SECURITY CONVERGENCE 2024

A Review of Organizational Drivers and Approaches for Converging Cybersecurity, Physical Security and Risk Management With Core Business Needs

SIA
SECURITY INDUSTRY ASSOCIATION

PRODUCED WITH SUPPORT FROM

Ai-RGUS
NO CAMERA LEFT BEHIND™

Alert Enterprise

Avangrid

safetrust

TABLE OF CONTENTS

INTRODUCTION

Since the first security camera was placed on an IT network, convergence has been talked about in our industry. For some, convergence has meant connecting technologies from physical security and IT, and for others, it means connecting cybersecurity, information security and physical security strategies.

At the Security Industry Association (SIA), we have closely followed the theme of convergence, as it impacts both our practitioner members and the technologies delivered by our manufacturer and integrator members. This convergence of physical security and cybersecurity continues to progress and has led SIA to invest in and develop resources to help our industry adapt to convergence, with efforts including operation of the Cybersecurity Advisory Board, which provides insights and resources in this foundational area; the Security Industry Cybersecurity Certification (SICC), the industry's first credential focused specifically on cybersecurity for physical security systems; interactive trainings, conference sessions and webinars focused on key cyber-physical security topics; conversations around convergence in the annual Security Megatrends report; and the creation of resources like product and system hardening guides, cybersecurity onboarding recommendations and more.

Convergence, while a buzzword for decades in our industry, has sometimes been slow to produce results and may look different now than we originally envisioned, but in the coming years, true convergence may finally become inevitable, as the networking of security devices and the increasing integration of security into other technologies could make silos not just inefficient, but impossible. In this SIA report, we've worked to distill where convergence is at a moment of change, provide some history on the concept and offer some future perspective.

PRODUCED WITH SUPPORT FROM

LOOKING BACK & MOVING FORWARD 1

In the past, interpretations of the topic of "convergence" were based on infusing technologies together, resulting in a new concept – or even a specific product offering. Did the industry get it wrong? Fast forward, and adoption hasn't quite matched enthusiasm of the original vision most in the industry held.

Time bestows the benefit of retrospection, and this paper details how the concept is actually flourishing, but in different, broader and more meaningful ways than originally anticipated. It also explores why convergence has evolved, as well as its application and impact within the physical security industry. Actionable steps will be outlined to provide insight into best practices in considering, investigating and applying concepts that are covered.

POSTMORTEM

Analysis of how convergence was promoted and applied in the past reveals that despite the topic being novel, concepts that were presented fell short on value, were too challenging to execute or both.

Perhaps one underlying cause was there was no clear universal definition of what "convergence" was. Ask 20 different security professionals, and they're likely to provide as many different answers. Understandably, there was a bit of confusion. Manufacturers weren't short on perspectives, and they provided a surrogate function to what convergence was. They were often hyperfocused on integrating technologies and delivering some operational and security improvements but inevitably struggled to get funding because the business case just wasn't compelling enough, as they delivered limited benefit to the greater organization and presented significant operational challenges.

Most concepts were new and required collaboration with resources outside of physical security, management support and additional skills than had been projected. Coordinating, refocusing and reallocating resources that were already committed to their existing functions were significant barriers.

If organizations got past the first two challenges, they encountered cultural and political obstacles. IT and physical security had been separated for so long that not only were their systems siloed apart from one another, but also their technologies, standards and policies were drastically different. Convergence requires harmonizing these aspects as a prerequisite to effectively plan, execute and maintain.

Ultimately, many organizations either didn't have the appetite to provide the level of transparency required for the efforts, relitigate significant portions of their security programs or work through the significant political aspects that eventually became apparent.

REVISITING THE CONCEPT

Despite the shortcomings of its original premise, in recent years convergence has been flourishing — but in different ways than originally anticipated. By all accounts, it's more relevant to end users and compatible with their current challenges and objectives.

MODERN CONVERGENCE PROJECTS THAT INVOLVE BROADER OBJECTIVES

Rather than being driven by industry and defined by specific offerings, convergence is being undertaken by end users whose organizations are determined to achieve specific outcomes that are at higher priority levels which can't be achieved in isolation from other systems, people and departments. Often, such initiatives may represent achieving a prioritized business directive which isn't owned by physical security yet is identified as a critical component in the solution to the desired outcome.

For example, at the start of the COVID-19 pandemic, many organizations experienced urgent demands by their executive management to redirect focus away from planned security projects and collaborate with other departments to achieve on-site attendance metrics, people tracking, wellness visibility, contact tracing and specific controls for compliance and reporting. This shift was purely a business demand that didn't impose a security outcome but rather required a great deal of engagement with stakeholders and collaboration with other departments to jointly determine a viable solution, fuse intelligence and reengineer some processes to achieve success of a business outcome.

Operational technology (OT) is another area where convergence is becoming commonplace for organizations that rely on industrial control systems (ICS). There are various classes of ICS which serve as the backbone of many organizations' critical infrastructure across a variety of industries. These systems fulfill a broad range of purposes, such as water and sewage treatment, pharmaceutical manufacturing, automotive manufacturing, chemical plants treatment, traffic signal controls, natural gas networks, electrical grids, pipeline systems, satellites and transportation.

The prospect of ICS being compromised represents a massive impact to an organization's operations and revenue and the safety of their customers (and communities they serve). Stopping bad actors at the network level alone isn't adequate. In fact, many ICS are older, predating the internet, but still serve their intended functional purpose and are too expensive to replace. Whether organizations are planning to upgrade their ICS or not, executives continue to increase priority on business continuity and resiliency, which requires in-depth physical controls to prevent noncompliant activities across a range of both bad actors and authorized personnel alike. In order to design meaningful controls, physical security professionals need to work with business managers, ICS engineers and risk managers to understand specific uses cases and determine what is noncompliant, otherwise such controls will be more generic and less effective.

INCREASED DEMAND FOR PHYSICAL SECURITY TO PLAY A LARGER ROLE IN OTHER DEPARTMENTS

On other fronts, departments executing their own objectives are experiencing increased needs relating to physical security. For example, the number of compliance mandates continues to increase, with many evolving to recognize that implementing controls to prevent noncompliant use or unauthorized access to systems over the network isn't adequate without also requiring commensurate controls over actors that may contemplate physical access to those systems or the adjacent environments that can provide a unique vector as an alternate path to success (e.g., the ability to do social engineering more effectively from within or gain physical access to one system and traverse to another from a route that has fewer barriers) .

It is not uncommon to see scenarios where a pharmaceutical lab needs high levels of assurance to prevent espionage of IP, contamination or safety events from occurring.

Many organizations are upgrading their data center security to increase resiliency and meet increasing compliance measures that require physical security elements (e.g., SOC2, PCI DSS and even the nascent CMMC 2.0).

While some colleagues know the business process well and others respective cybersecurity aspects, neither are physical security experts. There is increased recognition that their participation and assistance are needed to meet higher standards being set to achieve their own objectives.

PHYSICAL SECURITY IS THINKING BIGGER

Not to lose sight of the fact that all the while, physical security executives still have their own department-level challenges and improvements to make, there is more pressure now than ever before to demonstrate transformational outcomes in a business case to get funding appropriated for the effort.

The days of getting funding approved for iterative system upgrades, improving processes that those external to security won't experience or reducing risks that can't be measured or effectively articulated to be a priority to the business are in the rear-view mirror for most. But that doesn't mean security professionals are taking it lying down – on the contrary. Security leaders have been tuning in to how other departments are able to get funding, the level of innovation being incorporated and elements of the business case that need to be included.

The range of use cases are varied and mounting yet appear to share a common denominator where security leaders are changing how they engage with other functions within their organization. They are shifting from calling on colleagues in adjacent departments (such as information security (InfoSec) to advise on their own projects (typically as an approver function, such as guidance or assistance with network requirements) to soliciting what their top priorities are and identifying opportunities to build in capabilities that may provide benefits to them as well.

For example, a project slated to improve situational awareness within physical security might also provide some intelligence value to other departments as a byproduct to increase value to the organization, and as a result the business case is stronger and support for resources becomes more likely, particularly if that other project reflects an outcome that is already a high priority with executives. This isn't limited to specific technology functions but rather is unlimited across the rest of

the organization, whether it's workplace management, real estate, manufacturing, research and development or otherwise.

