature Review on the Cyber Security. ResearchGate; Valley International. https://www.researchgate.net/publication/357393481_A_Systematic_Literature_Review_on_the_Cyber_Security

Dwivedi, Y. K., Nir Kshetri, Hughes, L., Rana, N. P., Baabdullah, A. M., Arpan Kumar Kar, Koohang, A., Ribeiro-Navarrete, S., Belei, N., Balakrishnan, J., Basu, S., Behl, A., Davies, G. H., Dutot, V., Dwivedi, R., Evans, L., Felix, R., Foster-Fletcher, R., Mihalis Giannakis, & Gupta, A. (2023). Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse. https://doi.org/10.1007/s10796-023-10400-x

Fruhlinger, J. (2020, February 12). Equifax data breach FAQ: What happened, who was affected, what was the impact? CSO Online. https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

Harel, Y., Gal, I. B., & Elovici, Y. (2017). Cyber security and the role of Intelligent Systems in addressing its challenges. ACM Transactions on Intelligent Systems and Technology, 8(4), 1–12. https://doi.org/10.1145/3057729

Humayun, M., Niazi, M., Noor Zaman Jhanjhi, & Mahmood, S. (2020, January 6). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. ResearchGate; unknown. https://www.researchgate.net/publication/338419380_Cyber_Security_Threats_and_Vulnerabilities_A_Systematic_Mapping_Study

Ismail, N. (2022, December 1). A CTO guide: The main challenges of cyber security. Information Age. https://www.information-age.com/cyber-security-challenges-123474692

Keen, W. (n.d.). SAFEGUARDING CRITICAL INFORMATION INFRASTRUCTURE RISKS & OPPORTUNITIES. Retrieved June 6, 2023, from https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2020/RDF2020/Post%20Forum%20Day%203/CII-Whitepaper-WK.pdf

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. Energy Reports, 7, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Negrete-Pincetic, M., Yoshida, F., & Gross, G. (n.d.). Towards Quantifying the Impacts of Cyber Attacks in the Competitive Electricity Market Environment. Retrieved June 6, 2023, from http://www.dl.edi-info.ir/Towards%20Quantifying%20the%20Impacts%20of%20Cyber%20Attacks%20in%20the%20Competitive.pdf

Privacy and cybersecurity issues to watch in 2019. JD Supra. https://www.jdsupra.com/legalnews/privacy-and-cybersecurity-issues-to-25710/

Rajasekharaiah, K. M., Dule, C. S., & Sudarshan, E. (2020). Cyber security challenges and its emerging trends on latest technologies. IOP Conference Series: Materials Science and Engineering, 981(2), 022062. https://doi.org/10.1088/1757-899x/981/2/022062

Uddin, H., Hakim Azfar Ali, & M. Kabir Hassan. (2020). Cybersecurity Hazards and Financial System Vulnerability: A Synthesis of Literature. https://doi.org/10.2139/ssrn.3689162

Renaud, K., Solms, B. V., & Somls, R. V. (2019, July 9). How does intellectual capital align with cyber security?. UiTM Library e-Resources. Retrieved from https://www-emerald-com.ezaccess.library.uitm.edu.my/insight/content/doi/10.1108/JIC-04-2019-0079/full/pdf?title=how-does-intellectual-capital-align-with-cyber-security

Wikimedia Foundation. (2023, June 4). Computer security. Wikipedia. https://en.wikipedia.org/wiki/Computer_security

Cyber Security in Higher Education: Problem and Solution

Nur Najwa Izzaty Nasir[1], Siti NurFarahin Radzuan[2], Batrisyia Aqilah Azhami[3] and Huda Hamidon[4*]

[1] Universiti Teknologi MARA; 202086654@student.uitm.edu.my; 0009-0008-2067-4332

[2] Universiti Teknologi MARA; 2020602814@ student.uitm.edu.my; 0009-0008-5975-4364

[3] Universiti Teknologi MARA; 2020489248@ student.uitm.edu.my; 0009-0002-2295-4289

4 Universiti Teknologi MARA; huda685@uitm.edu.my; 0000-0002-7667-0743

* Correspondence: huda685@uitm.edu.my; +60137716589.

Abstract: *Cyber security has emerged as a critical concern in today's digital age, affecting various sectors and industries worldwide. Among these, higher education institutions have become prime targets for cyber-attacks and other security threats due to the vast amount of valuable and sensitive information they possess. These institutions house a wealth of personal, financial, and research data, making them attractive targets for malicious actors seeking to exploit vulnerabilities in their information systems. These threats may lead to reputational damage, financial losses, and even legal repercussions. Moreover, the disruption caused by such attacks can significantly hinder the academic and administrative functions of these institutions, affecting students, faculty, and staff alike. This paper aims to provide a comprehensive analysis of the problem of cyber security in higher education and offer viable solutions to address these issues. To achieve this objective, a thorough review of existing literature related to cyber security in higher education will be conducted. This review will delve into the various types of cyber threats faced by these institutions with a focus on the problems and their solutions. By highlighting the pressing nature of cyber security challenges in higher education and providing practical solutions, this paper endeavours to equip institutions with the knowledge and awareness of the current situation of the cyber threats. It is essential for higher education institutions to proactively address these issues to safeguard their reputation, maintain the trust of stakeholders, and ensure the continuity of their educational goals.*

Keywords: Information Security; Cyber Security; Higher Education.

DOI: 10.5281/zenodo.8182762

1. INTRODUCTION

The Internet is now a fundamental component of many people's daily lives. Users engage in a variety of activities involving their private data over the Internet daily. These activities include Internet banking, educational services, medical care, and e-commerce. According to Nazahah et al. (2020), higher education is one of the industries facing risks. There have been cases of institutions being subjected to cyber-attacks in which information was stolen. Users in higher education institutions rely on gadgets that allow them to be highly flexible. This has made it easier for them to adapt to the Internet and access it at any time and from any gadget. However, ensuring cybersecurity in higher education institutions is incredibly challenging.

According to Aruna (2017), Malaysia is highly associated with cybersecurity and is ranked third out of 193 countries. In 2017, there were 6,274 reported cyber-attack incidents. This demonstrates that the internet is not completely protected. Thus, awareness about cybersecurity is critical given the increasing dependency on computer systems and the internet. With several incidents recorded, higher education institutions have become common targets for cybercriminals (Rohan et al., 2023). These institutions keep and manage an enormous amount of vital research data, sensitive personal information of students, lecturers, and non-academic staff members, as well as teaching and academic information. As a result, hackers are interested in violating educational institutions, which could result in consequences such as intellectual property loss, reputation damage, economic costs, and disruption of education. According to Chabrow (2015), inadequate cybersecurity puts higher education at risk, and the abundance of academic research information has made educational institutions an appealing target for cybercriminals. This is concerning for the higher education industry, as cyber risks such as hacking can potentially interrupt academic operations. Hackers use the important details obtained from institutions and can effortlessly market the data because data has become an asset. Institutions' online systems are a potential subject of cybersecurity concerns.

Almost every activity in higher education institutions relies mainly on computer technology and internet access. Higher education systems are closely linked to the Internet world. However, cyberspace is dangerous due to theft and illegal behaviour, which results in cyber security issues. Cyber security protects computer-related systems, such as hardware, software, and digital information, from theft, destruction, interruption, or fraud (Nazahah et al., 2020).

The work presented here focuses on cybersecurity issues in higher education institutions and suggests solutions that can be utilized to address these issues. With this information, organizations can be well-informed and provided with targeted assistance to avoid falling victim to cyber threats.

2. METHOD & MATERIAL

This paper provides a brief review of the existing literature on cyber security in higher education, with a particular emphasis on the problem and its solution. The study was carried out to determine the source of the problem as well as the best solution to address information security. Higher education circles and discussion groups have been used to provide insights into the current undergraduate situation.

3. FINDINGS

3.1 Cyber Security Problems in Higher Education

3.1.1 Weak security system policy that affects cyber security

Among the cyber security problems in institutions of higher education include having a weak security system policy that affects cyber security. According to a report by BitSight (a cyber risk management company) higher education has the highest rate of ransomware attacks among all industries studied. Huge financial losses, due to ransomware attacks or data breaches (Noran Shafik Fouad, 2021). Ransomware virus is a virus or malware that can access all the data in the victim's laptop while the victim will not be able to access the data in his laptop until the money requested by the spreader is paid. According to (Eva D. Kundy and Benson James Lyimo, 2019) the impact of this vulnerability often comes from anyone who has access to IT-related networks or systems such as employees and vendors. According to (Hoog 2015) vendors often place and introduce unsafe products in the market thus creating risks. This problem is often labeled as 'technical security debt'. If the products sold in the market are used by most high institutions, the risk of this cyber threat will increase. Furthermore, those in charge of information system management in higher education institutions were found to be unconcerned about updating software and operating systems that would significantly improve their higher education institutions' security posture and reduce potential risks. (Dr. Joanna ywiytkowska, 2022). The risk of being attacked by a virus is very high if the system is not updated regularly. Hackers rely on known vulnerabilities since 2002 and there are almost 90% of recorded cases (Harrison, Pagliery 2015).

Furthermore, untrained workers and staff invite direct access attacks in large organizations, including school and university liaisons (George B. Liluashvili). One of the issues found in weak security system policies is untrained staff and workers. If the issues of worker skill shortages and job mismatches are not addressed, they can significantly increase cyber threats. This also happens because of the lack of support from top management, staff, and management security awareness of cyber security Alfawaz (2015). The superiors are not sensitive to the weaknesses of the security system implemented in institutions of higher learning, thus inviting various cyber threats that can damage the existing system. Among the attacks experienced in the case of weak security system policy include the risk of phishing attacks. According to (Christopher & Michele, 2015) phishing is a digital crime that targets the victim's sensitive information or data through email, social media uploads, or text messages. Arguably, phishing activities aim to entice people to voluntarily provide personal information unwittingly for criminal purposes. Not only that, having a weak security system will also cause higher education institutions to experience malware attacks. Malware can be defined as harmful software capable of interfering with or manipulating the normal operation of digital devices (Eric CK Cheng and Tianchong Wang, 2022). Malware can remain in the system for long periods without the knowledge of the system owner. These attacks often occur due to human error or lack of vigilance. From the attack the institution will receive various negative effects. Among them it will damage the good name of the company. The information system is affected if the system is damaged. Even if the system continues to work, it still needs to be implemented. This situation caused the reputation of the company to be damaged. The information system will be greatly affected if the system breaks down in a high-risk group. Almost half the system became unusable. For the system to work, it must be replaced. This situation affects the reputation of the company.

3.1.2 Cyber threats caused by the human factor

When developing human knowledge to protect society from technical attacks, a major pitfall and ongoing issue confronts higher education institutions. Despite modern cyber security preparedness and trained personnel, hacking activities flourish with malicious actions aimed at stealing critical sensitive information from higher education institutions. Furthermore, environmental, social, political, constitutional, organizational, economic, and personal factors influence the user's ability to detect and mitigate identified threats. According to the research, employees who are at risk of hacking must be classified after analyzing the challenges of traditional and modern tools and developing training programs to ensure that hacker actions are unsuccessful. Furthermore, eliminating social engineering breaches is nearly impossible unless efforts are made to raise the level of information security awareness among all employees to address the cyber security risks posed by students at higher education institutions. According to researchers, a person's email address will remain an online identity despite the many modern applications for communication. The purpose of the study is to identify security vulnerabilities in email. This allows malicious actors to engage in phishing via phishing emails.

The shortage of cybersecurity professionals will continue to be a major challenge for higher education institutions (the ISACA State of Cybersecurity 2020 report), with little progress to report (ISACA, 2020) to institutions of higher education (Burrell, 2020; Crumpler & Lewis, 2019). ISACA's Global State of Cybersecurity Study, which surveyed 2,000 above cybersecurity professionals across 17 industries, found:

- 62% stated that their cybersecurity team lacked manpower.

- 57% reported that they had not yet recruited for cybersecurity positions.
- 70% believe less than half of the security candidates are competent in network security.
- 73% of new cyber security university graduates lack practical experience and knowledge related to the basics of cyber security.

Tan et al. (2018) also discussed possible career paths. To design and maintain a victorious cybersecurity program, you should strive to stimulate then address the labor needs. Previous studies on cybersecurity education have focused on two themes such as specialized labs, platforms, and technologies used in cybersecurity courses and offerings. One example is cybersecurity training courses and also textbooks. Several studies have concentrated on pedagogical approaches or models for developing cybersecurity courses (Abraham & Shih, 2015; Hetea et al., 2006; Yuan et al., 2017). Yuan et al. (2017) proposed the POGIL (Procedural Guided Learning) model. POGIL aims to improve non-technical skills for instances, attitude, inducement, and interest in education. It also proposes a comprehensive model of cybersecurity education is developed from its blended learning theory (Abraham & Shih, 2015).

Cybersecurity covers many topics but figuring out the cybersecurity issue to educate be able to difficult. Due to the time constraints of each semester, each degree program is responsible for defining and designing the topics and methods discussed in the discussion. The U.S. federal government has implemented various programs to develop higher education security policies, standards, and policies over the past two decades, such as National Telecommunications Security Policy. The NIST Cyber Security Frame, the National Initiative for strategic scheme for Education in Cyber Security (NICE, 2019), the National Education and Training Program in INFOSEC, and the National Conference on Education in Security of Information Systems are part of this work. This initiative focuses on training college and university students for information security roles. However, there has been no research focused on the theoretical foundations for developing cybersecurity courses based on the requirements of higher education institutions.

3.1.3 External entities deceive users into providing their personal information.

Cybersecurity issues in higher education can occur when entities outside the institution deceive users into disclosing their personal data. External entities are people or organizations with no primary role in an interaction or deal between two different parties but might be influenced or concerned about it. Most organizations use passwords to secure their systems against illegal entry. Improper access to systems, as well as data theft or system exploitation, is typically the result of criminals "cracking" user login credentials or obtaining them through hacking. Human factors need to be included in the conceptualization of protection processes because security is conceived, carried out, applied, and violated by humans. Human considerations are now more significant to hackers compared to cybersecurity professionals. Social manipulation approaches, such as fabrication and manipulation to get passwords, will take advantage of consumers who lack security understanding (Adams et al., 1999). They develop advertisements using open-source applications to ensure the person who clicks on them is human.

In general, educational institutions keep extensive data relating to their students, academic and non-academic employees. For example, residence locations, dates of birth, and complete names. Although this information might not appear as important as banking information and identification numbers, it can benefit cyber criminals. It enables phishing attacks that impersonate relatives or close friend members. Cybercriminals may also use this information to impersonate students or staff members for profit.

Lötter and Futcher (2014) state that email clients provide sufficient protection. Emails can also be a helpful tool for hackers planning phishing scams. The more genuine and reliable the email is, the more valuable it becomes in a security breach. By gaining access to an institution's email account, fraudsters may gain from a website's reliability to their phishing emails. The significant value of '.edu' email addresses belonging to students and faculty members is also frequently exposed publicly, making it easier for attackers to find and select targeted ones. Nonetheless, cybercriminals can quickly obtain an educational domain email address for themselves. For these factors, higher-education thefts start with an email assault. Higher education institutions, particularly their staff members, are more at risk of becoming a victim of phishing attempts. It is needed for only one staff person to make a mistake, and the threat may attack the whole university system.