The fact of the matter is, wherever people physically are engaging with organizational assets and operations that are critical to the business, there exist elements of physical security that either are being overlooked or represent an opportunity for improvement.

IMPORTANCE OF OBSERVING THIS TOPIC

For years, physical security has operated in a silo, and not necessarily always by choice. Technology developed apart from IT systems disparate from one another, and personnel were allocated specifically to manage these unique aspects – so too was the management structure to support it. Over time, core principles, methodologies and practices of physical security were uniquely different than their IT counterparts.

Just get physical security and information security teams in a room to talk about "key management," and it might take 20 minutes for each side to realize that one side was referring to physical keys to open locks and how best to manage access to them while the other was thinking only about encryption keys and how best to distribute and manage them across devices.

Many physical security leaders found some success in being less encumbered by oversight to make autonomous decisions. Arguably, this fueled the status quo of separation. However, a more recent trend is that the same security leaders (or the next generation that inherited their programs) are often finding the silo that had been built is becoming more its own island of aging infrastructure, limited resources and trying to figure out how infuse modern resources afforded other departments that had long ago made the move to the mainland.

Ironically, many security leaders were around when InfoSec was stuck on the "basement" and witnessed their transformation to being well supported board room participants. More broadly, InfoSec isn't unique, as other departments have gone through similar evolution successfully. It's fair to say many physical security leaders express their desire for a similar shift.

For the most part, whereas convergence of the past was asserted by solution providers as a "destination" (acquiring a specific capability or obtaining specific

state), security leaders are demonstrating that it's rather an "exercise" of broader collaborative engagement, shared incentives and harmonizing practices so all participants have a realistic path for execution – an important remedy to where previous convergence concepts fell short.

TIMELINESS OF TOPIC

There is increased pressure on physical security leaders to address an expanded portfolio of threats while operating expenses (OpEx) budgets are at maximum utilization, with little appetite from executives to increase either OpEx or capital expenditures (CapEx) to address them; however, there are pathways to success. As the threat landscape evolves and expands, so do the range and gravity of risks that executives need to address. Ultimately, executives fund risk remediation, not security. Increased corporate governance requirements, regulations and liability mean that owning risk and making decisions can't be avoided.

Many security leaders struggle with designing an initiative that touches the core priorities of executives and compels them to fund what is being proposed. Convergence as an exercise will facilitate discovering those priorities, identifying stakeholders to collaborate with and initiatives to be part of, but physical security also needs the tools to deliver.

In the past, the industry as a whole wasn't set up to facilitate big crossdepartmental ideas; however, the physical security industry is undergoing arguably the most significant transformation in its history. The undeniable influx of advancing technology becoming available provides a unique opportunity to achieve things that previously weren't possible or do them in ways that are more efficient and extremely compelling.

Certainly, physical security leaders should exercise efforts to explore how these compelling advances can shift the paradigm for their programs ranging from projects that have a completely new profile to old challenges being solved in new ways; however, convergence also represents new challenges.

Most of the technological advances are areas where physical security end users have little experience, expertise and resources to get a handle on the capabilities, requirements and risks of employing them in the first place. This can quickly turn opportunities into cybersecurity liabilities or privacy violations or risk the project's

overall success in being rolled out and appropriately managed, yet there are steps within a convergence model that end users can take to address these risks and accelerate adoption and success.

OUTLOOK
THE END-USER JOURNEY IS CONTINUOUS

Convergence is occurring across a number of end-user programs and achieving different types of outcomes that change perception from being seen as a cost center to as a key contributor. Each convergence project brings together a variety of stakeholders, perspectives and new possibilities which in time brings into consideration changing specific practices, modifying operations or redesigning more fundamental aspects of the security program itself.

CONVERGENCE WILL CONTINUE TO BE DEFINED AND REDEFINED BY END USERS

End users have significant responsibilities of running security programs that span several specialized capabilities. They have the responsibility to ensure success and the burden of failure if things don't work out. As end users exchange ideas around similar challenges, socialize their success and share best practices, certain approaches become common within the industry, while others require further consideration by few to solve it for the many (who might not be as aggressive or adventurous or have as many resources at their disposal).

ALL CONSTITUENTS IN INDUSTRY WILL BE IMPACTED IN VARIOUS WAYS

As early adopter end users experience transformative outcomes through convergence and identify key elements they require, manufacturers will play a critical role in productizing solutions that can commoditize the implementation, accelerate time to value and reduce project risk. Manufacturers and respective channels will need to understand the nature of these demands and adjust their offerings, reconsider where they specialize and how they engage with perspective customers to support their revised objectives.

NEW ENTRANTS INTO THE MARKET

An outsized trait of convergence is the pursuit of taking on big challenges and solving them in bold, innovative ways that result in more meaningful outcomes. A big part of innovation is reserving high expectations and an open mind as to who can fulfill them.

The range of technologies that are well-positioned candidates to be major catalysts in this equation – such as artificial intelligence (AI), mobile, cloud and sensors – aren't inherent to the physical security industry. They need shape, purpose and expertise to be packaged and consumed. Interestingly, all these technologies (and others) are new to physical security but not necessarily to other industries. There exist two potential arguments where both could be true:

1. Manufacturers within the industry collectively need to play a bit of catch-up in harnessing and assimilating these new technologies into something that is compelling and can be delivered to their customers.

2. It could be argued equally that manufacturers from other industries who already successfully specialize in these areas could use their existing intellectual property, core resources and expertise to expand into physical security as a new opportunity for them (and may share the same customers, hence not entirely be "outsiders").

There exists a range of possibilities that could occur. For example, industry incumbents could embed AI into their existing product or a company that specializes in AI could develop hooks into physical security systems to make more compelling use of the data – both scenarios are actually currently playing out.

CYBERSECURITY CONTINUES TO ELEVATE TO THE BOARD LEVEL – PULLING PHYSICAL SECURITY ALONG WITH IT

As physical security technology increasingly becomes indistinguishable from those employed by IT, the same cybersecurity risks are inherited and need to be addressed. The industry has been acclimating to this realization for the past few years.

In July 2023, the Securities and Exchange Commission (SEC) adopted new rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance and incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934 (the "Exchange Act").[1] At a very high level, the rules require any publicly traded company to file disclosures with the SEC (via Form 8-K) concerning cybersecurity incidents that are determined to have material impact on the company (and investors), including the timing, scope

---

[1]https://www.sec.gov/corpfin/secg-cybersecurity

and nature of the incident. The Exchange Act also requires annual disclosure of cybersecurity risk management, strategy and governance (via Form 10-K).

Both of these requirements are significant material steps for advancing cybersecurity into the hearts and minds of corporate governance, but the second part is particularly interesting, as it includes companies to disclose their processes for assessing, identifying and managing material risks from cybersecurity threats. Companies are also required to describe board of directors oversight of risks from cybersecurity threats and identify board committees and subcommittees that are responsible for oversight and management's role in assessing and managing material risks from cybersecurity threats.

Translation – for any publicly traded company registered with the SEC, cybersecurity is no longer a "best effort" of placing bets through bullets gleaned by inviting IT up to the board room for occasional briefings. Rather, it holds executive management accountable to take ownership of risk and ensure there is process and capacity to facilitate continuous awareness, assessments and truthful reporting as they would with do with other aspects of their 10-k.

It's conceivable if not predictable that if organizations haven't already elevated the CISO role to be part of the executive team and inclusive in ongoing board activities, they are likely to do so quickly as reporting is required to start for fiscal years ending on or after December 2023.

Now the big question, if physical security systems are becoming indistinguishable from IT systems, inherit similar threat profiles, are cybersecurity risks of physical security systems excluded from these obligations? Consider that anytime physical security systems are integrated with other systems across the enterprise that do fall into this area (essentially every other system in the organization from financials to manufacturing to sales and marketing). Anything that is connected represents a potential vector for initial attack and parallel movement to another system toward the ultimate target. This is how targeted attacks work – the type of attacks that would likely meet the requirement for "material impact" and necessitate reporting.
It will be interesting to see how chief information security officers (CISOs) will view the evolution of physical security systems and whether they'll treat them like any other connected system with similar attack surfaces and vulnerabilities. Further, once they recognize the physical security industry's ongoing cybersecurity dilemma

of trying to catch up, will they acquiesce to traditional separation or impose a more formal relationship to ensure 10-k compliance?

It will take time to get some definitive answers, but it's at least likely that physical security shifts from the peripheral view of a facilities function and is thrust right into the executive compliance fold. Physical security will be an equal part of a common incentive model that is instituted at executive levels for all business, security and risk stakeholders to work together, align objectives, coordinate resources and harmonize practices. At minimum, it's starting to sound a lot like convergence taking shape.

MODERN CONVERGENCE 2

This section will outline the modern definition of convergence, analyze the broader organizational dynamics that help shape it and examine how various components influence one another.

2.1 A NEW REALITY

Convergence got a big push about 20 years ago in the physical security industry. Notwithstanding how it played out, much has changed since then, not only within the industry but also inside the greater business environment it endeavors to protect.

In that time, enterprises have transformed their operations to become mostly digital, implemented business intelligence and expanded automations, resulting in higher efficiency, agility and speed at which they operate. At the same time, technology within physical security has made significant advances, yet most end users' infrastructures are aging and increasingly experience challenges gaining adequate funding to take advantage of such advances.

Meanwhile, the scope of threats has only expanded, and the complexity to implement countermeasures, technology and employ more specialized resources to execute has become significant a challenge for physical security leaders. Engaging with executives on this premise might win some sympathy but seldom translates to tangible support that's requested.

The hard fact is that physical security leaders compete with the rest of the organization for funding. Many security leaders struggle with being perceived as a cost center, which doesn't help convince executives to prioritize allocating budgets to physical security over another department that proposes to increase revenues, profits or their competitive position. Physical leaders need to change their engagement model with the rest of the organization to be successful.

2.1.1 CONVERGENCE IS BROADER THAN PHYSICAL INTERACTION BETWEEN CYBERSECURITY AND IT

Executives have become more data driven and tend to support stakeholders that provide clear visibility, supporting metrics and relevance to core mandate success; as a result, along with stakeholders, they've developed a general consensus about how various departments engage – culturally, collaboratively and how they support one another and communicate these aspects. Focusing only on how executives and stakeholders can help approve project funding or respective requirements is an increasingly losing battle.

Stakeholders have transitioned from only focusing on program-level challenges to incorporating convergence, interoperability and business operational improvements as critical success components of key initiatives. Despite the significant advances in technology that have the potential to reshape part of a physical security program, making commitments to specific technologies or integration plans irrespective of identifying which initiatives to align with and prioritized business risks to help remediate is likely to result in choices that aren't optimized to support executive mandates.

In the process, corporate governance and cybersecurity have matured, arguably much further than they have within physical security. Most other departments adopted corporate policies for cybersecurity, privacy and compliance while embracing the same risk management framework the C-suite uses to make such decisions.

The rest of the organization continues to evolve a common operating model, and physical security leaders have a choice as to whether they want to push harder with their existing model or forge ahead transitioning to one that is proving to be more successful for other stakeholders.

If convergence was only about integrating with other technical or security domains, then the rest of the enterprise has already done this, and physical security is late to the party.

2.1.2 STAKEHOLDER SUCCESS CREATES UNIQUE PRESSURE FOR CORPORATE SECURITY

Increased success in how stakeholders navigate key initiatives reinforces executives' confidence in the feasibility of their mandates and influences expectations of how all stakeholders should successfully respond. A culture develops around principles that are applied, innovations employed and how they're communicated. Conversely, stakeholders that don't engage or successfully participate in this model become less visible.

SECURITY LEADERS HAVE UNIQUE CHALLENGES

Security leaders have a disproportionate challenge that distinguishes them from other stakeholders. In most cases, security isn't going to propose generating revenue since many aspects of security are difficult or nearly impossible to quantify (life safety in terms of occurrence and dollar values).

AN UNAVOIDABLE BLUEPRINT FOR SUCCESS

There exist successful examples across an organization that one can learn from. Physical security has witnessed InfoSec move from the basement to the board room, demonstrating that challenges unique to security can be overcome by balancing the desired security program and technology improvements while successfully participating in the broader organizational environment to gain support for security improvements that they want to make, get funding approved and support their efforts.

The success of the CISO has paved the way for executives to develop specific expectations of what a risk discussion sounds like, what a security briefing looks like, how a business proposal is composed and how these are critical elements of initiatives that support core mandates and need to be supported.

When physical security leaders employ a different approach within an organization where the CISO has been successful, it causes a disconnect in contrast to expectation. For example, executives often wonder "if physical and information security are both security domains, why do they often subscribe to entirely different sets of principles?"

- Why are similar technologies not subject to the same standards and guidelines?
- Why aren't physical security systems being assessed by the same auditors?
- Why are the risk metrics being presented not the same ones used by everyone else?

These aspects are often confusing to executives and aren't going to spend much effort rationalizing an answer. Rather, executives will just take a pass. Physical security could consider remediating these areas by observing the lessons of the CISO's journey (which was very intentional) and adopting some of their successful practices.

- How do they overcome quantifying security risks? What measurements are used?
- How do they successfully engage stakeholders to become part of key initiatives?
- How do they best communicate security issues in executive terms and align with boardroom-level concerns?

2.2 CONVERGENCE REDEFINED
ENVIRONMENT SHAPES HOW CONVERGENCE IS DEFINED

More than ever, physical security leaders need to be more engaged and get more creative. In many cases, convergence is emerging as the answer; however, since each organization determines their objectives independently from one another, risk profiles vary and how they're staffed and cultural, political and interpersonal dynamics differ, successfully engaging across the broader organization requires an interdisciplinary approach.

For these reasons, convergence is repeatable framework rather than a specific "thing" that is implemented. Internal dynamics shape how convergence is defined, while convergence shapes the manner in which we may respond to evolving business, risk and security demands.

2.2.1 ANATOMY OF CONVERGENCE

Convergence as a concept isn't static – it will continue to evolve – but is robustly anchored to four core pillars (which will be discussed later on in the paper along with best practice recommendations).

TECHNOLOGY

Technology is a requisite component to facilitate most desired outcomes in the modern business environment; however, convergence is defined neither by specific technologies nor the integration between them. Integration has been occurring within

physical security for decades, and some elements of these efforts may or may not qualify as convergence efforts but are not as a whole based on that single criterion. Failure for physical security practitioners to recognize this may result in misdirection opportunity, resources and impact.

The industry is entering an era where technology innovations are not just iterations but rather generational leaps. Unlike in the past, a considerable portion of advancements infuse innovations from outside physical security that completely change the paradigm to solve longstanding challenges that have persisted from the past and inform how we can tackle opportunities more efficiently in the future.

Practitioners will encounter technology that is credibly asserted to be better or faster or has more features, but it's critical to observe that these conclusions are in isolation from the context in which they are best applied. It could easily be argued that a technology that is inferior but has more relevant attributes to fuse logic layers, streamline processes and assimilate data into relevant insights and actionable outcomes for a key initiative that is more compelling.

BUSINESS ACUMEN

Between events that occur daily, persistent threats, systems and people to manage, security leaders have a lot on their plates. Often when knowing what needs to be fixed, improved or better resourced, it can be too easy to fall into a pattern of requesting support from executives that overlooks how we engage with the rest of the organization, which largely doesn't think about security or think about it in the same way.

Organizations are made up of people who have unique viewpoints, backgrounds and specializations. No matter how great ideas may be, building successful dialogue and support is essential. It requires an understanding of a stakeholder's business, environment, processes and challenges while often being able to communicate effectively in nonsecurity terms. These aspects are often a combination of adjusting interpersonal behavior and seeking aspects that are regarded in the organization's culture – such as business templates, processes, methodologies, metrics and governance practices.

Physical security leaders need to assimilate the priorities of the greater organization into their own objectives to achieve greater relevance and support from other stakeholders. For many, this will mean shifting from relationships with others in the

capacity of "approvers" of the elements of projects security is working on to being collaborators with stakeholders in solving organizational initiatives together.

RISK

In a perfect world, all security deficiencies would be funded; however, executives know that if they funded all security deficiencies, their organizations wouldn't be profitable. They have limited resources, most of which are going to be allocated to executing key initiatives. Ultimately, executives know they need to take many risks.