3.2 Solution for the cyber security problems in higher education

3.2.1 Improving the security system in higher education institutions

Artificial intelligence (AI) and the Internet of Things (IoT) have grown in popularity because of technological advances. This has resulted in an increase in cyber security threats in recent years (Eric CK Cheng and Tianchong Wang, 2022). The number of cyber-attacks has increased significantly as the Internet's interconnection has grown, and the nature of the attacks is changing (Eric CK Cheng and Tianchong Wang, 2022). As a result, corrective action should be taken to address this issue. Improving the security system in higher education institutions is one of the possible solutions to this problem. According to Mayieka Jared Maranga and Dr Masese Nelson, 2019 recommends that higher education institutions should invest in modern research laboratories and place a greater emphasis on individual and collective cyber security research and development. Higher institution also emphasizing that top management allocate appropriate financial resources to cyber security. Large allocations are required to provide related facilities and infrastructure, including obtaining the latest technology for use in higher education institutions to enable the digitization of security systems in national educational institutions. As a result, the government must play an important role in releasing the budget so that higher education institutions can further improve their security systems. Governments should think about implementing cyber security protection. Computers, networks, critical systems, software applications, and data in higher education institutions can all be protected from potential digital threats by using cyber security. Higher education institutions must maintain customer trust by implementing such cyber security safeguards.

Other than that, those in charge of the institution can also implement training and awareness programs aimed at increasing computer user awareness (Hussain Aldawood and Geoffrey Skinne, 2019). Cyber security awareness is critical for preventing society from becoming a victim of cybercrime. This awareness must be spread to all members of society. Students, on the other hand, are the group most vulnerable to cybercrime. This is because their age and level of thinking make them easy targets for cybercrime. As a result, school students must be educated on cybersecurity to avoid becoming victims of cybercrime. Because social engineering attacks are becoming more common, training and awareness programs have been developed (Hussain Aldawood and Geoffrey Skinne, 2019). Besides that, firewalls can be installed in educational institutions to improve cyber security. Firewalls and real-time protection antivirus programs have been developed as a response, according to (Eric CK Cheng and Tianchong Wang, 2022). Users can disable remote access from the computer with the proper firewall configuration and a modern operating system, preventing hackers from taking over the user's computer. By improving the cyber security system, higher education institutions can indirectly help to strengthen their cyber security systems from being compromised by irresponsible individuals.

3.2.2 National Initiative for Cybersecurity Education (NICE) Strategic Plan.

Users must be well-versed in recognizing and reacting to suspicious phishing emails before implementing technological alternatives. The research describes the critical aspects of a finished program for testing, training, measuring, and improving an entity's cybersecurity to address and minimize the possibility of phishing assaults. This program is based on practical experience in developing and carrying out training programs and working with National Institute of Standards and Technology guidelines. Increasing overall cyber security can lower the risk of phishing-based cyber-attacks.

As the demand for cyber security professionals grows, the National Institute of Standards and Technology (NIST) must launch Project NICE alongside the cyber security framework. The NICE Framework includes suggestions and directions for education professionals to establish training programs in cybersecurity that qualify graduates to fulfil the cybersecurity demand of higher education institutions. The framework lets lecturers develop a strict cybersecurity program that complies with the requirements of higher education institutions. (NICE Academic Spotlight, 2018).

In recent educational research, NICE has also been used to identify needs. For example, a recent study has used the NICE framework to pinpoint understanding, skills, and abilities to fulfil industrial cyber security requirements (Armstrong et al., 2020). The NICE framework serves as a critical reference for connecting cybersecurity education to the needs of higher education institutions. The NICE framework improves communication among cybersecurity educators, trainers, certifiers, employers, and employees. Second, primary analysis process highlights tasks that must be completed to function effectively in a specific work capacity. Third, skill analysis determines the position's job role and related tasks. Categories, areas of expertise, and job roles are all part of the NICE framework. The NICE framework's overall organizational components are provided by category. To fill industrial shortages, the National Institute of Standards and Technology (NIST) proposes the educational institutions match the courses of study with the NICE framework.

3.2.3 Create an effective cyber risk management strategy

Cyberattacks in higher education are common not because the IT infrastructures need to be more secure but because many institutions are vast, complicated, and use multiple systems programs and software. Users can connect to the internet via tablets or smartphones, making adopting safety measures harder. Higher education institutions use various cyber risk prevention techniques, including software and hardware upgrading to internet access management, traffic, and intrusion detection systems.

According to Liluashvili (2021), a proper cyber risk management plan is among the most critical aspects of an organization's cybersecurity. There are specific methods that institutions may employ to keep themselves protected when faced with the threat of risks associated with cyber security. To defend itself against cyberattacks, an entire organization must work together. Scholars and research institutes store vital research information that needs to be protected from cybercriminals. To preserve confidential data, researchers must work tactically with system authorities (Liluashvili, 2021). Higher educational institutions might develop collaborative teams comprised of heads of departments, researchers, and critical safety personnel. It is critical to remain cautious to guarantee that appropriate safety precautions are put in place to secure confidential private information and valuable research data. For effective operations of IT, those who use technology need to be allocated proper access credentials depending on the risk exposure.

According to Liluashvili (2021), a Privileged Access Management (PAM) solution is required to automate the administration of credentials and restricted access management. Another choice is to regulate user access by staged access to administration, where the higher level allows more access to the needed but restricts access to limited users. Because hackers target administrator credentials to gain access to valuable data and acquire more influence in vulnerable systems, any particular account must be regularly watched. Having protocols for securely resetting identities like passwords, tokens, and tickers is critical. To preserve an appropriate level of cybersecurity for any organization, it is vital to compartmentalize user credentials and login access to certain employees. Due to the dangerous actor's restricted access features, the impact will be minor if a single section is hacked. There are fewer incidents of system blackouts at educational institutions that use the system.

Managing passwords is also essential for data security. Strong passwords are critical for securing business and personal information and maintaining privacy. Password policies were crucial for both regular and remote users. There are several guidelines that users need to comply with when trying to establish a password that might enhance security (Vu et al., 2007). One of the guidelines is that there must be a particular length requirement. Passwords must be at least eight characters in length. The more complicated the password, the more unlikely it is to be broken. Furthermore, users must refrain from employing basic patterns. Users need to avoid using uppercase letters at the start of a password or unusual symbols and digits at the end. Simple motifs can help with password remembering. However, they also make the password simpler to guess.

4. DISCUSSION

Based on the first issue mentioned above, having a weak security system policy can have an impact on cyber security. According to the evidence presented above, the party in charge of managing the system in higher education institutions does not update the software, and the operating system is the most vulnerable. This is because if the responsible party is not sensitive to the responsibility held, many parties will accept the consequences. This is because systems that have not been updated in a long time are more vulnerable to virus threats than devices that are serviced and updated regularly. To improve cyber security, responsible parties may consider installing firewalls in educational institutions. Some cyber threats can be blocked indirectly using a firewall. Furthermore, vendors frequently place and introduce unsafe products into the market, posing a risk. Products that are unsafe and of poor quality are frequently sold at lower prices. This will draw the attention of unscrupulous higher education institutions looking to cut costs. This is one of the primary causes of ineffective security systems. As a result, the government must play an important role in allocating additional funds so that higher education institutions can improve their security systems. Institutions with a larger budget can find higher-quality products. Furthermore, untrained workers and staff contribute to direct access attacks in large organizations, including connections to schools and universities. Untrained workers frequently make mistakes. Such errors can exacerbate cyber threats. Untrained employees are also more likely to be targeted by hackers. As a result, the party in charge of the institution can also implement training and awareness programs aimed at increasing computer users' awareness. The existence of such a program will indirectly open the eyes of the staff to a more responsible attitude toward user data. Employees will make greater efforts to learn how to use the system correctly and to prioritize safety. Finally, a lack of top management support contributes to the vulnerability of cyber systems. If the higher authorities refuse to release more funds to strengthen the system, the higher education institution will face numerous challenges. Superiors must be aware of their responsibility to strengthen their higher institutions' security systems to prevent information leakage. As a result, higher-level officials should invest in modern research labs and place a greater emphasis on individual and collective cybersecurity research and development. This is due to. A strong security system is necessary to ensure that higher education institutions' security levels are more stable.

According to Information Systems Education Research, IS courses must be formed to comply with the current needs of industries and businesses to train IS graduates for their future careers. This effort includes the Cybersecurity Framework developed by NIST, Role-Based Cybersecurity Training

Framework, National Initiative on Cybersecurity Education Strategic Plan (NICE, 2019), National INFOSEC Education and Training Program, and National Conference on Information Systems Security Education. However, no previous study has emphasized the conceptual framework to establish a cybersecurity program that meets the industry's requirements. The research's significant finding was the significance of creating a complete phishing education program in addition to email protection technologies. The National Institute of Standards and Technology (NIST) developed Project NICE alongside the cybersecurity framework to satisfy the increased request for cybersecurity specialists. The project’s framework offers recommendations and guidelines for professionals in education to build cybersecurity training programs that prepare graduates to fulfil the industry's cybersecurity demands. The framework offers lecturers to create a strict cybersecurity program that meets the demands of the marketplace (NICE Academic Spotlight, 2018). For example, utilizing the NICE framework, a recent study has highlighted understanding, skills, and abilities to address industrial needs in cyber security (Armstrong et al., 2020). As main guidance, the framework significantly connects cybersecurity training with industrial demands in various ways. The National Institute of Standards and Technology (NIST) suggests educational institutions match the programs with the NICE framework to fill industrial gaps.

Cyber-attacks are becoming more common across every sector. The increasing focus on assaults on government institutions and important infrastructure has heightened interest in cybersecurity measures and laws. Higher education networks necessitate a complicated blend of convenient accessibility and very efficient safety measures. Because higher education institutes keep private and sensitive information of students and employees, they have become A popular aim for hackers seeking for the purpose of stealing data stored by these institutions. Furthermore, most colleges are becoming more forthcoming and open about their infrastructures. These educational institutions ensure that students and parents may access their sites fast and efficiently. This unintentionally opened the way for cybercriminals. Email phishing is a simple approach for cybercriminals to get access to university or college systems. Scholars and workers at higher education institutions can easily accept and finally fall for this hacker's fraud if just a trustworthy domain name such as '.edu' or '.org' is used. This security problem can be reduced by implementing a Privileged Access Management (PAM) system. This is because PAM software can allow safe distant access without requiring outsiders to supply domain identification, restricting access to necessary sources, and lowering the probability of illegal access to sensitive information. It can also guarantee that all external activities are tracked and documented.

5. CONCLUSION

Cybersecurity is no longer a hidden issue that only hackers are aware of. Higher education institutions have become more vulnerable to the problem as internet usage has increased. Due to a lax management environment, many higher education institutions are vulnerable to cyber-attacks. Based on our observations, hackers can exploit flaws in the defense system to steal data from any individual involved in a higher education institution, whether they are students, instructors, or staff. All higher education institutions that are transitioning from paper-based data should pay close attention to and prioritize cybersecurity when storing, accessing, and retrieving critical information. In this era, protecting information and data is a requirement for most higher education institutions around the world because data is an asset that can become problematic later if it falls into the hands of unauthorized individuals. Although cybercrime cannot be completely eradicated, higher education institutions must remain vigilant when using the internet to ensure that all online transactions are completed safely and without any data leakage. Therefore, higher education institutions must work together to maintain constant focus and attention to ensure information security, as well as implement appropriate security controls to prevent information leakage.

Acknowledgments: This research was funded by the Universiti Teknologi MARA Kelantan Branch. Therefore, we would like to express our gratitude for the funds provided that enable the writer to participate in the Glocal

Symposium on Information and Social Sciences GSISS, 2023 program organized by the School of Information Science, College of Computing, Informatics and Media UiTM Kelantan Branch.

References

Adams, A., Sasse, M. A., & Lunt, P. (1997). Making passwords secure and usable. *People and Computers XII*, 1–19. https://doi.org/10.1007/978-1-4471-3601-9_1

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3), 73. https://doi.org/10.3390/fi11103007

AL-Nuaimi, M.N. (2022), "Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: a systematic review", Global Knowledge, Memory and Communication, Vol. ahead-of-print No.ahead-of-print. https://doi-org.ezaccess.library.uitm.edu.my/10.1108/GKMC-12-2021-0209

Alzahrani, B., Bahaitham, H., Andejany, M., & Elshennawy, A. (2021). How ready is higher education for quality 4.0 transformation according to the LNS research framework?. *Sustainability*, *13*(9), 5169.https://doi.org/10.3390/su13095169

Aruna, P. (2019, November 29). *Combating cyber crimes*. The Star. https://www.thestar.com.my/business/business-news/2017/11/18/combating-cyber-crimes/

Carson, J., & FitzGerald, A. (n.d.). What is Privileged Access Management (PAM)? https://delinea.com/what-is/privileged-access-management-pam

Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. Journal of Cybersecurity, 5(1), tyz001. https://doi.org/10.1093/cybsec/tyz001

Chabrow, E., & Ross, R. (2015, May 15). *China blamed for Penn State Breach*. DataBreachToday. http://www.databreachtoday.com/china-blamed-for-penn-state-breach-a-8230

Chang, C. H., Wenming, S., Wei, Z., Changki, P., & Kontovas, C. A. (2019, November). Evaluating cybersecurity risks in the maritime industry: a literature review. In *Proceedings of the international association of maritime universities (IAMU) conference*. https://doi.researchonline.ljmu.ac.uk/id/eprint/11929

Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information*, *13*(4), 192. https://doi.org/10.3390/info13040192

Fouad, N.S. (2022), "The security economics of EdTech: vendors' responsibility and the cybersecurity challenge in the education sector", Digital Policy, Regulation and Governance, Vol. 24 No. 3, pp. 259-273. https://doi-org.ezaccess.library.uitm.edu.my/10.1108/DPRG-07-2021-0090

Futcher, L., Schroder, C. and von Solms, R. (2010), "Information security education in South Africa", Information Management & Computer Security, Vol. 18 No. 5, pp. 366-374. https://doi-org.ezaccess.library.uitm.edu.my/10.1108/09685221011095272

Kundy, E. D., & Lyimo, B. J. (2019). Cyber Security Threats in Higher Learning Institutions in Tanzania, A Case of University of Arusha and Tumaini University Makumira. Olva Academy–School of Researchers, 2(3), 2.

Liluashvili, G. B. (2021). Cyber risk mitigation in higher education. *Law and World*, *7*(2), 15–27. https://doi.org/10.36475/7.2.2

Lötter, A., & Futcher, L. (2015). A framework to assist email users in the identification of phishing attacks. *Information & Computer Security*, *23*(4), 370–381. https://doi.org/10.1108/ics-10-2014-0070

Maranga, M. J., & Nelson, M. (2019). Emerging issues in cyber security for institutions of higher education. International Journal of Computer Science and Network, 8(4), 371-379.

Mogoane, S. N., & Kabanda, S. (2019). Challenges in information and cybersecurity program offering at Higher Education Institutions. *Kalpa Publications in Computing*, *12*, 202–212. https://doi.org/10.29007/nptx

Rahim, N., Othman, Z., Hamid, F. Z., & Yeop, O. (2020). Cyber Security and the Higher Education Literature: A Bibliometric Analysis. *International Journal of Innovation, Creativity and Change*, *12*(12), 852–870.

Rastenis, J., Ramanauskaite, S., Janulevicius, J., & Cenys, A. (2019). Credulity to phishing attacks: A real-world study of personnel with Higher Education. *2019 Open Conference of Electrical, Electronic and Information Sciences (eStream)*. https://doi.org/10.1109/estream.2019.8732169

Rohan, R., Funilkul, S., Chutimaskul, W., Kanthmanon, P., Papasratorn, B., & Pal, D. (2023a). Information security awareness in higher education institutes: A WORK IN PROGRESS. *2023 15th International Conference on Knowledge and Smart Technology (KST)*. https://doi.org/10.1109/kst57286.2023.10086884

Shan, M. and Yang, J. (2022), "Investigating the accessibility and impacts of cybersecurity programs on high-school girls' long-term industry engagement", Information and Computer Security, Vol. 30 No. 3, pp. 309-323. https://doi-org.ezaccess.library.uitm.edu.my/10.1108/ICS-05-2021-0067

Świątkowska, J. (2020). Tackling cybercrime to unleash developing countries' digital potential. *Pathways for Prosperity Commission Background Paper Series*, (33).