Too often, physical security culture speaks of risk in colloquial terms, interchanging security events as "risks." A security event may become a risk, and it may not. Often, the context around an event's occurrence shapes what aspect of the business is affected and to what extent the impact. It's the latter part that is risk, which is what executives want to discuss. This is really important, since most organizations have formal frameworks for identifying, evaluating and measuring risk, which is much broader than security, ranging from risks within their markets to supply chain, sales, innovation and more. Generally, the bottom line that executives want to know is – "What's the impact of not funding specific risk item?" so they can determine if they have the appetite for doing so. The risk framework they employ will give them the information they require in familiar terms. If physical security leaders aren't subscribing to the same framework and presenting security events (even if they are critical), odds are that executives don't have the tools to properly consider (or appreciate) what is being presented. Integrating the organization's risk framework into the physical security practice is also critical for physical security leaders to properly understand risks that exist across the organization and how they're prioritized and demystify what's likely to get funded (and consider participating in those).

GOVERNANCE

Broadly speaking, governance is how an organization manages its obligations, defines its execution and attains reliability and insight into its performance. Obligations can range from external forces (e.g., regulatory compliance) to internal forces (specific measures the organization believes it needs to regulate to operate effectively). Policies, practices and controls are just some areas many may find familiar.

While cybersecurity has gained considerable awareness in the physical security industry, "governance" hasn't but is arguably even more important. How can security ever be better than an organization's ability to govern it?

Even for security practitioners who aren't planning to undertake convergence as a practice, preparing for the modern threat landscape necessitates collaboration between people, departments, systems and intelligence. Formalizing ways that data can be shared and secured, maintain integrity and comply with privacy requires that the different stakeholders working together adopt common practices.

Convergence will require physical security to observe the governance structure of the organization and its implementation within various departments and harmonize (if not adopt) with physical security. Collaboration across the organization can't be successful with stakeholders subscribing to different principles and methodologies and conflicting policies. Without alignment, there won't be trust, consistency or acceptable oversight, and many projects will be unable to get off the ground.

2.2.2 ENGAGEMENT

Convergence is generally working across at least two of the four pillars. Most modern projects and technologies will require it anyhow. Many examples exist: Implementing mobile identity/credential solutions will require participation from IT, IT operations, InfoSec and governance (privacy, audit) at minimum just to allow the app to be installed, rolled out and serviced – additional layers get added if physical identity lifecycle gets integrated with IT's process.

OT inherently requires domain expertise across a broad spectrum to even entertain modifications, upgrades and weighing risks associated with all those choices – from people who know the old system to those who understand the existing process and desired changes. This expands to include multiple security and risk professionals to assess the various physical, digital and analog attributes and associated risk.

For some, much of this will be familiar. For others, it may seem as if convergence is an unstructured alphabet soup of the day. While it does take some getting used to, once security leaders are plugged into the various elements discussed in this paper, working within the framework isn't a heavy lift.

Figure A: Overview of Convergence as a Framework

	SECURITY PROGRAM CHALLENGES	NEW TECHNOLOGY	CYBERSECURITYSECURITY		STAKEHOLDER PRIORITIES	EXECUTIVE PRIORITIES
DEFINE	**BUSINESS ACCUMEN** • Perception • Justifying Investments	**FUNDED UPGRADES**	**JOURNEY (LESSONS LEARNED)** • Blueprint for Success • Methdology		**INITIATIVE PRIORITY** • Stakeholder Objectives > Business Solutions • Contribution vs Cost Center	**BUSINESS PRIORITY ALIGNMENT** • Top Corporate Initiatives • Executive Priority Alignment
PRIORITIZE	**RISK** • Justifying Budgets • Quantify & Manage Risk	**FUNDED REMEDIATION MEASURES** • Planning • Countermeasures & Re-engineering	**REMEDIATE** • Operations Technology (OT) • Assessment Maturity		**TREATMENT** • Risk Owners • Risk Collaboration	**ESRM** • Prioritized Risk • Risk Alignment
INNOVATE	**TECHNOLOGY** • Visibility • Status & Impact • Prevention • Preparedness & Response	**SECURITY PROGRAM IMPROVEMENTS** • Intelligence • Situational Awareness • Behavior Analysis • Detection	**MONITORING** • Alerts • Blended Threats • Reporting		**DESIGN INTENT** • Clear Solution Definition • Solving Business Problems • Expanded Value for Stakeholders • Gain Stakeholder Support	**EXECUTIVE SUPPORT** • Compelling Business Proposals • Increase Project Approval Rate
OPERATE	**PROGRAM GOVERNANCE** • Program measurments & KPIs • Consistency & Repeatability • Enforcing Policy and SOPs • Operational Efficiency	**TECHNOLOGY GOVERNANCE** • Privacy • Audit • Modernize Standards • Device Lifecycle Management	**CONFORMANCE & CONTROLS** • Identity Entitlements & Permissions • New Connected Devices • Insecure Legacy Devices • Application Conformance		**INTEROPERABILITY** • Data Standards • Metadata Standards • API Standards • Identity Lifecycle Managment	**CORPORATE GOVERNANCE** • Alignment • Standards • Regulatory Compliance • Asset Management
TEAMING	**SPECIALIZATION** • Specific Skills	**IT & IT OPS EXPERTISE** • AI Engineers & Data Scientists • Maintenance & Custodial Operations	**CYBERSECURITY EXPERTISE** • Validation & Managerment • Patching & Key Management	**BUSINESS CONTEXT** • Critical Business Process • Business Use Cases		
	RESOURCE COLLABORATION • Staffing Limitations	**SHARED SERVICES** • Application and Device Mgt • Implementation	**JOINT OPERATIONS** • Intelligence Analysts • Validation & Penetration Testing			

Harmonize Business & Security

Bold Colors are Core Convergence Areas
• Plain Text bulleted items are key challenges

Security programs have their own core challenges and objectives (far-left column). Security leaders seek solutions via innovation (second column from left) but have specific increasing obligations such as cybersecurity (third column) from left. Meanwhile, these activities can't be undertaken successfully in a silo. Leaders need to consider how their program objectives converge with organizational mandates and initiatives from executives (far right) and stakeholders (second from right).

The flow from the left (security) intersects with the inward flow from the right (business side) to align security objectives with the concerns of the business.

The four core pillars of convergence (illustrated as horizontal purple, blue, green and red headings) are key areas of intersection between solving specific security leadership challenges (all regular text bulleted items in the matrix) in the respective area of consideration (from the highest order of the organization to program level, top and downward).

RANGE OF OUTCOMES

The purpose of convergence is for security practitioners to be more successful. How will proactively undertaking convergence improve security programs and experience of practitioners?

- Working across the decision-maker spectrum to understand their priorities and partner in their success changes the perception of security.
- Align security projects to deliver more value to stakeholders, increasing the likelihood for funding.
- Solve new and inherent security challenges through innovative approaches, new methods and practices.
- Building credibility with stakeholders to gain access to specialized resources (cyber, IT, audit, AI, etc.)
- Building partnerships to eliminate the need for duplicitous resources to operate or maintain systems.

3 TECHNOLOGY: NAVIGATING UNPRECEDENTED OPPORTUNITY & COMPLEXITY

The physical security industry has undergone three major technology paradigm shifts throughout its history. This section reviews the latest paradigm shift in key areas of technology within the physical industry, advantages they bring, considerations and how convergence is applicable (if not requisite) for success, not to lose sight of existing technology which needs to be addressed, ranging from legacy to current, that may be insecure or conflict with InfoSec policy.

INDUSTRY SNAPSHOT: THREE TECHNOLOGY PARADIGM SHIFTS FROM MECHANICAL APPARATUS TO ELECTRONIC SYSTEMS

This shift ushered in a different range of controls to monitor, interact and react to specific environment states or events in different ways, but mainly the ability to specify and scale and add consistency due to less reliance on humans which were needed to perform all functions through presence, observation and enforcement.

HELLO WORLD: IP-ENABLED DEVICES AND SYSTEMS

The next shift occurred when the industry eventually embraced network-enabling systems and devices. This shift led to a variety of operational and financial benefits by enabling technology to join a digital community, enabling systems to communicate with one another, facilitating remote management, centralizing logs data and reporting and delivering alerts from one device to some other interface in a different location, and also facilitated centralizing systems, consolidating databases and infrastructure, where many users could share access (as opposed to servers in each location that could only be accessed at that location).

MODALITY AND LOGIC

The current wave represents technology that is fairly diverse but is best summed up by two concepts: First, newer modalities in terms of where they deploy or exist in different ways that provide more advantages, such as cloud, mobile and virtualization, and second, newer technology that specializes in greater visibility, deeper intelligence and increased logic (e.g., AI, machine learning, automations).

In reality, both areas are seldom isolated from one another, and combined they result in a superset application – for example, an anomaly detection system in the cloud that analyzes system logs, virtual identity and user mobile telemetry data to analyze user behavior against specific controls and in turn producing alerts and automated response actions).

RIPPLE EFFECT

Each paradigm shift represented significant opportunities but also substantial challenges that set the stage for the industry to work through in subsequent years. It's not a bad thing, and not even a situation unique to physical security; nevertheless, it's a reality that must be confronted.

The major paradigm shifts generally take root in the physical security industry borrowing technology innovated and being adopted in other domains, none of which the physical security industry are experts previously. While the industry embarks on adopting AI, it's still getting its arms around encryption, properly securing IP devices or adequately managing them (status, patching, asset class, etc.).

3.1   EVERYTHING LOOKS A LOT LIKE IT

A couple of decades ago, physical security systems were fairly siloed from other departments and in most cases other systems within their own programs. Forward another decade, integration between physical security systems became more common, but systems were still fairly closed, commonly proprietary, with limited APIs and a range of other deficiencies that were common in IT systems.

In recent years, many aspects have improved. In fact, they had to as a prerequisite to even consider adopting the recent innovations. Imagine an intelligence project that needs data from a system that has no APIs to get the data out effectively (hint: limited data = limited insights)?

In fact, most of the improvements that have been iterating aren't novel but are things that IT systems already had already incorporated as common practice. It's hard to see, because it wasn't any single thing or event, but physical security systems came to look very similar to IT systems. Aside from their application (how they are applied and the environment in which they are used, i.e., "purpose"), modern physical security systems are nearly indistinguishable from those in IT.

Considering the challenges the industry has had with the backside of adopting new technology, having an IT system profile both places a specific burden on physical security professionals but also eliminates quite a bit of ambiguity about what the appropriate response needs to be.

3.2 CYBERSECURITY IN PHYSICAL SECURITY

As the attack surface expands for new technology being considered, existing nonconformant implementations will easily get flagged by IT, InfoSec and auditors in the normal course of transparency, planning or collaboration of resources to better sustain environment.

It's in the realm of impossibility that IT and InfoSec will adopt physical security's policies and practices to make their own in reconciling these types of variances. IT ops and cybersecurity have spent years refining their approaches, establishing best practices and gaining the type of maturity that physical security should have already possessed; however, cybersecurity requires specific skills, and there are several areas within it that require deep expertise. For example, professionals that specialize in network security generally aren't application security engineers, and neither are cryptographers penetration testers. For these reasons, many physical security leaders are overwhelmed by the pressure of meeting cybersecurity measures. But it's for those very same reasons leaders don't have to go it alone and should be looking to partner with existing specialized resources within their organizations rather than tasking physical security staff to spend years on becoming cybersecurity experts (because this is really what it takes). Other departments have demonstrated that they can work through similar pressures and transition toward having these functions become more of a central shared service model that can be relied upon (even shift such responsibility to) and get out of the business of running a parallel duplicitous set of functions.

While new technology presents opportunity and a new set of challenges, the physical security industry will need to also reckon with challenges regarding their existing environments, some of which might be more recent investments that need to be brought into compliance, while others may be older and make doing so not feasible or even possible.

3.3 CONVERGENCE BEST PRACTICES FOR PHYSICAL CYBERSECURITY

Too often recommendations are oversimplified to "work closely with IT to address cybersecurity," but it would be misleading to infer that this was either the first step or adequate in scope. The reality is that IT has applicable scope that intersects with cybersecurity, InfoSec sits squarely in the middle of it, yet neither of them addresses the complete picture.

Ultimately, end users are responsible for what's selected, what's installed and the impact that may result within their environment – regardless of the actions of other parties. This is why physical security leaders need to devise a plan to increase cybersecurity maturity throughout their selection process, requirements, design, valuation of proper configuration, regular audits and periodic penetration testing.

Physical security end users won't become experts in cybersecurity; neither will their integrators. It's too deep, there are too many specializations within, and would be duplicitous to those resources that already exist on the InfoSec side of the organization. Convergence is the most efficient, effective and reasonable way to achieve this.

ALIGN CYBERSECURITY PRINCIPLES AND POLICY

The core objectives of physical and cybersecurity are quite similar. While specific scope, context, and application may be different, the core principles really shouldn't be. Concerning systems, cybersecurity has a great deal more maturity and specialization in developing effective policy than physical security. Therefore, physical security should seek all InfoSec policies and embrace them as their own — if the device is electronic, it should be in scope.

ENGAGE AUDITORS WHERE POSSIBLE

InfoSec can only help with remedies based on what's presented to them or they test for themselves. Unfortunately, physical security experts aren't cybercity experts and often can't adequately identify what should be put forward for consideration nor does it make sense for InfoSec to test everything.

Rather, physical security should first seek to understand ALL of the nonconformities (against organizational cybersecurity policies). Auditors, who are commonly separated from IT and InfoSec's reporting structure (for good reason), independently perform this specific role in nearly every other part of an organization. In fact, it's likely to happen in the future anyhow so it's best to involve them early to help them

acclimate to looking at physical security the right way. While they won't be familiar with physical systems, they will know what to look for concerning conformance to specific policy and regulatory obligations.

PARTNER WITH INFOSEC

Keeping in mind that audit compliance is well intended, but being compliant means just that, not necessarily that it goes far enough. Work closely with InfoSec in reviewing audit findings, areas of noncompliance and potential remedies. In addition, critical applications and devices should undergo further review, potential testing and threat modeling for selective consideration.

ENGAGE IT

Some remedies and improvements will require IT's assistance, while for others they can offer advice. Very little of this is new to them, as they've already worked through these same issues in their own environments and have developed repeatable and scalable operations, which should be the goal versus ad hoc solutions for each issue, device or application. IT is also going to be in the middle initiative that supports different departments and will have insight into how internal standards are developing so being interoperable with others tomorrow is more likely and sustainable.

BE AWARE OF SPECIALIZATION

IT is often thought of this all-inclusive umbrella, but it isn't. Physical security should endeavor to identify who in IT to engage for productive conversations. For example, those that specialize in networking are completely different than those making decisions about password management mechanisms. While identity and access management specialists would be appropriate on technical matters, a project could also require nontechnical stakeholders who may own the identity itself (in some cases, HR).

Similar considerations exist on the InfoSec front. There are several specializations within the InfoSec domain in which it takes years to become an expert. Being an expert in one area doesn't translate to having requisite knowledge in another area to provide sound advice. For example, it wouldn't be appropriate to solicit advice from a network security specialist regarding application security. For the latter, an application security specialist should be engaged. The same goes for encryption matters (cryptographers) and so on.

EVALUATE RISK

Physical security leaders must commit to moving away from practices that don't incorporate system integrity and cybersecurity by design. While it's impossible to secure everything to the degree desired, decisions should be made using an enterprise security risk management (ESRM) (CH 6) model – not by estimating based on past experience or occurrence.

PERFORM VALIDATION

The bulk of deployments within physical security will continue to be performed by integrators who are indispensable for their expertise – getting these applications and devices to do what is intended – but they too are in a similar learning curve regarding cybersecurity. While they have the best intentions, end users should consider a process to inspect every deployment for conformance with cybersecurity policy and practices.

It might not be feasible to inspect all work at scale in all locations. This is where partnering with IT and InfoSec is critical to consider using the same methodology and tools they employ for the same purposes – by implementing specific controls (limiting access or what settings can be performed), using automated remote auditing to detect noncompliance and even spot checking some devices in some locations.

GLOBAL SOURCING AND PROCUREMENT

Another area where physical security hasn't been well integrated is how they work with purchasing and global sourcing departments. Physical security often partners with purchasing but using different sets of requirements and contracts than what others use, which often leads to certain nonconformities, vulnerabilities and nonstandard technologies making their way into the program in the first place.