Towhidi, Gelareh and Pridmore, Jeannie (2023) "Aligning Cybersecurity in Higher Education with Industry Needs," Journal of Information Systems Education: Vol. 34 : Iss. 1 , 70-83. Available at: https://aisel.aisnet.org/jise/vol34/iss1/6

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, *13*(2), 39. https://doi.org/10.3390/fi13020039

Vu, K.-P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B.-L. (Belin), Cook, J., & Eugene Schultz, E. (2007a). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, *65*(8), 744–757. https://doi.org/10.1016/j.ijhcs.2007.03.007

Weirich, D., & Sasse, M. A. (2001). Pretty good persuasion: A First Step Toward Effective Password Security in The Real World. *Proceedings of the 2001 Workshop on New Security Paradigms*. ttps://doi.org/10.1145/508171.508195

Research Article

Assessing The Relationship of Ethics and Morals in Information Technology

Aisyah Radhiah Mohamad Azri[1], Nur Adilah Hanim Nordin[2], Nur Athirah Husna Mohd Faddli[3] and Nurulannisa Abdullah[4,*]

[1] Universiti Teknologi Mara; 2020852818@student.edu.my; 0009-0000-0129-2883
[2] Universiti Teknologi Mara; 2020489008@student.uitm.edu.my; 0009-0001-8814-9963
[3] Universiti Teknologi Mara; 2020846724@student.uitm.edu.my; 0009-0004-0388-1066
[4] Universiti Teknologi Mara; Nurulannisa Abdullah; 0000-0002-5294-9125
[*] Correspondence: annisa@uitm.edu.my; 019- 3633936.

Abstract: The concept of morality and ethics involves evaluating both good and evil in the context of the rules that govern an institution. But there is some argument about what constitutes morality and the guiding principles known as ethics, particularly in the context of research, which calls into question this idea. While ethics emphasizes a social structure in which those morals are applied, morals determine a person's character. The objective of this paper is to analyze the understanding of ethical and morality arise in the technology development and to identify the ethics and morals that have been utilized in several kinds of fields. This paper collected information and documents from an online database and results from a combination of case studies, observed individual behavior and decision making processes. The findings revealed that ethics and morality in emerging fields were positively related in the edge of technology development.

Keywords: Moral; Ethics; Information Technology; Information Ethics; Information System

DOI: 10.5281/zenodo.8182891

1. INTRODUCTION

In a broader sense, ethics takes into account a person's freedom, responsibility, and sense of justice as well as how they interact with others and the surroundings. It can be said that ethics is generally concerned with human independence when it focuses on the interaction that occurs between humans and the rest of the world. This independence is a must for any impartial assessment of the facts and for ethical decision-making. Independence is shown when a person chooses to put themself as far away from their influence as possible. As long as this process demands a level of clarity that enables us to assess something objectively and select an acceptable course of action, it will be noticed that selecting an ethical course of action is hard. The distinction between suitable (good) and improper (wrong) intentions, decisions, and acts is known as morality (from the Latin moralitas, "manner, character, proper behavior"). Morality can be a set of rules or guidelines that are drawn from a code of conduct that is specific to a philosophy, religion, or society, or it can be a norm that an individual feels ought to be universal. Another way to express morality is as a synonym for "goodness" or "rightness". Although there are some distinctions in their usage, morals and ethics are both used in the plural and are frequently regarded as synonyms. A person's personal standards of what is right and wrong are commonly referred to as their morals. Even if the word "ethics" may be used to refer to moral principles more widely, it is typically employed to explore questions of proper action in a relatively small number of contexts.

2. LITERATURE REVIEW

2.1 Ethics

Every culture has a set of laws that establish the boundaries of what is considered appropriate behavior. The individual rules all come together to produce the moral code by which a community lives, and they are frequently articulated in statements about how individuals should behave. Unfortunately, because there are so many different regulations, it can be confusing for people to know which one to follow.

The Ancient Greek word thikós, which means "relating to one's character," is the source of the English word ethics, which itself is derived from the root word êthos, which means "character, moral nature." This word was translated into Latin as ethica, from which it was taken into French as éthique, and finally into English. A subfield of philosophy known as ethics is focused on how people behave, particularly how they act in social situations. In order to understand what is morally right or wrong, just or unjust, ethics investigates the intellectual justifications for our moral judgements. In a broader sense, ethics considers how people interact with one another and with nature, as well as their own freedom, responsibility, and sense of justice (Singer, 2018).

According to Baker's (2008), the fundamental concepts of ethics are "should and ought" in life. However, ethics also relates to the values of acceptable and unacceptable behavior. The term "ethics" is not just a phrase; it refers to understanding and adopting moral values in our daily life (Baker, 2008). There are many different types of ethics and virtues that differ from one situation to another (Baker, 2008). Aristotle pointed to two within our soul. The first engages in reasoning and the second in that "cannot itself reason" (Kraut, 2010). However, in order to become "virtuous and practically wise" we must go through the two stages: develop proper habits in childhood and gain "practical wisdom" (Kraut, 2010). And only when the two fuse, are the ethical virtues fully developed (Kraut, 2010)

Information technology (IT) ethics have been gaining a lot of attention recently. Most people rely on technology in both their personal and professional life, and it is practically ubiquitous (Nissenbaum, 1998).Data storage, utilization, and transmission between various computer systems are all made available by information technology. In a wide range of sectors, including healthcare, banking, education, and more, people rely on IT. It is important to understand why ethics are important in information technology. The right use of information technology is therefore necessary to appreciate its full significance and enhance human development. Ethics must be taken into consideration in the application and development of information technology. This will ensure that societal problems are not amplified and spread by technology.

2.2 Moral

A moral, commonly referred to as a message or the lesson to be gained from a story or an event, originates from the Latin term morālis . The moral may be implicitly conveyed in a maxim or left up to the listener, reader, or viewer to decide for themselves. A moral is also a lesson learned through a tale or from experience. In another sense, morals are the accepted norms of conduct that allow individuals to coexist peacefully in groups. While morality refers to what is sanctioned by societies as proper and appropriate. Most people have a tendency to behave decently and obediently.

Morality often calls for putting society ahead of one's own short-term interests. Amoral individuals or entities do not care about right or wrong, whereas immoral individuals or entities commit wicked deeds. The term "morality" refers to the particular values held by a given community at a certain moment. Morality has historically had a strong connection to religious traditions, but today the secular world recognises its importance as well. Businesses and governmental organizations, for instance, have codes of ethics that personnel are obliged to follow and abide by.

Several main technological advancements that raise issues of morality and ethics such as nuclear technology, biotechnology, and information technology (IT). The main moral or ethical problems with technology include gender, health problems, employment displacement, and ethical dilemmas. In terms of IT, the topic of whether it is morally right or wrong to share confidential information within a company is brought up. Utilizing computer programmes, businesses can gather data on individuals and even utilize that data for their own gain without regard to morals.

2.3 Information System

Technological advances make it easy for users easily modify records, making concerns about the accuracy and reliability of the data. Utilisation of technologies have the ability to bring about a great deal of harm among the defenceless, which is unethical. Such a problems, which resulted in a number of health issues, is shown by the fact that nuclear technology has the potential to kill countless people and further ruin the environment. In addition, numerous persons who were impacted by nuclear pollution, such as those seen in Hiroshima and Nagasaki, are thought to have genetic conditions. These effects could negatively impact the afflicted persons' future generations.

The components of modern technology that raise moral and ethical questions need to be recognised and handled with regard for all parties involved. Some philosophers argue between ethics and morality. However, a lot of individuals misinterpret the terms morality and ethics when referring to subjective verdicts, deeds, or ideals. Morals are the standards for appropriate behavior in a society with democracy. Although morality can change over time, it nevertheless serves as a benchmark by which we determine what is good and wrong.

3. METHODOLOGY

The objective of this paper is to assess the relationship between ethical and morality arise in the information technology and to identify the utilization of ethics and morals in various fields. An analysis has been conducted by reviewing previous literatures including researches, papers and other sources to identify the needs. A literature review surveys books, scholarly articles, and any other sources relevant to a particular issue, area of research, or theory, and by so doing, provides a description, summary, and critical evaluation of these works in relation to the research problem being investigated. This study will first review various meanings of ethics and morals and their characteristics. Based on this understanding, a classification method will be developed to categorize and identify the relationship between ethics and moral in the selected field.

4. FINDING

4.1 Business

Corporate business environments demand high standards of morality and ethics. Ethics and morality are frequently used together, although they are completely different conceptions that require careful differentiation to prevent misunderstanding. Depending on the environment they live in, various people have different ethics and morals. In a business set up, issues related to ethics are based on an individual's good conduct or misconduct in relation to the workplace expectations (McHenry, 2003, p. 1). All employers require their employees to be morally upright.

Each party to a contract has a responsibility to carry out their responsibilities effectively and on time. Whether it's cash, goods, or services, each party must exchange something of value. Morals and ethics both have a place in business, even though these concepts are not typically associated with value. Consider a newly established company that has only recently opened for business. Their recent public relations have been mediocre, despite their above average sales. Due to their moral failings and unethical actions, they might be able to land a few contracts with smaller businesses, but they have very little chance of growing as a business. While morality and ethics clearly play a vital role in business, the obligations outlined in each building contract are generally based on legal requirements rather than just morality and ethical behavior.

When a party signs a contract, it could have responsibilities that go against their morals but not necessarily against the law. Unfortunately, if any of the contractual responsibilities go against company ethics, a corporation almost always cannot break the agreement. The contract may only be invalid when laws are broken. The main difference between ethical obligations and contractual obligations is that, if a party does not uphold them, there are no legal consequences. In contrast, if one party breaches a contract, the offending party may face legal repercussions. Laws, which are the rules and regulations that law enforcement enforces, are contractual obligations. Ethics, on the other hand, are the accepted social standards of a particular group or culture.

4.2 Social Aspects

In the words of Victor and Cullen (1988, p. 101), there is an increasing belief that organizations are social actors accountable for the ethical and illicit conduct of their workers. This opinion is supported by the widespread agreement that situational influence can improve both morals and immoral behavior. When moral surroundings are taken seriously, a fundamentally social picture of the good life emerges, with participants cooperating and competing but at least having shared ideals. As a theoretical and useful concept of moral ecology, it connects environmental philosophy, notably lessons from the "tragedy of the commons" to the moral and social worlds. It implies that the idea of moral ecology offers a convincing representation of real-life human behaviors.

A word of caution beforehand. It seems likely that the perceived moral ecology has an equal impact on behavior as the real moral ecology. According to an examination done at the individual level, a person's perception of the moral context affects their choices and actions more than the actual moral environment would (Victor and Cullen, 1988). Of course, because other players in the ecosystem act on people's perceptions, moral ecology can have an impact regardless of how they perceive the world. Individuals can act against their views of a moral ecosystem that does not support them, much as in the case of whistleblowers. However, even the "objective" moral ecosystem is largely influenced by the attitudes, commitments, and intents of its participants. One of the challenges facing participants in moral ecology is its complicated subjective nature. Measuring moral ecology likewise faces substantial challenges due to this complexity.

The moral ecosystem, like the other parts of the paradigm, influences behavior rather than causing it in most cases. It also alters in shape and strength depending on the times and circumstances, just like the other parts of the model. As a result, while some circumstances may yield a high degree of agreement about wrongdoing, other circumstances can give room for individuals with different personalities, moral convictions, or skill sets to make their case. Due to the fact that it both impacts and is impacted by the individual, this aspect is more complex than the others.

4.2.1 Ethics Codes and Moral Ecology

Ethics codes are becoming more prominent and prevalent as a result of the belief that they help to define responsibilities and prevent unethical behavior (Harrington, 1996). There is hardly any work that really evaluates how professional codes affect professionals' behavior. Professionals in the field of computing occasionally utilize professional codes as justifications for or against specific design decisions. Even though some of our 24 moral role models had served on committees to draft codes, it is interesting to note that none of them mentioned the importance of professional ethics codes in their interviews with moral role models in computers (Huff and Rogerson, 2005; Huff and Barnard, n.d.). There was a lot of chance to talk about the impact of codes because everyone was particularly asked to name influences on their behaviour during these open interviews, which lasted longer than three hours apiece. We may discover this conflicting pattern of rule effects in the research on organizational ethical codes. The basic objective of organizational ethics codes is to officially state the organization's point of view on moral issues. Some of them have definite rewards, sanctions, or punishments, and they outline broad principles and procedures.

There are many varieties in this area. For instance, Marnburg (2000) identifies 16 fundamental principles that organizational ethics codes frequently contain and groups them into four major categories: capability (creating as much value as possible), integrity and equality, stability (keeping commitments and expectations), and/or protecting the future (taking care of the environment and future generations). On each of these dimensions, codes differ greatly from one another, and presumably moral ecology is no different. Compared to smaller organizations, larger corporations or organizations are more likely to have ethics codes. Only 25–33% of organizational ethics codes have formal processes in place to deal with violations. It is hardly surprising that these codes may have distinct behavioral impacts than those that have no formal repercussions.These compliance-based rules (Paine, 1994; Weaver and Trevino, 1999) usually focus on controlling the behavior of their staff in order to reduce the prevalence of illicit conduct. They maintain this control by strictly adhering to rules and regulations. However, everything that is not expressly forbidden is frequently taken to mean that it is allowed.

4.2.2.1 Organizational Moral Ecology

The practical limitations, moral attitudes and working conditions for a company’s employees are undoubtedly impacted by the moral ecology that it cultivates and upholds. The unspoken expectations and guidelines that a corporation has for its employees have a greater impact on the moral ecosystem than any written code or set of principles. A business with a caring ethical culture priorities providing excellent customer service. The obligation to "workers, management, and the community" is of secondary importance. Financial returns are least important in this situation. Climate regulations is the propensity of an organization to make ethical decisions based on guidelines created by outside parties, such as laws or professional codes. Using internally created codes to make decisions is referred to as the rule's climate. Due to the instrumental environment, the main drivers are self-interest and financial gain. Last but not least, the independent atmosphere characterizes occupations where individuals are reminded to preserve their own moral principles. The greatest mean score determines the impression of the dominant environmental type, or moral ecology, in these surveys, which derives a mean score for each of these five climate types.

4.3 Healthcare

A good use of technology is one which improves human physical, mental, spiritual, and moral well-being. It can help people become healthier, more educated, more loving and better at making moral decisions. Bad or overuse technology will do the opposite such as make us sicker, less educated, less loving of others, and worse at making moral decisions. Technology often simply makes actions easier for us and we want good technology that will facilitate good actions, not bad technologies that will facilitate bad actions.

Ethical values are essential for any healthcare provider. Ethics within healthcare are important because workers must recognize healthcare dilemmas, make good judgments and decisions based on their values while keeping within the laws that govern them. To practice competently with integrity, nurses, like all healthcare professionals, must have regulation and guidance within the profession. It is important for the nurse to understand all privacy guidelines with regards to patient care and patient identifiers (Epstein B, 2015).

Other than that, ethical values are also essential for all healthcare workers. Ethical practice is a foundation for nurses, especially those who deal with ethical issues daily. Ethical dilemmas arise as nurses care for patients. There are four main principles of ethics such as autonomy, beneficence, justice, and non-maleficence (Haddad, L. M, 2022). Each patient has the right to make their own decisions based on their own beliefs and values (Morrell TJ, 2019). This is known as autonomy. A patient's need for autonomy may conflict with care guidelines or suggestions that nurses or other healthcare workers believe is best. Healthcare workers also have a duty to refrain from maltreatment, minimize harm, and promote good towards patients (Haddad, L. M, 2022).

In addition this duty of particular treatment describes beneficence. Healthcare workers demonstrate this by providing a balance of benefits against risks to the patient. Assisting patients with tasks that they are unable to perform on their own, keeping side rails up for fall precautions, or providing medications in a quick and timely manner are all examples of beneficence (Haddad, L. M, 2022). Many organizations have ethics boards in place to review ethical concerns. It is also important to advocate for patient care, patient rights, and ethical consideration of practice (Haddad, L. M, 2022). Ethics inclusion should begin in medical school and continue as long as the healthcare professional is practicing.

5. DISCUSSION

Information technology (IT) ethics have attracted a lot of attention recently. Most people rely on technology in both their personal and professional lives, and it is practically ubiquitous. In critical industries like healthcare, banking, education, and more, almost everyone depends on IT. Understanding the value of ethics in information technology is crucial. Other than that, ethics are a standard that helps to ensure people behave honestly. IT is still being developed, monitored, and used in a way that is based on ethics. Personal information must not be tainted or used in any way that is harmful or negative. Technology ethics must advance along with technology's power in order to protect the people and organizations that rely on it.

After that, keeping the human element of technology in place is a part of information technology ethics. Human values and attitudes are employed to ensure that the systems on which we rely can be maintained and continue to provide useful, beneficial gains to meet our needs. Information technology has significantly improved human health. Equipment for hospitals and medical supply companies frequently uses information technology in their manufacturing processes. An unborn child can now be seen long before it is born thanks to information technology. These information technology developments should be utilized to improve human health. However scenarios arise where it is used unethically in health matters.For instance, information technology can be utilised to encourage abortions or to identify an unborn child's gender with the goal of aborting the child if it is not what the parents were hoping for.

Moral conflicts arise when good and evil are in conflict with one another. The question of whether it is ethically proper or bad to exchange secret information within an organization comes up often in the context of IT. Businesses can collect data on people using computer programmes and even use that data for their own advantage without regard to morality. Users' ability to swiftly update records made available by information technology raises questions about the quality and reliability of the data. In addition, could genetic engineering improve or impair life quality? These are a few of the outstanding ethical issues. Additionally, biotechnology raises certain ethical questions. It is difficult to defend the use of living human beings for research and other technological breakthroughs. For instance, women who are unable to conceive might undergo the vitro fertilization procedure. Because these practices go against their philosophies, religious organizations are against them.

When it comes to ethical or moral issues in information technology, gender is an important consideration. Most frequently, prejudice against women is manifested in a variety of technical developments. For instance, it is believed that men are more productive than women in systems of manufacturing. Males have developed and continue to make many technical advances, and they subsequently construct the systems to favour their gender, which has an influence on the question of gender equality. For instance, the computer business is more male-dominated since women like straightforward subjects. Many female students avoid majors in science, technology, engineering, and math, or if they do, they frequently drop out due to the intimidating environment.

6. CONCLUSION

The study has investigated and identified the relationship between ethical and morality arise in the information technology development and the utilization of ethics and morals in various fields. The investigation led to identifying various meanings of ethics and morals and their characteristics since it has different implications for different fields.

The study has contributed to the understanding of why ethics are important in IT. The findings proved that ethics serve as a guide to help people act honorably. Apart from that, keeping the human element of technology in place is a part of information technology ethics to ensure that the system we rely on provides benefits to meet our needs. In morality, it is an issue in the IT field such as sharing confidential information always becomes the point of discussion whether it is right or wrong. This is because IT allows users to modify and alter the records which will interfere with the authenticity of the records.

The study also assesses the ethical and moral issue of IT in various fieldsIt comes to the conclusion that almost everyone depends on IT in key sectors like business, healthcare, banking, and education. The analysis revealed that ethics and morality in those emerging fields were positively related in the edge of technology development.

Acknowledgments: The authors would like to thank the lecturers from the Faculty of Information Management for guiding us to do our research paper and keep supporting us until we are able to complete the paper easily.

References

Alavi, M., Kayworth, T. and Leidner, D.E. (2006), "An empirical examination of the influence of organizational culture on knowledge management practices", Journal of Management Information Systems, Vol. 22, pp. 191-224.

Aristotle (1942),The Nicomachean Ethics, (translated by Ross, W.D.) Random House, New York, NY.

Bebeau, M.J. and Brabeck, M. (1994), "Ethical sensitivity and moral reasoning among men and women in the professions", in Puka, B. (Ed.), Caring Voices and Women's Moral Frames, Garland Publishing, New York, NY, pp. 240-59.

Bebeau, M.J. and Thoma, S.J. (1999), "'Intermediate' concepts and the connection to moral education", Educational Psychology Review, Vol. 11, pp. 343-60.

Gert, B., & Gert, J. (2020). *The Definition of Morality* (E. N. Zalta, Ed.). Stanford Encyclopedia of Philosophy; Metaphysics Research Lab, Stanford University. http://plato.stanford.edu/entries/morality-definition/

Ethics Unwrapped. (2022, November 5). *Morals - Ethics Unwrapped*. https://ethicsunwrapped.utexas.edu/glossary/morals

Haddad, L. M. (2022, August 22). *Nursing Ethical Considerations*. StatPearls - NCBI Bookshelf. https://www.ncbi.nlm.nih.gov/books/NBK526054/#:~:text=There%20are%20four%20main%20principles,and%20values.%5B4%5D.

Huff, C.W. (1996), "Practical guidance for teaching the social impact statement", in Huff, C.W. (Ed.), Proceedings of the 1996 Symposium on Computers and the Quality of Life, ACM Press, New York, NY, pp. 86-90.

Information Technology and Moral Values (Stanford Encyclopedia of Philosophy). (2018, November 9). https://plato.stanford.edu/entries/it-moral-values/

Kraut, R. (2018). *Aristotle's Ethics* (E. N. Zalta, Ed.). Stanford Encyclopedia of Philosophy; Metaphysics Research Lab, Stanford University. http://plato.stanford.edu/entries/aristotle-ethics/

Moral and Ethical Issues in Science and Technology. (2023, April 15). Free Essays. https://ivypanda.com/essays/moral-and-ethical-issues-in-technology/#:~:text=The%20major%20ethical%20or%20moral,%2C%20job%20displacement%2C%20and%20gender.

Singer, P. (2023, June 8). ethics. Encyclopedia Britannica. https://www.britannica.com/topic/ethics-philosophy

Santa Clara University. (n.d.). *The Relationship of Morality and Technology*. Markkula Center for Applied Ethics. https://www.scu.edu/ethics/all-about-ethics/the-relationship-of-morality-and-technology/#:~:text=A%20bad%20technology%20will%20do,that%20will%20facilitate%20bad%20actions.

The theory of moral ecology - JSTOR. (n.d.). https://www.jstor.org/stable/1408255

Treasury Board of Canada Secretariat. (2015). *What is ethics? - Canada.ca*. Canada.ca. https://www.canada.ca/en/treasury-board-secretariat/services/values-ethics/code/what-is-ethics.html#A1

Wikipedia contributors. (2022). Moral. *Wikipedia*. https://en.wikipedia.org/wiki/Moral

Research Article

Measuring the Ethics Understanding & their Behaviour among University Students: A Study at UiTM Kelantan Branch

Nur Awatif Kamarudin[1], Nor Hanisah Sakri[2], Nurshahirah Mohd Nor[3], and Mohd. Zafian Mohd Zawawi [4,*]

[1] Universiti Tekonologi MARA; 2020898536@student.uitm.edu.my; 0009-0009-1318-7701
[2] Universiti Teknologi MARA; 2020819546@student.uitm.edu.my; 0009-0002-5617-7633
[3] Universiti Teknologi MARA; 2020495328@student.uitm.edu.my; 0009-0003-0576-4747
[4] Universiti Teknologi MARA; zaffian@uitm.edu.my*; 0000-0001-7863-7034
[*] Correspondence: zaffian@uitm.edu.my.

Abstract: *This article seeks to assess the ethical awareness and conduct of undergraduate students at the UiTM Kelantan Branch. It goes into greater detail about the effects of gender and academic fields on these four moral processes. Malaysian undergraduates from the UiTM Kelantan Branch totalled 200 for the study. Based on the information received from the survey, 14 ethical statements were created. Data analysis techniques included descriptive analysis (using measures like mean), and Analysis of Variance (ANOVA). However, this survey managed to collect data from 214 respondents. In order to obtain this information and data, quantitative data collection activities were conducted through questionnaires among the students involved. The majority of the average responses from this survey indicate that undergraduate students at the University of Kelantan have an average level of ethics. However, Cronbach's Alpha accomplishment findings demonstrate that the survey's stated questions are reliable given a sample size of 30 respondents Cronbach's Alpha getting >=0.7.*

Keywords: *Students; Ethics; Academic faculty, gender, behaviours*

DOI: 10.5281/zenodo.8183005

1. INTRODUCTION

Ethical awareness should be a big concern by teaching ethical values, good morals, and integrity from childhood and continuing the good morals taught to higher students in education. This ongoing teaching in ethics may result in students who maintain the moral principles they have learned in class and future professionals equipped to handle moral conflicts when entering the workforce. According to (O'Leary, 2009), ethics can be referred to as even while a person is sensitive to or aware of ethical situations, this does not necessarily imply how their decision will turn out. Early exposure to moral issues is needed, especially for university students, who should receive instruction to gain specialisation in dealing with moral problems when facing the future. According to (Moore & Gino, 2013), when people are aware of the essential moral principles and the possible effects of their choices, they are more likely to act ethically. Controlling emotion also can be included in good morals. It is because when we are mad and in uncontrolled emotion, we are likely to do nonsense things. According to (Aquino et al. 2011, Schnall et al. 2010), positive moral emotion can be included in ethical attitudes as well. The objective of this study is twofold: first, this study determines the ethics among undergraduate students in the UiTM Kelantan Branch, based on processes, judgment, awareness, morals, behaviour, and intention. The second objective is that this paper also wants to identify differences between faculty, gender, and their level of ethics. According to (Haynes, 1998,) ethics should be a big concern since it is not only an ethical problem but also responsible for the next generation. It is crucial to learn ethics, especially for students in higher education since ethics can help with better decision-making.

Moreover, as the next generation of leaders, higher education students look forward to achieving Malaysia's aim to grow an ethical community by the year 2023. According to YAB, Minister Dato' Seri Anwar Ibrahim has encouraged us to develop "Malaysia Madani", which will make Malaysia respected and known as a flourishing nation. In order to achieve "Malaysia Madani", good values, trust, fairness, and governance is essential. Therefore, in 2023, UiTM will be one of the universities that will grab the opportunities to develop Malaysia Madani by focusing on globally marketable activities linked to the strategic plan UiTM 2025 towards becoming the best university in the world. According to(Ndoye, 2002), good education management also can contribute to national development and the quality of education is important which is related with ethical behaviour. Then, Good morals also can improve leadership which is a needed characteristic to become a leader. According to (Hassan, 2015; Hassan et al., 2014; Lu & Guy, 2014), good values and morals of a leader could impact the effectiveness of the leadership which lead to a successful growth of an organization especially in education. If a leader shows a good ethical behaviour such as fairness, honesty and trustworthy for the fellow student, the student will follow the ethical morals either and this is because they tend to follow what they have watched and seen since a leader is always describe as a role model as according to (Brown and Treviño, 2006; Lee et al., 2010) mentioned that followers look out for the behaviours of their ethical leaders, consider them as attractive and reliable role models, and eventually learn to copy those behaviours. Meanwhile, according to Eisenberger et al. (2001), specific action coming from a leader could impact work behaviour for the followers. Furthermore, according to (Gardelli, 2014: 19), schools have a big potential in helping students to develop morality and have a good life. When students have good morals, they will become more successful. That is why ethical education since childhood is a must so the children will have good morals and a sense of humour reflecting their situation. Not only that but continuing ethical education to higher students in universities also is needed to help the student have better decision-making based on good values since they will be the next generation of leaders in this country.

2. LITERATURE REVIEW

The selected research topic is "Measuring the ethics understanding & their behaviour among university students: a study in UiTM Kelantan branch". The survey that has been created was an intention for UiTM Kelantan's students regarding their understanding and behaviour regarding ethics. Therefore, the quantitative survey has been made in UiTM Kelantan as we are from there to collect the data from the students and lecturers.

The questionnaires have been divided into a few categories of graduations in the institution of Kelantan. Those categories include ages, courses, level of education, and religion. Based on the academics or courses, the data collected among the students are influenced by the results of ethics surveys. The distinctions across academic disciplines, due to the nature of work, motivate the present study to examine whether academic discipline impacts students" ethical perceptions. Ethical issues in research are of the utmost importance in 2019, according to the Centre for Innovation in Research and Teaching (CIRT). The main goal of the research is to gather information and the truth; ethical norms act as protections against the fabrication or falsification of data. In collaborative work, ethical conduct is significant since it helps to create a culture of trust, responsibility, and respect among researchers. This becomes extremely important when dealing with issues like data sharing, co-authorship, copyright regulations, confidentiality, and other associated concerns.

It is essential to uphold ethical standards if a person wants the public to accept and believe in their study. The general public anticipates that scientists will adhere to rules governing human rights, animal welfare, legal compliance, conflicts of interest, safety, health standards, and other ethical issues. The integrity of the research project is substantially impacted by how these ethical difficulties are handled, which also impacts its chance of receiving funding.

According to research, the gender differences are also affecting the results of surveys. For example, according to the article that we referred to "Ethics of Undergraduate Students: A Study in Malaysian Public Universities" (Rodzalan & Saat, 2016), the studies have looked at student ethics, paying particular attention to gender disparities. According to most of this research, female students generally display higher ethical behaviour than their male counterparts. For instance, a recent study [18] indicated that female students demonstrated higher moral and religious beliefs. Apart from that, according to the same article also, another study examined the ethical practices of 725 business students across five universities. Female students displayed more outstanding ethical behaviour than male students, according to the results of a survey asking participants to score a list of 17 ethical behaviours. In particular, they rejected preferential treatment by refusing presents or favours and were less likely to take organisational equipment for personal use. Therefore, the results support a study by [20], which discovered that female students were less likely to cheat than male students. This discrepancy might be explained by the potential adverse effects of cheating, like suspending their education. Most of the research examined in this context indicates that female students are more likely to be ethical than male students, displaying higher levels of honesty, religiosity, and a decreased desire to cheat.

3. FINDINGS

3.1 *Demographics*

A survey has been conducted among students at UiTM Kelantan with students needing to answer some questions to achieve the survey result. The question comes with two parts, part A and Part B. Part A is focused on demographic questions, including gender, age, religion, and faculty. The students were provided with some choices as their answer. For age, students can choose from 18 to 20, 21 to 25, 26 to 30 and more than 31. The highest average age level is between the ages of 21 and 25, with an average of 73.8 per cent.

In contrast, the second highest age level falls between the ages of 18 and 20, where the average is only 22.8 per cent, and age level of 25 to 30 is the lowest rating with only 2.8 percent. Furthermore, for gender, there is a female and male choice in the survey. The female gender outperformed the male gender in this survey, collecting an average of 63.1 percent of the data to the male gender's 36.9 percent. This shows female students are more concerned about ethics compared to male students. Meanwhile, for the religion, there were Islam, Buddha, Tamil, and others for students to choose from most of the respondents are Muslim; there is also Campus Kota Bharu and Machang choice since UiTM Kelantan Branch is divided into two small branches. Most of the data collected is from students in the Machang branch, where the average percentage is 72 percent, and only 16.8 percent collected data from Campus in Kota Bharu. Moreover, level of study is also a concern in this demographic section which involves Pre-Commerce, Diploma, Degree and Master and Degree is the highest rating with 69.6 percent. Then, faculty, there were six faculty participating in this survey which are Faculty of Accountancy with 11.7

per cent collected data and Faculty of Business & Management with 8.9 percent. Same as the Faculty of Administrative Science & Policy Studies. Meanwhile, for the Faculty of Computer Science & Mathematics collected data is 26.6 percent and for the College of Creative Art is 9.3 percent and the highest rating is from the Faculty of Information Management with 34.6 collected data. All students in the UiTM Kelantan Branch have an impact on the demographic data of each student enrolled in this survey, including gender, age, religion, and faculty.