In addition, physical security should partner with global sourcing and legal to ensure that contracts evolve to reflect the desired supported validation process for work to be signed off, handling for vulnerabilities that are discovered and paths for remedy so it doesn't become a problem that persists throughout the rest of the application's life. The simplest manner to achieve this is to not be separate from IT and InfoSec in these relationships, or at least to try to use the same contracts to address similar topics as they do. Some procurement departments are so large and so isolated from one another in the same organization that they aren't aware that another person in their group interfaces with InfoSec with a different set of contracts than how they work with physical security — overlooking the common interests.

ENLIST RESOURCES

There already exist multiple IT and InfoSec functions within most organizations that perform all these aspects on behalf of nearly all other departments. Physical security leaders should ask themselves if owning these challenges is core to their charter and success or a distraction which is better served by experts already equipped to do so.

BUSINESS ACUMEN 4

This chapter discusses the key concepts of how physical security can assimilate their objectives into the interests of the business, hearts and minds of those who approve of budgets and where convergence facilitates these aspects.

4.1 PUTTING PHYSICAL SECURITY INTO ORGANIZATIONAL CONTEXT IS CRITICAL

All organizations have limited resources; therefore, it's not possible to fund the majority of requests for investment. Executive management will generally only fund either what is critical to achieving their core business objectives or risks where the impact exceeds their appetite to defer addressing them (and suffer the consequence). It's increasingly important to demonstrate that security and business objectives are relevant and should coexist.

4.1.1 CHANGING PERCEPTION

The perception of departments within an organization is highly correlated to the nature of their business function and contributions to organizational objectives. For example, a major manufacturing facility that produces a product that makes up a large share of revenue is quite obvious. Conversely, security isn't as straightforward, as its core function doesn't generate revenue, impact competitive market position or serve as a primary source for increasing profitability (again, core charter, perception, etc.).

OFTEN MEASURED INCORRECTLY AND PERCEIVED AS A COST CENTER

Aligning with stakeholders from departments that are closer to the direct contribution model changes the visibility and perception of how others see security. Too often, physical security is siloed on the outer edges of this model, leading to the perception that it's a cost center, a part of real estate or a bundle of facility "assets." This frequently leads to being structured to report into a similarly perceived business function (real estate, facilities, etc.). The downside is then physical security is often measured by those same departmental metrics, such as cost + value of services delivered per square foot. The result is significant incentive for nonsecurity management to endeavor setting cost containment objectives to improve these metrics, which aren't even remotely aligned with security objectives. Additionally,

real estate management executives too often won't prioritize security objectives if they jeopardize said metrics.

SOLUTION VS. TACTICAL

As compelling as technology has become, the era within physical security end-user environments won't be defined by security being better, faster or more feature rich. Rather, how intimately we understand the challenges and selectively infuse innovations to improve outcomes ultimately changes the paradigm for end users.

Recent technical advances represent unprecedented opportunities; however, the ones chosen to be pursued must correlate back to enabling the business's core objectives and operate within a model used by the rest of the organization to gain greater support. Without this, security remains on the edges, unable to adequately influence support to execute.

DEFINING RETURNS ON INVESTMENT (ROI)

Executives expect an effective business case. Too often, security leaders are able to demonstrate how their proposals will be cash flow positive, yet the majority of the time they still fail to get funding. Executives already have detailed plans to increase top and bottom lines. For example, if the chief financial officer has committed goals to increase profits by $200 million, cobbling this together across dozens of projects isn't desirable – too many projects, resources spread thin and not core to their business. Rather, they primarily want to know if what's being proposed is absolutely essential. In more direct terms, "can I afford to NOT fund what's being proposed?" If the answer is "yes," funding is unlikely (at least this time around). If the answer is "no" then regardless of ROI, budgets get moved around to provide appropriate support. ROI adds sensibility to a story but can't be the main theme. Security leaders need to tie into the success of executive's core commitments.

Executives don't endeavor to spend money on technology or security; rather, they invest in solutions where success has a major dependency on the technology being proposed. From this viewpoint, executives that approve of budgets, technology and security are respectively the technical components of solutions achieving solutions and mitigating risk.

4.1.2 LEADING ORGANIZATIONAL DRIVERS

While business fundamentals remain constant, how executives chart a strategic course to execute changes based on markets and business environments evolves. The following section outlines contemporary drivers that are defining key initiatives where physical security is increasingly requested to participate with other stakeholders or represents an opportunity to do so (Detailed information on this topic can be found in Appendix 9.1-4)

- Business Transformation
- Pandemic Response
- Sustainability
- Governance & Compliance
- Risk

4.2 SUMMARY OF BEST PRACTICES FOR BUSINESS ASSIMILATION

IDENTIFY THE ORGANIZATIONAL LANDSCAPE

- What are the CEO's top three mandates?
- Who are key stakeholders?
- What are each stakeholder's top initiatives?

DETERMINE RELEVANCE, ROLE AND CRITICAL NATURE WITHIN PRIORITIZED INITIATIVES

- Do they have any physical security components?
- Have these been assessed and determined without engaging physical security?
- What additional value and impact can physical security have to achieve desired outcomes?

DEVELOP COMMON INCENTIVES

- Assimilate the needs of security to align with the established business goals of the organization.
- Convey the indispensable role of physical security's needs to the success of business goal.
- Can the business afford NOT to approve physical security's proposal?

REEVALUATE REPORTING STRUCTURE

- What are the specific success metrics for physical security? Can they be quantified?
- Do they accurately represent physical security's charter or someone else's?
- Does current reporting structure facilitate or present a barrier to a success model?

BUILD ALLIANCES AND BORROW PAGES OF OTHERS' PLAYBOOKS

- Build relationships with key stakeholders, not for one project but rather ongoing as the plan for them.
- Explore if there exists another risk domain which already uses the correct measurement of success.
- Learn, borrow and adopt successful models from other departments.

CONVERGING PERSPECTIVES ABOUT RISK AND SECURITY 5

Let's face it – security only exists to mitigate specified risks. Good risk management requires a proven and effective methodology to assess, determine and manage. It's also critical to be able to be able to communicate the scope, criticality and potential remedy of risks to different constituents within the organization to gain support.

Just as physical security generally practices tiering of different types of facilities and access points pertaining to their critical nature and using as a basis for relevant guidance, the greater organization also has well-established guidance mechanisms for risk guidance. It's generally used for all business facing functions to make decisions. However, too often, physical security doesn't observe it (or aware of its existence) which leads to lack of proper classification, relevance and context of security concerns being presented – and more often than not being declined for funding. This section will review how physical security converges with how the rest of the organization practices risk and how to participate and achieve greater success in moving security concerns forward.

According to Helen Negre, chief cybersecurity officer at Siemens USA, "Siemens is a high-collaboration, high-communication environment, and that feeds into everything we do, including risk management. Risk is not something hidden or siloed – it's discussed across all areas of our organization. You cannot have true enterprise risk management without evaluating risk across the entire enterprise and having a response strategy that includes reduction, transference and avoidance efforts that take the entire organization into account."

5.1   ORGANIZATIONAL MINDSET

Executives responsible for approving security funding generally entertain remediating dozens or even hundreds of risks, yet they only have resources to approve a fraction of them. When proposed investments fail to impress executives as to whether they are required to execute strategic objectives, they often decline, no matter the asserted ROI. The exception is for risks that executives can't afford NOT to approve (because the impact of the risk occurring is far greater than their appetite to carry the risk). It's those stakeholders who can communicate most effectively with decision makers on their terms that are more inclined to get funding. Most risk owners in an organization aren't within the security domain but are able to place risk in a business context within a framework that executives use and expect.

Executives are accustomed to how these conversations play out with stakeholders and are looking for a very specific exchange of information. When physical security proposes budgets for program improvements, increased preparedness or event mitigations without converting them into the same metrics that everyone else uses, it's effectively two different conversations about the same thing.