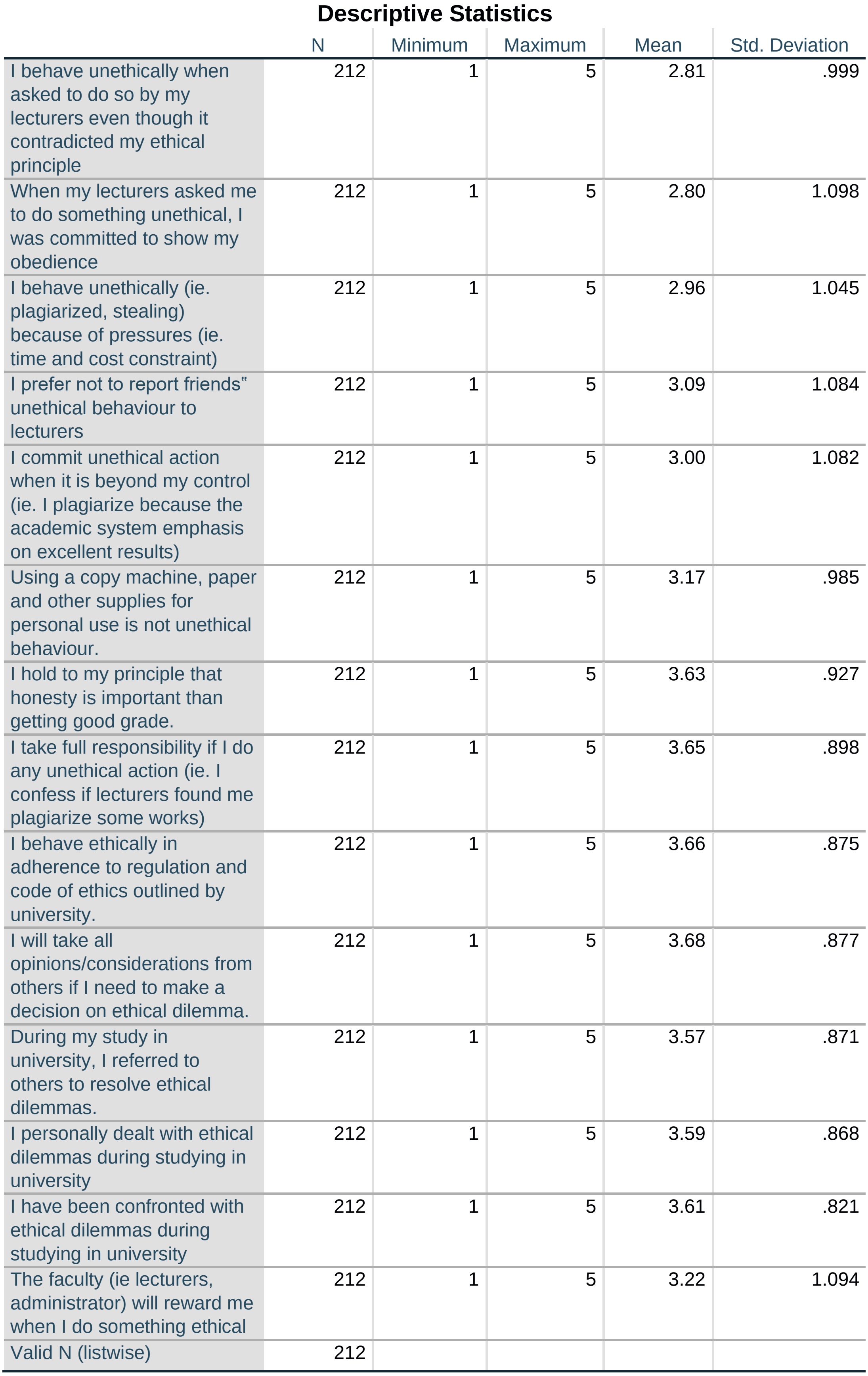
3.2 knowledge and understanding about ethics

Good questions are essential to put into a questionnaire to achieve the goals of a survey. This survey is involved with two parts which are Part A and Part B. For this Part B, students were provided with a few questions relating to knowledge and understanding about ethics. There were 14 questions provided. Which first question is about "I behave unethically when asked to do so by my lecturers even though it contradicted my ethical principle", which collected 56.10 percent, and "When my lecturers asked me to do something unethical, I was committed to showing my obedience" is 47.7 percent, and for "I behave unethically (i.e., plagiarised, stealing) because of pressures (ie. time and cost constraint)" is 43.0 percent and for the next question "I prefer not to report friends" unethical behaviour to lecturers" is 38.3 percent is the highest rating meanwhile for "I commit unethical action when it is beyond my control (ie. I plagiarise because the academic system emphasises excellent results)" is 45.3 percent as a moderate choice. Moreover, "Using a copy machine, paper and other supplies for personal use is not unethical behaviour" is 41.1 percent and "I hold to my principle that honesty is important than getting good grade" is 37.9 as the highest rating and "I take full responsibility if I do any unethical action (ie. I confess if lecturers found me plagiarising some works) is 42.1 and for this question "I behave ethically in adherence to regulation and code of ethics outlined by university" is 39.3 percent as the highest rating. Then, for this question "I will take all opinions/considerations from others if I need to make a decision on ethical dilemma", is 40.7 percent, and "During my study in university, I referred to others to resolve ethical dilemmas" is 40.2 percent and for "I personally dealt with ethical dilemmas during studying in university" is 41.6 percent as moderate and for "I have been confronted with ethical dilemmas during studying in university" is 43.0 percent and for "The faculty (ie lecturers, administrator) will reward me when I do something ethical" is 32.2 Based on these 14 questionnaire, the first question "I behave unethically when asked to do so by my lecturers even though it contradicted my ethical principle" is the highest rating with moderate as an answer compared to other question. This shows students are confused about whether to stand on their principle or follow the lecturer's instruction due to respect and to maintain the relationship with the lecturers.

4. Discussion

Based on the result that has been conducted among students at UiTM Kelantan Branch, the result shows an unexpected answer as we expected to be. The survey was provided with 14 questions with strongly agree and strongly disagree as an answer.

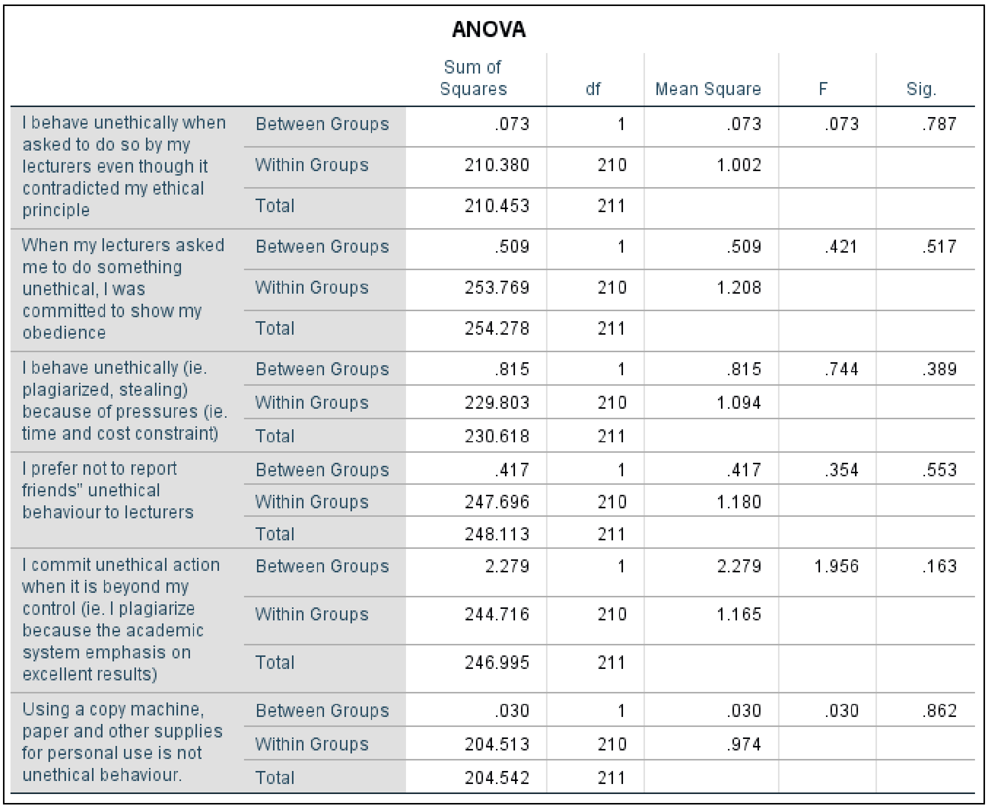
Table 1. Descriptive Statistics



Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
I behave unethically when asked to do so by my lecturers even though it contradicted my ethical principle	212	1	5	2.81	.999
When my lecturers asked me to do something unethical, I was committed to show my obedience	212	1	5	2.80	1.098
I behave unethically (ie. plagiarized, stealing) because of pressures (ie. time and cost constraint)	212	1	5	2.96	1.045
I prefer not to report friends" unethical behaviour to lecturers	212	1	5	3.09	1.084
I commit unethical action when it is beyond my control (ie. I plagiarize because the academic system emphasis on excellent results)	212	1	5	3.00	1.082
Using a copy machine, paper and other supplies for personal use is not unethical behaviour.	212	1	5	3.17	.985
I hold to my principle that honesty is important than getting good grade.	212	1	5	3.63	.927
I take full responsibility if I do any unethical action (ie. I confess if lecturers found me plagiarize some works)	212	1	5	3.65	.898
I behave ethically in adherence to regulation and code of ethics outlined by university.	212	1	5	3.66	.875
I will take all opinions/considerations from others if I need to make a decision on ethical dilemma.	212	1	5	3.68	.877
During my study in university, I referred to others to resolve ethical dilemmas.	212	1	5	3.57	.871
I personally dealt with ethical dilemmas during studying in university	212	1	5	3.59	.868
I have been confronted with ethical dilemmas during studying in university	212	1	5	3.61	.821
The faculty (ie lecturers, administrator) will reward me when I do something ethical	212	1	5	3.22	1.094
Valid N (listwise)	212				

Table 2. Analysis of Variance ANOVA

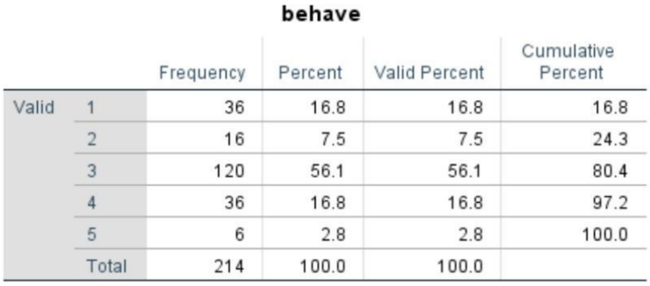


ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
I behave unethically when asked to do so by my lecturers even though it contradicted my ethical principle	Between Groups	.073	1	.073	.073	.787
	Within Groups	210.380	210	1.002		
	Total	210.453	211			
When my lecturers asked me to do something unethical, I was committed to show my obedience	Between Groups	.509	1	.509	.421	.517
	Within Groups	253.769	210	1.208		
	Total	254.278	211			
I behave unethically (ie. plagiarized, stealing) because of pressures (ie. time and cost constraint)	Between Groups	.815	1	.815	.744	.389
	Within Groups	229.803	210	1.094		
	Total	230.618	211			
I prefer not to report friends" unethical behaviour to lecturers	Between Groups	.417	1	.417	.354	.553
	Within Groups	247.696	210	1.180		
	Total	248.113	211			
I commit unethical action when it is beyond my control (ie. I plagiarize because the academic system emphasis on excellent results)	Between Groups	2.279	1	2.279	1.956	.163
	Within Groups	244.716	210	1.165		
	Total	246.995	211			
Using a copy machine, paper and other supplies for personal use is not unethical behaviour.	Between Groups	.030	1	.030	.030	.862
	Within Groups	204.513	210	.974		
	Total	204.542	211			

Table 2 presents the ANOVA results which show that there are differences in the level of ethics based on academic discipline. The differences were highly significant in all negative and positive statements as p<0.01. The faculty of administrative science and policy studies received the lowest score when compared to the faculty of information management, which can be used to further analyse the disparities in these claims. At this point, The mean difference between the six items that were chosen from the 14 that were included in this questionnaire can be seen using the ANOVA method. We may effectively compare data calculations and data observation methods using this method as well.

Table 3. (Question 1) I behave unethically when asked to do so by my lecturers even though it contradicted my ethical principle.

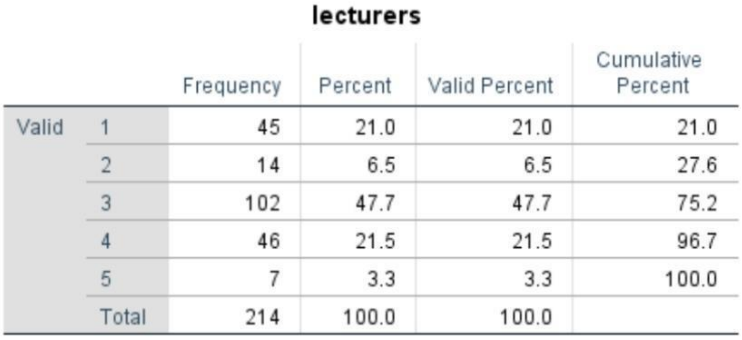


behave

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	36	16.8	16.8	16.8
	2	16	7.5	7.5	24.3
	3	120	56.1	56.1	80.4
	4	36	16.8	16.8	97.2
	5	6	2.8	2.8	100.0
	Total	214	100.0	100.0	

For the first question, the result shows most of the respondents choose moderate as the answer, 56.1 percent. This is because the student is confused whether to do or not since it was an instruction from the lecturer. The students who choose not to do it even if it was an instruction for the lecturer has a strong mindset and principle. Meanwhile, a student who did the unethical thing that was instructed by the lecturer may do it out of respect for the lecturer. Moreover, the data regarding the answer strongly disagree and agree recorded the same percentage which is 16.8 percent, and the lowest percentage is strongly agreed which is only 2.8 percent only. For instance, it shows that only a few respondents (2.8 percent) behave unethically when doing their instructions even though it contradicts their ethical principle while most respondents were moderate (56.1 percent). The highest average mean is 3.00 and it is those aged 26 to 30 years old, while the lowest average mean is 1.00 and it is among those aged 31 years and above.

Table 4. (Question 2) When my lecturers asked me to do something unethical, I was committed to showing my obedience.

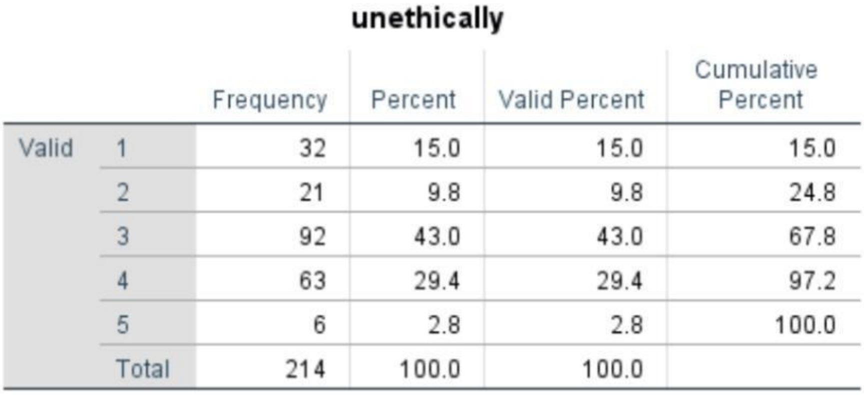


lecturers

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	45	21.0	21.0	21.0
	2	14	6.5	6.5	27.6
	3	102	47.7	47.7	75.2
	4	46	21.5	21.5	96.7
	5	7	3.3	3.3	100.0
	Total	214	100.0	100.0	

Next, the findings indicate that 47.7 percent of respondents do not actually support the stated question, with none of them expressing either excessive agreement with the assertions made or experimenting with them. Therefore, the data clearly shows that the respondents have a difficult decision whether they agree or disagree with the question they are facing. It is possible that students do not understand the question a hundred percent even though the question is asked as they have to do something unethical that is asked by their lecturers. Only 21.5 percent strongly agree, representing 45 respondents and almost half from the highest respondents wheres as 47.7 percent (102 respondents). It concludes that some of the respondents still understand the question. The highest average mean is 3.00 and it is those aged 26 to 30 years old, while the lowest average mean is 1.00 and it is among those aged 31 years and above.

Table 5. (Question 3) I behave unethically (i.e., plagiarised, stealing) because of pressures (ie. time and cost constraint).

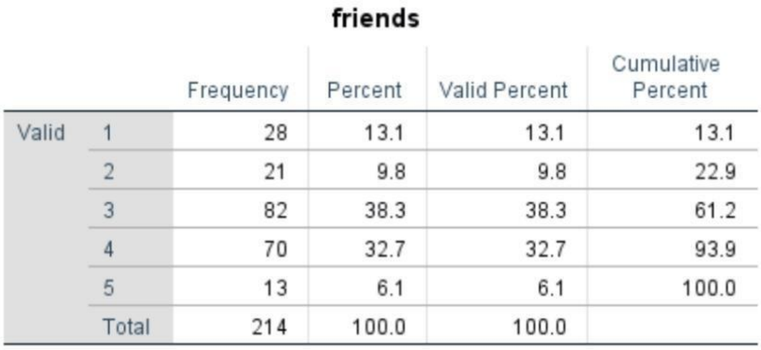


unethically

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	32	15.0	15.0	15.0
	2	21	9.8	9.8	24.8
	3	92	43.0	43.0	67.8
	4	63	29.4	29.4	97.2
	5	6	2.8	2.8	100.0
	Total	214	100.0	100.0	

Then, for this question, the result shows "I behave unethically such as plagiarising and stealing because of pressure" is moderate with 43.0 percent who cannot ascertain whether they are involved in plagiarism and stealing. This behaviour demonstrates negative qualities. However, the data was able to get information from 32 students, and the percentage of those who did not engage in immoral behaviour like plagiarism and stealing because of pressure was 15.0 percent. The second highest data is agreed that 29.4 percent define 63 respondents whereas 2: 3 with the answer for moderate (43.0 percent = 63 respondents). The results seem almost the students that are admit that they behave unethically because of pressures (ie. time and cost constraint). As students want a short way to complete their tasks so that they can complete their tasks according to submission date that have been given. The highest average mean is 3.50 and it is those aged 26 to 30 years old, while the lowest average mean is 1.00 and it is among those aged 31 years and above.

Table 6. (Question 4) I prefer not to report friends" unethical behaviour to lecturers.

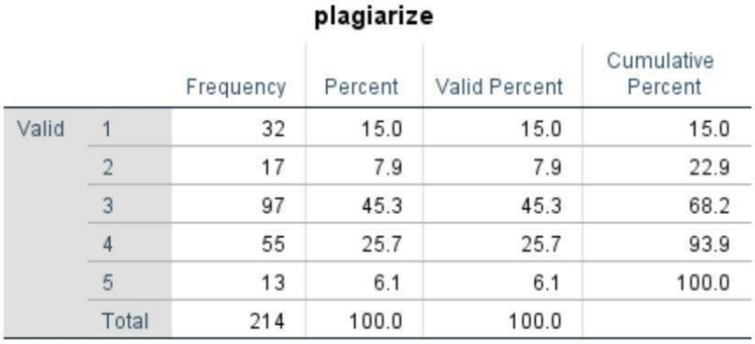


friends

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	28	13.1	13.1	13.1
	2	21	9.8	9.8	22.9
	3	82	38.3	38.3	61.2
	4	70	32.7	32.7	93.9
	5	13	6.1	6.1	100.0
	Total	214	100.0	100.0	

Other than that, according to question number 4, the results showed that there are two answers that have a competitive percentage. It is between 3 and 4 which are natural and agree (38.3 percent, 32.7 percent). The Agreed answer is the second highest percentage in the data above. Basically, most of the students agree (32.7 percent second highest data) to not report their friend's unethical behaviour to the lecturers. It seems that students prefer to not expose their friend's behaviour to the lecturers. At the same time, only 6.1 percent (the lowest data recorded) prefer to back up their friends even though they know that their friends have the wrong attitude. In comparison, the respondents that answered naturally might not be sure which is the right way to take action whenever their friends do unethical behaviour during the time. The highest average mean is 3.50 and it is those aged 26 to 30 years old, while the lowest average mean is 1.00 and it is among those aged 31 years and above.

Table 7. (Question 5) I commit unethical action when it is beyond my control (ie. I plagiarise because the academic system emphasises excellent results).

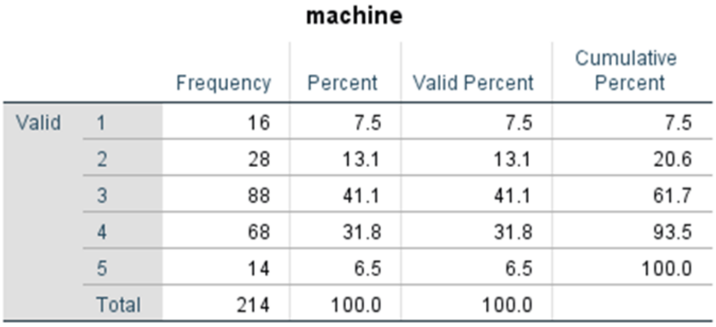


plagiarize

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	32	15.0	15.0	15.0
	2	17	7.9	7.9	22.9
	3	97	45.3	45.3	68.2
	4	55	25.7	25.7	93.9
	5	13	6.1	6.1	100.0
	Total	214	100.0	100.0	

Next, according to the data for the fifth question, the question asked whether the students commit unethical behaviour when it is beyond their control (I plagiarise because the academic system emphasises excellent results). The highest percentage is the answer moderate, 45.3 percent representing 97 respondents. While the second highest percentage is 25.7 percent, define 55 frequencies for an agreed answer. It shows almost all the respondents admit their unethical behaviour during the study process, for example, plagiarising the article whenever completing their tasks. Apart from that, there are a few frequencies that answered strongly disagree with 15.0 percent (32 frequency). It concludes that these days, there are still some students who are being honest towards their responsibility in completing their assignments among UiTM students. The highest average mean is 5.00 and it is those who are over 31 years old and above, while the lowest mean average is 2.81 and it is among those aged 18 to 20 years old.

Table 8. (Question 6) Using a copy machine, paper and other supplies for personal use is not unethical behaviour.

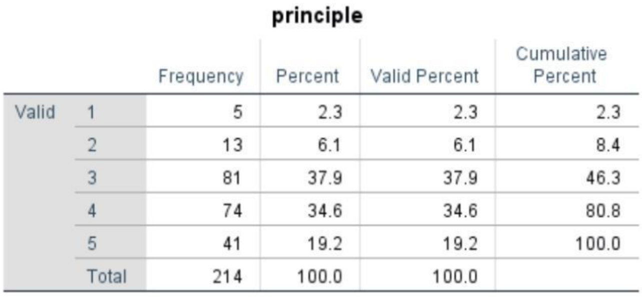


machine

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	16	7.5	7.5	7.5
	2	28	13.1	13.1	20.6
	3	88	41.1	41.1	61.7
	4	68	31.8	31.8	93.5
	5	14	6.5	6.5	100.0
	Total	214	100.0	100.0	

Furthermore, for the "using a copy machine, paper and other supplies for personal use is not unethical behaviour" question, the result shows that the respondent chose moderate as their answer 41.1 percent, ten percent higher than the answer for agree, which is 31.8 percent. It may be that they are used to using the tools that make them feel that behaviour is not unethical. This is due to the possibility that it will somewhat aid them in finishing the jobs they excel at. In fact, it can assist students in adding more information to their articles and drawing similarities with their own work. However, there are also few answers that strongly disagree, for 7.5 percent representing 16 frequencies. It seems these respondents do not think that using a copy machine, paper and other supplies for personal use is not unethical behaviour. The highest average mean is 3.50 which is among those aged 26 to 30 years, while the lowest average mean is 1.00 among those aged 31 and over.

Table 9. (Question 7) For the statement part of the question, "I stick to my principle that honesty is important to get a good grade"

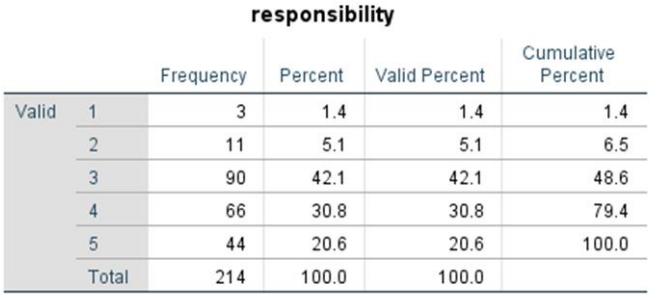


principle

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	5	2.3	2.3	2.3
	2	13	6.1	6.1	8.4
	3	81	37.9	37.9	46.3
	4	74	34.6	34.6	80.8
	5	41	19.2	19.2	100.0
	Total	214	100.0	100.0	

This survey was able to collect a frequency of 81 respondents who selected response number 3, and the percentage derived from this frequency is 37.9 percent. The data gathered shows that almost half of the population believes that being honest throughout the exam can help students succeed and earn a decent score as opposed to engaging in exam cheating. However, five students were polled on their opinions, and they found that none of them agreed that answering honestly on the test would improve their marks. Additionally, the percentage result based on the five times more disagreeable votes is 2.3 percent. This has demonstrated that there are still college students in Kelantan who have been found guilty of duplicating answers during exams. The highest mean is 5.00 and it is those who are over 31 years old, but the lowest average mean is 3.48 and they are in the age range of 18 to 20 years.

Table 10. (Question 8) Meanwhile, for this question, "I take full responsibility if I do any unethical action (I confess if lecturers found me plagiarising some works).

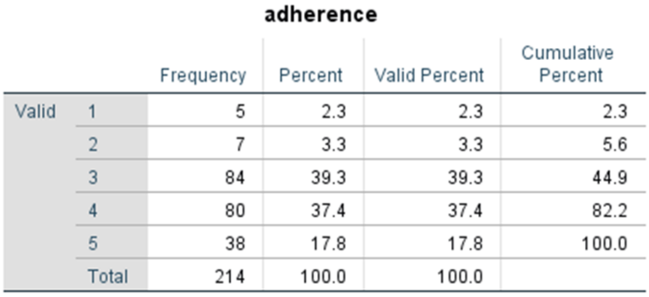


responsibility

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	3	1.4	1.4	1.4
	2	11	5.1	5.1	6.5
	3	90	42.1	42.1	48.6
	4	66	30.8	30.8	79.4
	5	44	20.6	20.6	100.0
	Total	214	100.0	100.0	

For this part it is rated as moderate as well with 42.1 percent. According to the data gathered through this study, there are 1.4 percent of students who decide not to inform and accept their fault if they are found committing a mistake, with a frequency of three times. It's possible that they're worried about the penalty they'll get later. It is a little bit disappointing since the students are not choosing to strongly agree with their answer. The highest mean number is 3.75 and it is those who are in the age group of 21 to 25 years old. But the lowest is 1.00 among those aged 31 and above.

Table 11. (Question 9). Next, for the survey question, "I behave ethically in adherence to regulation and code of ethics outlined by the university having two answers that are almost the same.

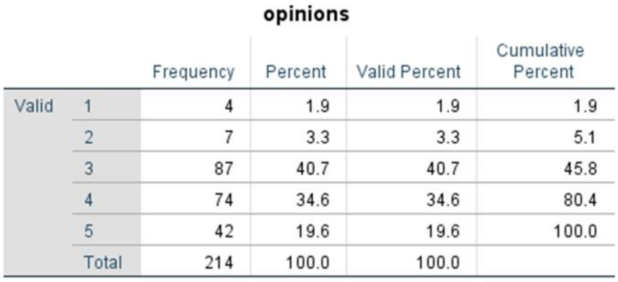


adherence

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	5	2.3	2.3	2.3
	2	7	3.3	3.3	5.6
	3	84	39.3	39.3	44.9
	4	80	37.4	37.4	82.2
	5	38	17.8	17.8	100.0
	Total	214	100.0	100.0	

There are moderate and second strongly agree (4). The percentage for moderates is 39.3 percent with 84 respondents, while the percentage for second strongly agrees at 37.4 percent with 80 respondents. When the data gathered revealed that among the students who responded to this survey question, the frequency of votes was five times against this statement, and the percentage acquired was as high as 2.3 percent, it is pretty upsetting. This has demonstrated the university's failure to uphold moral and civic behaviour among its students at all times. The highest mean number recorded for this section is 4.00 and it covers among those aged 26 to 30 years, and the lowest mean number is 1.00 recorded among students who are over 31 years old.

Table 12. (Question 10) "I will take all opinions/considerations from others if I need to make a decision on an ethical dilemma".

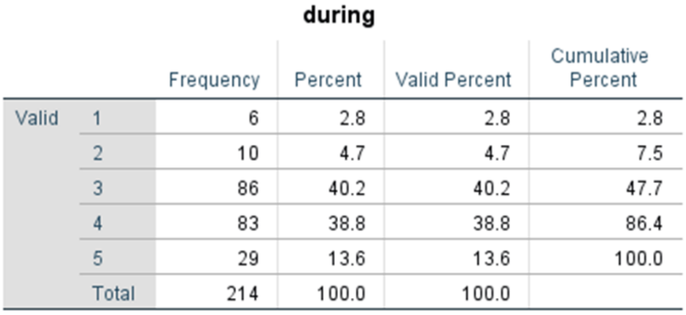


opinions

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	4	1.9	1.9	1.9
	2	7	3.3	3.3	5.1
	3	87	40.7	40.7	45.8
	4	74	34.6	34.6	80.4
	5	42	19.6	19.6	100.0
	Total	214	100.0	100.0	

The question's statement for this problem's level discusses how students should resolve ethical dilemmas by consulting outside sources, such as people and examples. Despite this, students consistently choose option three and continue to have doubts about the validity of the source they used; 40.7 percent of students chose this option, choosing to agree or disagree. If they face this moral conundrum, it's likely that they will decide to find a solution on their own rather than consulting any sources or other individuals. Next, the highest mean recorded is 3.72 and it is in the range of those aged 21 to 25 years, while the lowest is 1.00, and this number is recorded from the age group of 31 years and above.

Table 13. (Question 11) “During my study in university, referred to others to resolve ethical dilemmas”.