PRIORITIZING FOCUS AROUND RISK MAKES SENSE TO ACHIEVE SECURITY OBJECTIVES

For years, physical security had been able to manage risks within their program inside an opaque wall – part art of this has been that some aspects of physical security are difficult to quantify, and to some extent the culture of operating as a silo apart from other business units (BUs) and risk functions was pervasive. However, with increased pressure on OpEx budgets and CapEx requests, this approach just isn't sustainable, and physical security needs to embrace the same risk practices as the rest of the organization to be viewed as a relevant risk stakeholder – not just as security experts.

Organizations need experts who look at their environment from a security perspective, but they need to contemporaneously see security in context of risk and be able to communicate this effectively to the rest of the organization while surrendering to the fact that most decisions are made outside of the security domain.

5.1.1 CONVERGING LANGUAGE AND PRACTICES TO WORK TOGETHER (METHODOLOGY)

Most organizations have established and employ risk management frameworks. While maturity of actual implementation between organizations may vary, these frameworks are generally based on published standards and share core elements (for example, ISO 310000:2018 focuses on the principles, process and integrating risk across an organization, while IEC 31010:2019 dives deeper into specific techniques for assessment, risk management and decision making.).

Unfortunately, most physical security leaders haven't yet redesigned their approach to risk around these standards and have only marginally aligned practices to those of their internal stakeholder peers. As a result, there are significant gaps between how groups would assess, interpret, quantify and make decisions about the same risk. The transition can be daunting for many physical security leaders, ranging from upending entrenched practices to trepidation about how to design such a new approach. The good news is physical security doesn't need to reinvent how to do this on its own. Rather, the process is about discovery of what practices have already been established and are in use and engaging with others internally that employ them – convergence of people and process to get there.

5.1.2 CONVERGENCE OF CULTURES

This journey will require a significant adjustment for most physical security leaders: not only embracing a new model, but trickling down into how remediation measures are prioritized, controls are purposely designed and various operational areas are adapted.

PRACTICES

Risks that don't involve security elements do exist throughout the organization, which is why there's a broad risk framework that can be used by all stakeholders across the organization, including security. Frameworks generally entail practices that are repeatable, scalable and employable regardless of business unit, which helps all participants collaborate on multifaceted risk, understand the potential impact and accurately consider the context of the property treatment.

STRUCTURE

Most risks have owners but have many elements that require participation of various expert resources to properly assess and design appropriate remedies. For collaboration across various disciplines that report into different business units (and not have concerns stuck within a specific BU), a specific risk program management structure needs to be employed through committees, dotted-line reporting and procedures to enable appropriate visibility, progression and handling.

LANGUAGE

Not to be underestimated, adoption of common practices across a broad spectrum of business disciplines (within a committee structure) requires a common language. Using common references from one discipline might not be well understood by the rest of the participants or be best suited to be applied within a diverse group.

5.2 GUIDANCE

Ultimately, the goal for a security leader should be to reduce risk that is determined to be undesirable for the organization and in turn gain support for adequate resources to execute. In the increasingly complex business environment and evolving threat landscape, employing a risk-reduction strategy is required.

However, when a security leader's objective is to gain support for addressing specific risks, the core focus should be on determining if the business can afford to NOT support the proposed treatment. If the answer is any variation of "yes," then unless it's packaged under another initiative that had the opposite answer, it's unlikely that support will be provided. There are steps physical security practitioners can take.

BECOME A CRITICAL COMPONENT OF FUNDED RISK

Funded risk exists somewhere in the rest of the organization. Often, physical security functions are components of the treatment, but it is poorly defined, inaccurate and not disclosed to physical security. Don't assume these are being quantified and specified correctly.

Physical security leaders need to engage proactively with other risk owners, identify risks that are likely to have higher ratings and help define treatments which include physical security measures that reduce residual risk metrics (improve projected outcomes).

OBTAIN DOCUMENTATION

Seek and collect all information regarding the ESRM program employed within the organization. Identify and familiarize the organizational risk classification model, governance structure and decision-making process.

ADOPT AND ADAPT

Security leaders need to embrace how the rest of the organization thinks about risk – and work with them. Bridging the gap between physical security culture and practices and how the rest of the organization makes risk-based decisions requires adopting their frameworks and processes.

FIND MENTORS

Reach out to stakeholders about their journeys – everyone has gone through some transformation to use the same methodology from where they were prior.

REVISE RISK PERSPECTIVES

If not already using an ESRM model, reassess the currently employed methodology on how physical security defines, documents and managed risk. Ensure that risk management is bifurcated from event response and the standard operating procedure (SOP) process.

MEET WITH STAKEHOLDERS

Generally, risk owners will be either stakeholders or those designated by them. Note the difference between technical "requirement approvers" and risk owners – seldom are they the same.

BRIEF DIRECT MANAGEMENT

Brief direct management about changes that need to be made regarding risk management, how this impacts existing program priorities and where their support is needed.

MEET WITH THE CHIEF RISK OFFICER

While well versed in risk, the chief risk officer (CRO) might not completely understand the scope of physical security and some of the unique aspects that accompany it. The objective here is not to advocate any specific risks but rather to get their advice in ramping up participation in ESRM and gain their support in navigating obstacles commonly presented to physical security leaders that don't report directly into a risk function.

There's quite a bit CROs can do – they are executives and are accustomed to meeting with senior executives to create common incentive models and dotted lines that can't be ignored by direct reports which have competing objectives or metrics. In fact, this is a top priority for a CRO, so there should be common ground.

WAIVERS

If waivers are implemented in the organization's risk framework, investigate the criteria for how durations are assigned. Revisit past proposals which requested support for risk remediation that were declined. Seek documentation as to whether a waiver was provided or reasons why they weren't – this could be due to misclassification of risk or process not being followed. Attempt to get waivers mapped to them in retrospect or be prepared to request a waiver the next time they're proposed and deferred.

STAY ENGAGED

Sometimes security can feel like good security isn't a priority for the rest of the organization, but through these measures practitioners will find a broad community that is passionate about risk. Now knowing how to leverage risk to prioritize and improve security outcomes, consider getting involved on committees to establish physical security leadership as a peer and help shape the process (and perhaps more influence to implement the waiver if they aren't already).

GOVERNANCE 6

Governance is generally thought of as oversight, but it has broader meaning and application including the structures, processes and practices in place to ensure execution and accountability. From a security standpoint, these are critical mechanisms to ensure that expectations are defined, managed and executed.
- Implement decision-making authorities, decision processes and accountability.
- Program charter, goals and core principles
- Ensure that obligations are managed and achieved (regulatory, third parties, etc.)
- Create and oversee methodologies, practices and policies
- Processes to validate implementation measure performance against intended results
- Facilitate improvement and corrective action for noncompliance

CRITICAL CONTENT FOR PHYSICAL SECURITY

A key concept of convergence is the ability for various business functions that possess different domain expertise to work together to achieve better outcomes. This paper has underscored the functional areas where this occurs: technology, risk and assimilating these aspects into the business both beyond and inclusive of physical security departmental interests.

While cybersecurity has gained recognition across the physical security industry as a top priority to reconcile, governance hasn't made the headlines. However, for the rest of the organization, governance arguably has higher billing than cybersecurity since executives recognize that the two are inextricably linked and cybersecurity can never be better than their ability to govern it. Good governance is necessary for good security.

CONFUSION BETWEEN GOVERNANCE AND COMPLIANCE

Whereas governance is focused internally on unique circumstances ("what should we do"), compliance measures are due to an external mandate resulting in having to meet a specific criterion ("what must we do") such as industry and regulatory requirements. They definitely intersect, and the key is devising solutions that incorporate both. For example, meeting a compliance item might satisfy a regulatory

obligation item but likely doesn't go far enough to adequately remedy a specific risk or scope of risks in that environment. Most compliance measures are specific for an industry and designed as the lowest common denominator to ensure most that need to comply find it feasible to do so.

Translation: contrary to broad perception, compliance is really the minimum – not the end state. It's up to the organization to look at the bigger picture across all regulatory obligations, risks and business considerations to formulate the best policies, controls and plans that meet all commitments and program goals holistically.

KEY TRANSITION AREAS

IT has long subscribed to an IT governance model where all organization regulatory and organizational commitments are documented, crossmapped, performed and audited. Conversely, most physical security programs haven't yet instituted a formal and comprehensive governance program and largely distribute some of these responsibilities across practice areas or teams.