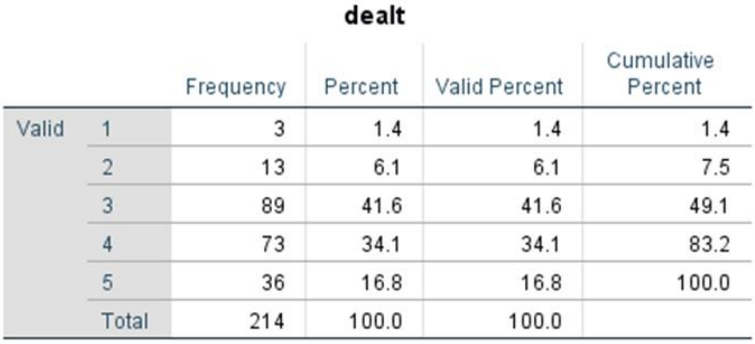


during

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	6	2.8	2.8	2.8
	2	10	4.7	4.7	7.5
	3	86	40.2	40.2	47.7
	4	83	38.8	38.8	86.4
	5	29	13.6	13.6	100.0
	Total	214	100.0	100.0	

In the survey, the average student reported that only 40.2 percent of the data collected indicated that they either strongly disagreed or did not strongly disagree with the statements in this question. Additionally, the fact that most students have doubts about their ability to solve these ethical conundrums while in college is demonstrated by the ethical dilemma-solving section of the study. "When I attended university, I was faced with a moral conundrum." The majority of students, according to 40.2 percent of respondents, are not sure if they have faced ethical dilemmas while in college. In fact, this figure shows that even if the average student is at a good level, they are concerned about ethical difficulties when they attend university. However, given that 2.8 percent of survey participants said they actually met this ethical conundrum while at university, it's likely that half of them were exposed to similar moral dilemmas. For the mean part, the most recorded the highest mean amount of 3.67 among the age group 26 to 30 years old. While the lowest mean is 1.00 among those aged 31 and above.

Table 14. (Question 12) “I personally dealt with ethical dilemmas during studying in university”.

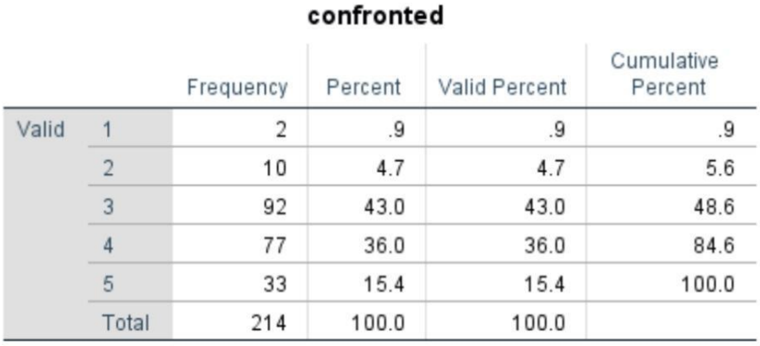


dealt

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	3	1.4	1.4	1.4
	2	13	6.1	6.1	7.5
	3	89	41.6	41.6	49.1
	4	73	34.1	34.1	83.2
	5	36	16.8	16.8	100.0
	Total	214	100.0	100.0	

The number of frequencies acquired is 89 times, and the calculated percentage rate is 41.6, indicating that students are still having second thoughts about their choice. However, the information gathered also managed to identify pupils whose frequency is three and included 1.4 percent who were unable to regulate the pomegranate's manners while enrolled in university courses. This has actually exposed the unethical side of the students who must grapple with this moral conundrum. As a matter of fact, this may have an impact on their accomplishments, their health, and other aspects of their lives. The university must also take action on this matter to inform professors about the significance and drawbacks of issues like these. For the mean part, the most the average age that has the highest mean level of 3.66 is 21 to 25 years. While the lowest mean is among those over 30 years old and recorded a mean total of 1.00.

Table 15. (Question 13) "I have been confronted with ethical dilemmas during studying in university".

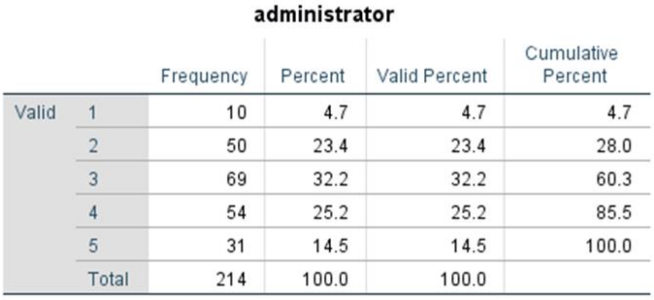


confronted

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	.9	.9	.9
	2	10	4.7	4.7	5.6
	3	92	43.0	43.0	48.6
	4	77	36.0	36.0	84.6
	5	33	15.4	15.4	100.0
	Total	214	100.0	100.0	

This question is intended to find out if other students at the University of Kelantan are experiencing ethical problems, as I did while I was a student there. The proportion calculated using the highest frequency of 92 students who selected answer number 3 is 43 percent. Most of the students who selected option number 3 were unsure of whether they had truly encountered this ethical conundrum or not. Additionally, there was the lowest frequency recorded, which was that a small number of students disagreed with the total frequency recorded of 2. Based on the frequency of these two individuals, the percentage recorded is 9 percent, clearly demonstrating that these students have never encountered this ethical dilemma. However, the response to this question in the survey revealed a sad fact when there were 33 frequencies and the percentage recorded was 15.4 per cent of respondents who selected they had encountered this issue while in college. It is hoped that the institution will recognise and address people who encounter this issue. The mean for this question who have the highest number are those in the age group over 30 years old who recorded a mean number of 5.00. However, the lowest mean is among the age group of 26 to 30 years old who recorded a mean total of only 3.62.

Table 16. (Question 14) For the last question "The faculty (i.e., lecturers, administrator) will reward me when I do something ethical.".



administrator

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	10	4.7	4.7	4.7
	2	50	23.4	23.4	28.0
	3	69	32.2	32.2	60.3
	4	54	25.2	25.2	85.5
	5	31	14.5	14.5	100.0
	Total	214	100.0	100.0	

The data reveals that most students' responses to this final question are not confident or certain; this is because most of their university faculties do not and do not usually reward students; the highest average found was only 32.2 percent nonetheless, the frequency for this percentage is 69. However, ten students claimed that neither the university nor their professors had ever given them anything to cheer them up when they had success while they were students. This has demonstrated that the students who responded to the survey are distraught and are still unsure of whether the university recognizes their accomplishments or not. This is a very unfortunate development since it may have an impact on how well future students perform. At this point, the highest of mean is 4.00 among the age from 26 until 30, while the lowest mean for this question is among the undergraduate students age more than 30. The mean for this age is only 1.00.

5. CONCLUSION

Ethic is a crucial component that must be taken care of and ingrained in each person to shape them towards a better; for instance, a humane society can exist in a state of peace and harmony without encountering any issues or being subjected to inappropriate crimes, the author wants to emphasise the importance of ethics and morality in the individual to form a good and good individual. Because this journal exists, readers can consult it and learn how crucial ethics are in a solitary life because morality affects the attitudes and situations of those around them. Based on the result that has been conducted among the student UiTM Kelantan branch, we can assume that the students are not too open and less concerned with ethical issues. According to (Kohlberg (1969, 1981), we still can create a person to an ethical behaviour through ethical training which refers to education. Moreover, universities must add an ethics subject for each cost and faculty to expose the student to good behaviour, values, morals and attitude. According to (Ponemon, 1993; Bay and Greenberg, 2001; Thomas, 2004), even though students score high positive ratings on the ethical survey also could act unethically because they do not normalize the ethical education they have learnt. Ethical education is not the only thing that is essential and is not enough to lead the student to good behaviour but normalization also is a must to create an ethical student, environment, and education as Aristotle said "educating the mind without educating the heart is no education at all".

Acknowledgements: Prior to anything else, we would like to express our deep gratitude to Sir Ts. Inv.Mohd. Zaffian agreed willingly for being our corresponding author in our symposium, for his direction, understanding, and patience, but most significantly for his encouragement and guidance in helping us complete this research study.

References

O'Leary, C. (2009). An empirical analysis of the positive impact of ethics teaching on accounting students. *Accounting Education: an international journal*, *18*(4-5), 505-520.
Rodzalan, S. A., & Saat, M. M. (2016). Ethics of undergraduate students: A study in Malaysian public universities. *International Journal of Information and Education Technology*, *6*(9), 672.

Debes, G. (2021). Teachers' and administrators' perception about the concepts of "ethical behavior" and "attitude". *International Journal of Curriculum and Instruction, 13*(1), 756–772

Cremer, D. D., Moore, C. (2019). Toward a Better Understanding of Behavioral Ethics in the Workplace. *The Annual Review of Organizational Psychology and Organizational Behavior, 7,* 369-93.

Drumwright, Minette & Prentice, Robert & Biasucci, Cara. (2015). Behavioral Ethics and Teaching Ethical Decision Making. *Decision Sciences Journal of Innovative Education. 13*. 10.1111/dsji.12071

Su, X., Lin, W., Wu, J., Zheng, Q., Chen, X., & Jiang, X. (2021). Ethical Leadership and Knowledge Sharing: The Effects of Positive Reciprocity and Moral Efficacy. SAGE Open, 11(2). https://doi.org/10.1177/21582440211021823

Xia, Zhichen & Yang, Fan. (2020). Ethical Leadership and Knowledge Sharing: The Impacts of Prosocial Motivation and Two Facets of Conscientiousness. *Frontiers in Psychology. 11*. 10.3389/fpsyg.2020.581236.

Gülcan, Nur. (2015). Discussing the Importance of Teaching Ethics in Education. *Procedia - Social and Behavioral Sciences.* 174. 2622-2625. 10.1016/j.sbspro.2015.01.942.

Amadi, Chikweru. E. Emenike. O. (2019). Influence of Ethics and Training on Students' Academic Achievement in Public Senior Secondary Schools in Phalga, Rivers State. I*nternational Journal of Innovative Social & Science Education Research 7*(4):55-63

Research Article

The Importance of Information Skill In Digital Age

Mhd Yusuf Ahmad[1], Muhammad Zulhaziq Muhammad Sidek[2] , Nur Ili Naj'aa Zainudin[3], Nur Shairah Atiqah Mohd Hamzar[4] and Najatul Afiqah Mohd Affandi[5,*]

[1] Universiti Teknologi Mara; yusufftaiyyob@gmail.com
[2] Universiti Teknologi Mara; Haziqsidek2001@gmail.com
[3] Universiti Teknologi Mara; ilijaaz1a@gmail.com
[4] Universiti Teknologi Mara; shairah.atiqah@gmail.com
[5] Universiti Teknologi Mara; najatul@uitm.edu.my
[*] Correspondence: najatul@uitm.edu.my; +60 13-325 2500.

Abstract: In the digital age, the rapid advancement of technology has transformed the way we access, process, and utilize information. As a result, information skills have become increasingly crucial for individuals to navigate and thrive in this information-rich environment. This abstract explores the problem of information overload and the lack of information literacy among individuals, which hinders their ability to effectively evaluate and utilize information. The solution proposed is to enhance information skills through comprehensive educational programs and training, empowering individuals with the necessary tools to critically analyze, interpret, and apply information in various contexts. The impacts of improving information skills are manifold, ranging from improved decision-making and problem-solving abilities to increased digital citizenship and media literacy. Additionally, individuals equipped with strong information skills are more likely to engage in lifelong learning, adapt to changing technologies, and effectively participate in the digital economy. Furthermore, this abstract highlights the commercialization potential of information skill development, as organizations can capitalize on the demand for information literacy training by offering tailored programs, consulting services, and innovative digital tools. The importance of information skills in the digital age cannot be overstated, as it has far-reaching implications for individual empowerment, societal development, and economic growth. By recognizing the significance of information literacy and implementing measures to enhance these skills, we can foster a more informed and knowledgeable society capable of harnessing the vast potential of the digital era.

Keywords: information skills, digital age, information overload, information literacy, educational programs.

DOI: 10.5281/zenodo.8183171

1. INTRODUCTION

In today's rapidly evolving digital age, information has become an invaluable currency that shapes every aspect of our lives. With the vast amount of data available at our fingertips, the ability to navigate, evaluate, and effectively utilize information has become a critical skillset. Information skills are no longer optional, they are essential for success in academic, professional, and personal spheres.

Information skills encompass a broad range of abilities, including critical thinking, information literacy, digital literacy, and media literacy. These skills empower individuals to effectively evaluate, interpret, and use information in an increasingly complex digital landscape. They go beyond mere searching and skimming, enabling us to discern reliable sources from misinformation, analyze data critically, and make informed decisions.

In today's digital age, misinformation and disinformation proliferate at an alarming rate, blurring the lines between fact and fiction. The ability to navigate this informational minefield is essential for individuals to safeguard themselves against manipulation and make well-informed choices. Information skills equip us with the tools to critically assess the credibility, relevance, and bias of the information we encounter, empowering us to become discerning consumers and active participants in the digital realm.

2. METHOD & MATERIAL

To investigate the importance of information skills in the digital age, a quantitative research design employing a survey approach was adopted.

First, Population and Sample Size. The study focused on the population of specified populations in the name of organization/institution. Using a random sampling technique, a sample of number participants was selected to represent the population. The inclusion criteria for the sample were explained criteria. The sample size was determined based on statistical considerations, ensuring an appropriate representation of the population and providing sufficient data for analysis.

Next, Research Instrument. This was a self-developed survey questionnaire consisting of three sections. The first section collected basic demographic information from the participants. The second section assessed the participants' information skills in the digital age, focusing on digital literacy, web-based research, information evaluation, and critical thinking skills. Participants rated their proficiency on a scale from 1 to 5. The third section explored the utilization of digital resources and challenges encountered by the participants. They rated their level of usage for different digital resources and the level of challenge they faced in acquiring and improving their information skills. The questionnaire underwent a pilot test to ensure validity and reliability, and necessary adjustments were made based on the feedback received.

Last but not least, Validity and Reliability of the Instrument. To ensure the validity and reliability of the survey instrument, a pilot test was conducted prior to the main data collection phase. The pilot test involved a number of participants who were not included in the final sample. The collected data from the pilot test were analyzed to establish the internal consistency of the questionnaire. Cronbach's alpha coefficient, which indicates the internal reliability of the items, was calculated. A value above 0.70 was considered acceptable, demonstrating a high level of internal consistency.

3. FINDINGS

In the digital age, where vast amounts of information are readily available at our fingertips, possessing effective information skills has become more critical than ever. Individuals with strong information skills are better equipped to navigate the digital landscape, make informed decisions, and evaluate the credibility and reliability of the information they encounter.

3.1 Information Skills are Crucial for Navigating the Digital Landscape

Effective information skills are essential for navigating the digital landscape and making informed decisions. They have the ability to critically evaluate information, identify misinformation, and determine the credibility and accuracy of the content they encounter. These skills not only help individuals make well-informed decisions but also save them time by efficiently finding the information they need amidst the overwhelming amount of data available.

3.2. Information Skills Foster Lifelong Learning and Adaptability

Information skills promote lifelong learning and adaptability in the digital age. With the constant advancements in technology and the ever-changing nature of the digital world, individuals need to continuously acquire new knowledge and skills to stay relevant. Strong information skills enable individuals to stay updated with the latest developments, trends, and tools in their fields of interest. They foster critical thinking, problem-solving, and creativity, which are crucial for adapting to new challenges and finding innovative solutions. Furthermore, information skills facilitate effective collaboration and communication in remote work environments and virtual teams, enhancing productivity and enabling individuals to contribute meaningfully to projects.

4. DISCUSSION

4.1 Benefit of Digital Age

4.1.1 Communication and social connection

Communication and social connections are important parts of how people deal with each other because they help people understand each other, form bonds, and share information. They are very important in personal connections, in the workplace, and in society as a whole. Communication is when two or more people or groups send and receive information, ideas, thoughts, and feelings. Both the sender and the receiver must be able to understand and read messages correctly for them to work. Communication can be vocal, nonverbal, written, or visual. People who are digitally literate can effectively communicate through email, social media, instant messaging, video calls, and other digital platforms (Subaveerapandiyan A. et al., 2022). This facilitates staying connected with friends, family, and colleagues, even across long distances. Communication is important for making and keeping connections, letting people know what you need and want, solving problems, working together at work, and sharing knowledge and information (Konstantina Martzoukou et al., 2020). It helps people understand each other, have empathy for each other, and work together, which leads to better connections and more productive interactions.

The term "social connection" refers to the relationships and ties that people make with other people. It includes different kinds of relationships, such as friendships, family ties, romantic relationships, and participation in the community. Social ties help people feel like they belong, get support, and feel better overall. People gain in many ways from having strong social connections. They give social support, lessen feelings of loneliness and isolation, improve mental health, and make life more enjoyable overall (Fang Zhao et al., 2021). Social relationships can also help you grow as a person, work with others, and share experiences. In recent years, technology has made it easier for people to talk to each other and make friends. People can meet and talk to each other all over the world thanks to social media platforms, messaging apps, video calls, and online communities. Technology can help people connect with each other, but it's important to keep a healthy balance and not forget about face-to-face interactions and deeper, more meaningful relationships. There are many things that can get in the way of good communication and social connections. There are language barriers, cultural differences, a lack of active listening, distractions, electronic limitations, social anxiety, and time constraints. To get past these obstacles, you have to work hard, have compassion, and be willing to understand and connect with others.

Communication has become the most important part of digital literacy in a world where technology is changing quickly. It's no longer enough to know how to use digital tools well; you also need to be able to communicate, understand others, and get around in digital relationships. There are many ways to communicate digitally, from emails and instant messaging apps to social media sites and video conferencing tools (Janne Anderson et al., 2018) For effective communication, digital literacy means having a deep knowledge of these channels and how they work. It means learning how to write messages that are clear and to the point, adapting communication styles to different platforms, and making the most of the benefits of each channel to get the most out of it.

In the fast-paced digital world, it's important to be brief. Digital conversation requires being able to say things in a short, clear way that grabs attention and is easy to understand. People who know how to use technology well are able to communicate with clarity and accuracy, providing information in a way that doesn't lose depth or meaning (Ivette K. Caballero et al., 2018) This skill is especially useful when you have to talk to someone in a small place, like a social media post or a chat platform. In the digital age, visual communication has become more important. To be digitally literate, you need to know how to use visual elements to get your point across. Digital marketers need to learn how to make images, infographics, and videos that grab and hold the attention of their audience. Visual literacy is the ability to choose the right pictures, make material that looks good, and use visual clues to help people understand and connect.

Digital literacy includes being able to think critically about what you find online. Because there is so much digital content, people need to be smart about what they choose to read and how they share knowledge (Isto Huvila et al., 2012) Digital speakers need to learn how to check sources, check facts, and tell the difference between accurate information and false information. Individuals add to an informed digital society and build trust within their digital networks by learning to think critically and use information well.

4.1.2 Critical thinking and problem solving

In the fast-changing digital world of today, critical thought and problem-solving skills are more important than ever. As technology becomes part of every part of our lives, we need to be able to find, analyze, and use digital information. Critical thinking is the process of actively and skilfully analyzing, synthesizing, and evaluating information to make well-reasoned judgments and choices (Atlantic University et al., 2022) In the digital age, when we have access to a lot of data and information at our fingertips, critical thinking is more important than ever. It helps us tell the difference between trustworthy sources and false information, check claims against facts, and evaluate the trustworthiness and validity of information. It gives people the chance to question assumptions, find biases, and use logic to come to good decisions.

Finding, analyzing, and solving complicated problems is an iterative process. In the world of digital literacy, problem-solving skills help people deal with technology problems, adjust to changing situations, and come up with new ways to solve them (Yottabyte et al., 2023) As the digital world changes quickly, people need to learn how to solve problems to deal with things like cybersecurity threats, privacy concerns, and the moral effects of new technologies. Also, people who know how to solve problems can use technology to improve their efficiency, productivity, and general well-being. Critical thinking gives people the tools they need to judge the quality, usefulness, and trustworthiness of digital material. By learning how to find reliable sources, check claims for accuracy, and analyze data, people can make good choices and avoid being fooled by false information or manipulated.

In the digital age, technology changes quickly and surroundings are always changing. Critical thinking makes people more adaptable and flexible, so they can accept change, predict problems, and change their plans accordingly (YK Dwivedi et al., 2021) People can confidently deal with the complexities of the digital age if they have a growth attitude and learn throughout their lives. Critical thought and coming up with creative solutions to problems go hand in hand. Critical thinking drives creativity by getting people to think outside the box, question assumptions, and look at things from different points of view. It lets people come up with new ways to solve hard problems and take advantage of how technology can change things.

Understanding the ethical implications of technology and making good choices are both parts of digital literacy. People who can think critically can evaluate the moral aspects of digital practices, like privacy, data safety, and the fair use of technology. By taking ethics into account when solving problems, people can make sure that their activities help society in a positive way. In a complicated and interconnected world, people need to be able to think critically and solve problems in order to do well. By developing these skills, people can evaluate material well, adjust to changing situations, and come up with creative solutions to hard problems (K. Martin et al., 2019) By learning to think critically and solve problems in the digital world, people can confidently move through the digital world, make good choices, and contribute to the progress of society. As technology continues to change the way we live, developing and using these skills will be key to making the most of the digital age for the benefit of everyone.

4.1.3 Health and well-being

In today's linked world, people need to know how to use technology well in order to do well in many areas of life. It's important to be able to move around in the modern world with skill and confidence. But even with all the possibilities and changes that technology has brought, it is still important to put health and well-being first (Sara Atske et al., 2019) Digital literacy, which often involves using devices for long amounts of time, can hurt physical health. When people spend too much time in front of screens, they often become sedentary and have bad posture. It is important to find a balance by making physical exercise a part of everyday life. Regular breaks, stretching routines, and being aware of your posture can help reduce the risks of spending too much time on digital devices.

There is a chance that the digital world could affect mental health. Constant connectivity, too much information, cyberbullying, and the pressure to keep up a good online image can all lead to stress, anxiety, and other mental health problems. It is important to learn digital literacy skills that help people think critically, be skeptical, and act responsibly online. Mindfulness, setting limits, and taking care of offline relationships can help you have a healthy connection with technology and improve your overall health (CL Nixon et al., 2014) Digital literacy is the information and skills that people need to keep themselves and others safe online. It's important to know how to stay safe online, like making strong passwords, spotting scam attempts, and keeping personal information safe. Also, knowing the private settings, permissions, and possible risks of sharing personal information can stop bad things from happening. Promoting digital citizenship and good behavior is another way to make the online world better and healthier.

Because there is so much knowledge on the Internet, it is important to learn how to use it. To be digitally literate, you need to be able to judge, analyze, and figure out the credibility and trustworthiness of online sites. With so much misinformation and fake news out there, it's important to have these skills to make good choices, develop critical thinking, and stop the spread of false information (N. Sirlin et al., 2021) Information literacy gives people the tools they need to form well-rounded opinions and have useful conversations online. In our always-connected world, it's important to take breaks from digital devices and social media sites every so often. A digital detox gives people a chance to relax, refocus on offline activities, and take care of their mental and physical health. Setting aside time for hobbies, spending real time with family and friends, and being in nature all help people feel connected and refreshed.

When it comes to digital literacy, health and well-being should be seen as two of the most important parts of a healthy digital living (DHT Force et al., 2019) By putting physical health first, taking care of mental health, promoting online safety and privacy, learning how to find and use information, and practicing "digital detox," people can use the power of digital tools without risking their overall health. Finding a balance between the digital and real worlds makes it possible to have a fulfilling, enriching, and long-lasting connection with technology. Let's start this path of digital literacy with an eye on our health and well-being and a commitment to being mindful.

4.2 Challenges in digital literacy

Digital literacy has become an essential skill set in our increasingly interconnected and technology-driven world. It encompasses the ability to access, evaluate, and effectively use digital tools and information for personal, educational, and professional purposes (Giannikas et al., 2020) While digital literacy offers countless opportunities, it also presents several challenges that need to be addressed.

One of the primary challenges in digital literacy is the rapid pace of technological advancement. The digital landscape is constantly evolving, introducing new tools, platforms, and trends. This poses a continuous learning demand on individuals, who must keep pace with these changes to remain relevant (A Haleem et al., 2022) However, this can be overwhelming for those who struggle to adapt or lack access to resources for learning. As a result, a significant portion of the population may face difficulties in acquiring and maintaining the necessary digital skills.

The proliferation of misinformation and the spread of fake news represent a significant challenge in digital literacy. With the ease of sharing information online, it has become increasingly difficult to discern accurate information from false or misleading content. Many individuals struggle to critically evaluate sources, fact-check information, and identify biased or manipulated narratives (L. Soetekouw et al., 2022) This challenge undermines informed decision-making, public discourse, and trust in reliable information sources, posing risks to individuals and society.

Digital literacy also encompasses the understanding of cybersecurity principles and practices. As individuals engage in online activities, they face various risks such as identity theft, phishing attacks, malware, and other forms of cybercrime (F. Quayyum et al., 2021) Lack of awareness and skills in cybersecurity can make individuals vulnerable to these threats, potentially resulting in financial loss, privacy breaches, or reputational damage. Developing robust cybersecurity knowledge and adopting secure practices is crucial for protecting personal information and maintaining digital well-being.

Another challenge lies in utilizing digital tools effectively for communication, collaboration, problem-solving, and creative expression. While technology offers numerous opportunities for productivity and innovation, many individuals struggle to leverage these tools to their full potential (YK Dwivedi et al., 2022) A lack of familiarity with digital platforms, inadequate training, or limited exposure to advanced tools and techniques can hinder individuals' ability to effectively navigate and utilize digital resources.

Digital literacy is indispensable in the modern world, enabling individuals to participate fully in the digital age and unlocking opportunities for personal and professional growth. However, challenges such as the rapid pace of technological advancement, the digital divide, misinformation, cybersecurity risks, and the effective use of digital tools must be addressed to ensure equitable and inclusive digital literacy for all (Romina Bandura et al., 2022) Efforts should be made to promote education and awareness, expand access to technology and the internet, foster critical thinking, and develop cybersecurity and digital competency skills. By tackling these challenges head-on, we can empower individuals to navigate the ever-evolving technological landscape with confidence and competence.

5. CONCLUSION

The ability to navigate the large quantity of information available online is essential in the digital era. In summary, having strong informational abilities is crucial in the digital era. They enable people to find, assess, and use information efficiently, encouraging critical thinking, digital literacy, lifelong learning, and responsible online behaviour. The success of academic, professional, and personal endeavours in today's information-driven culture depends on the development of these abilities. The value of information literacy in the digital age cannot be emphasised, in my opinion. Making educated judgements, navigating the huge internet environment, and remaining current in a world that is changing quickly all depend on one's capacity to properly obtain, assess, and use information. The ability to critically assess sources, conduct research and analysis, and become lifelong learners are all made possible by information skills.

Additionally, they support career advancement, appropriate use of technology, and digital citizenship. To succeed in academic, professional, and personal endeavours in a culture where information and digital resources are pervasive, it is crucial to have good information skills. The task of educating consumers to critically evaluate, reflect on, and make use of the incredibly diverse spectrum of available media makes media and information literacy in the twenty-first century an ambitious objective. Users now need to be media literate with regard to the abundance of new technology accessible and the development of apps providing whole new methods of sending information, in addition to conventional media literacy and visual representation.

References

Oseghale, O. (2023, January 23). Digital information literacy skills and use of electronic resources by humanities graduate students at Kenneth Dike Library, University of ibadan, Nigeria. Digital Library Perspectives. https://www.emerald.com/insight/content/doi/10.1108/DLP-09-2022-0071/full/html

Deegan, M., & Tanner, S. (n.d.). Digital Librarians: New roles for the information age (Chapter 9) - digital futures. Cambridge Core. https://www.cambridge.org/core/books/digital-futures/digital-librarians-new-roles-for-the-information-age/7A63075640B8292FFBDCDB2AD0ADD8A3

Digital Literacy: Survival Skill for librarians in the digital era. (n.d.). https://www.researchgate.net/publication/330975918_Digital_literacy_Survival_skill_for_librarians_in_the_Digital_Era

Martzoukou, K., Fulton, C., Kostagiolas, P., & Lavranos, C. (2020, June 30). A study of higher education students' self-perceived digital competences for learning and everyday life online participation. Journal of Documentation. https://www.emerald.com/insight/content/doi/10.1108/JD-03-2020-0041/full/html

A., S., Sinha, P., & Ugwulebo, J. E. (2022, September 9). Digital Literacy Skills Among African Library and Information Science Professionals – an exploratory study. Global Knowledge, Memory and Communication. https://www.emerald.com/insight/content/doi/10.1108/GKMC-06-2022-0138/full/html

Zhao, F., Barratt-Pugh, L., Standen, P., Redmond, J., & Suseno, Y. (2021, September 15). An exploratory study of entrepreneurial social networks in the Digital age. Journal of Small Business and Enterprise Development. https://www.emerald.com/insight/content/doi/10.1108/JSBED-10-2020-0359/full/html

Tuamsuk, K., & Subramaniam, M. (2017, May 8). The current state and influential factors in the development of digital literacy in Thailand's higher education. Information and Learning Science. https://www.emerald.com/insight/content/doi/10.1108/ILS-11-2016-0076/full/html

Ahmed, S., & Rasheed, T. (2020, May 14). Relationship between personality traits and Digital Literacy Skills: A Study of University Librarians. Digital Library Perspectives. https://www.emerald.com/insight/content/doi/10.1108/DLP-02-2020-0005/full/html

Oseghale, O. (2023), "Digital information literacy skills and use of electronic resources by humanities graduate students at Kenneth Dike Library, University of Ibadan, Nigeria", Digital Library Perspectives, Vol. 39 No. 2, pp. 181-204. https://doi-org.ezaccess.library.uitm.edu.my/10.1108/DLP-09-2022-0071

Khan, A. (2020, May 14). Digital Information Literacy Skills of Pakistani librarians: Exploring supply-demand mismatches, adoption strategies and acquisition barriers. Digital Library Perspectives. https://www.emerald.com/insight/content/doi/10.1108/DLP-01-2020-0003/full/html

Rafi, M., JianMing, Z. and Ahmad, K. (2019), "Technology integration for students' information and digital literacy education in academic libraries", Information Discovery and Delivery, Vol. 47 No. 4, pp. 203-217. https://doi-org.ezaccess.library.uitm.edu.my/10.1108/IDD-07-2019-0049

Preface

It is our pleasure to present the proceedings of the 1st Glocal Symposium on Information and Social Sciences (GSISS) 2023 organized by School of Information Science, College of Computing, Informatics & Mathematics, UiTM Kelantan Branch, Faculty of Administrative Sciences and Policy Studies, Faculty of Law, and Perpustakaan Tengku Anis in collaboration with several local and international strategic partners; DIGIT360 Sdn Bhd; Universitas Airlangga (UNAIR), Indonesia; Universitas Ngudi Waluyo (UNW), Indonesia; and Camarines Sur Polytechnic Colleges (CSPC), Philippines. The 1st GSISS is an international symposium that brings together researchers, academics, industry professionals, and policymakers to share and exchange knowledge and insights related to information science and technology. This year's conference, held physically and virtually, saw a significant turnout of participants from across the world, highlighting its success and relevance in the field. The conference covered a wide range of topics, including information systems and technology, data science and analytics, cybersecurity, ethics, and e-commerce, among others. The proceedings capture the valuable contributions made by the conference participants through research papers, case studies, and presentations. We hope that these proceedings will serve as a valuable resource for researchers, educators, and practitioners in the field of information science and technology, facilitating continued collaboration and advancement in this dynamic and constantly evolving domain.

Glocal Symposium on Information and Social Sciences

GSISS2023

اونيۏرسيتي تيكنولوݢي مارا
UNIVERSITI TEKNOLOGI MARA
Cawangan Kelantan

ACADEMICA
PRESS SOLUTIONS

9 786299 753667