Evidence of this is such that physical security programs that formalize governance programs tend to cover the same areas of their IT counterparts and consider very similar standards around systems, security, audits, validation, etc. Many of the common practices within physical security wouldn't be compliant using the same metrics, and prioritizing cybersecurity would have come much sooner.

Interpreting what is secure, why and what approaches would be acceptable is based on core principles that shouldn't vary between the physical and IT realms. How things might be executed may vary due to circumstance (application, resources, feasibility, etc.), but perspective, assessment methodologies and decision making should be the same. The fact that for so long that they haven't been is arguably the root of the delay of cybersecurity consideration and the connective tissue for all aspects of convergence. For these reasons, many physical security leaders are advised to implement or reengineer their governance programs to incorporate and align with those which already exist within IT and InfoSec and across the organization. They should avoid duplicity and only be unique where an area of physical security requires further consideration to execute.

6.1   BEST PRACTICES FOR GOVERNANCE CONVERGENCE

For many physical security leaders, prioritizing and building a formal governance program will be a significant shift in methodology, practice and skill sets; however, if leaders are expecting different results with respect to cybersecurity, intelligence outcomes and being accepted by their counters, it's an inevitable journey.

UNDERSTAND ORGANIZATIONAL COMMITMENTS

- Meet with stakeholders outside of physical security.
- Gain insight into what specific regulatory compliance obligations the organization must meet.
- Perform a documented mapping between compliance items, controls and physical functions.

PARTNER WITH INTERNAL GOVERNANCE, RISK, COMPLIANCE (GRC) TO UNDERSTAND THEIR FRAMEWORK

- Adopt all policies that currently don't exist or would be duplicitous.
- Engage in gap areas that don't exactly comport from IT to the concerns and nature of physical security.
- Don't reinvent the wheel, and leverage GRC tools, templates and guidelines.

DEVELOP CAPABILITIES

- Develop, improve and revise controls.
- Detection should distinguish from single events to control nonconformance and prioritize risk.
- Build device life cycle management policy and capabilities.

PARTNER WITH FINANCE

- Understand the data they use and assumptions they make for security assets.
- Implement asset management capabilities.
- Negotiate with finance, based on adequate visibility and more realistic "useful life" metrics.

NAVIGATE PRIVACY

- Determine compliance of systems and data with existing organizational privacy policy.
- Share existing data collected and plans for future collection (i.e., for intelligence).
- Consider federal and local laws, evolving laws and the ability to manage compliance at scale.

INVITE TRANSPARENCY

- Increase audit frequency, starting in areas that impact business critical operations and integrity.
- Share audit findings with GRC, InfoSec and IT to get coaching on how they deal with similar situations.
- Inite professional auditors to perform audit functions as they would in the rest of the business.

ESTABLISH DATA STANDARDS

- Industry vendors race to offer AI capabilities within applications.
- Consider how this data can be used outside their applications (and vice versa) to avoid new silos.
- Work with stakeholders to develop data standards that facilitate these objectives.

BUILD COMPETENCY

- Identify skills and resources required; provide training.
- Design metrics, means for visibility and regular reviews for corrective action.
- Consider partnering with resources from other departments who have unique skill sets.

WORK WITH OTHER STAKEHOLDERS TO IDENTIFY COMMON FUNCTIONS

- Evolving technology increasingly requires deep IT and InfoSec expertise.
- Explore a "shared" resource model with internal areas of expertise.
- Consider divesting custodial management where internal expertise exists (other departments already do this).

CONVERGENCE USE DISCUSSION IN KEY AREAS 7

This section will explore use cases of convergence, considering how to more effectively address challenges than with traditional approaches. The use cases focus on increasingly common challenges that physical security leaders face.

7.1.1 USE CASE: SURVEILLANCE MANAGEMENT
THE CHALLENGE

Most physical security organizations have a disproportionate number of people and facilities and more square footage to manage than resources they can allocate for appropriate coverage. Surveillance is an indispensable component of every security program – it's the eyes and ears of the security apparatus. But let's be honest: most organizations don't have the resources to watch even a fraction of them in real time. This is a major contributing factor leading the average enterprise to spend 35% to 60% of OpEx budgets on manned guard-related expenses and a major driver for leveraging AI to remedy real-time visibility and awareness.

Beyond challenges of visibility remain increasing pressure to improve how this infrastructure to implemented, managed and maintained. As discussed in Section 3, surveillance devices are becoming similar to those in IT and require the same approach to ensuring that their purpose remain available, maintain integrity and have reasonable controls in place to ensure that the proper custodial operations are being carried out such as firmware versions, patches, field of view or password compliance.

Unfortunately, the physical security industry hasn't had tools that were up to the task, leading to many organizations performing manual inspection rotations to inspect and validate each camera's operation, compliance and stream quality. Even in the best of cases, this approach is only a snapshot in time contracted by vulnerabilities which are pervasive the rest of the time.

SHORTCOMINGS & IMPACT

Key stakeholders, such as legal, compliance and investigators, rely on the availability, clarity and quality of surveillance artifacts to take meaningful action. This can range from prosecution to defense, or negotiation. Too often, when an event occurs prompting recall of video, it can't service its intended purpose due to being pixelated, choppy or never recorded. These can be caused by either technical or human errors. It's possible that they weren't set up properly. Bandwidth can be low or inconsistent, choking out quality. Even bad actors have been known to change the direction of the camera (or even repurpose them to surveil security while performing their attacks). In addition, as IT increasingly looks over the shoulders of physical security, these defects won't go unnoticed by seasoned auditors (even those not familiar with physical security systems).

CONVERGENCE APPROACH

While there's much (valid) discussion to use AI to alleviate the shortcomings of monitoring surveillance streams, AI can also be purposed to perform all of the audits and quality checks, validate settings and even possess the logic to self-correct issues that are found (like calling another application to fix the field of view of the camera to the designated setting, updating firmware, invoking credential updates or generating a service ticket subsequently alerting a group of people) – all automated at scale, performed continuously and arguably better than humans.

Implementing this model goes beyond technology. The use of AI leverages technology from other domains (algorithms, rules engines, specialized processors and protocols). It also requires an accurate accounting of the governance measures to implement. Many will require collaboration between people who have expertise in designing controls which baseline normative behaviors and define parameters for the AI to recognize outliers and subsequent orchestrations for meaningful actionable response.

OUTCOMES

Traditional approaches allocate disproportionate portions of their limited resources and budgets while falling far short of acceptable performance or result. This model is difficult to justify to management, as increasing additional resources doesn't really solve the scope of the issue since it just doesn't scale.

Conversely, when using convergence, possibilities for a solution become tangible, enabling stakeholders who rely on meeting executive-level mandates, executing key initiatives and addressing prioritized risk to be successful. Recognizing the difference

in relevance this makes to their priorities, stakeholders can more appropriately consider the benefits, value and consequences of their support – for example, driving down liability and litigation costs might actually be a CFO problem (and they sign the checks).

7.1.2 IDENTITY
THE CHALLENGE

In the business of security, many of the decisions that need to be made rely on understanding the identity of an individual and whether they have the permission to perform that's being observed or considered. Physical security has taken a narrow view, somewhat limited to an authorized user's permissions for access to a physical location, as a specific time and date.

Conversely, other security domains have long understood that a person's role, policy, behavior and events unrelated to access are critical considerations to performing conformance with controls that would otherwise escape them. As physical security organizations now endeavor to employ intelligence for predictive models to prevent undesirable events from occurring or produce more real-time data to reduce response times and impact, other elements concerning identity will need to be brought into scope for consideration and analysis and to archive the insight that's desired.

SHORTCOMINGS & IMPACT

There's a significant difference in objectives between managing access of authorized users and detecting and preventing whether specific risks are in play. For starters, recognizing that authorized users are compelled to follow policy while unauthorized users aren't in the age of zero trust, it could be argued that it's better to assume everyone isn't a good actor and ensure every assertion made by a person meets a minimum criterion that not only permits access, but also ensures that it's legitimate, observed and controlled.

From the perspective of physical security common practice, a narrower approach to managing access cards and door permissions might be acceptable; however, meeting evolving organizational demands such as OT initiatives requires a broader context, different perspective and more advanced practices (see 5.2.1).

For this, two things need to be recognized.
- First, the "identity of things" needs to come into scope. What types of objects users interact with, their proximity to them, and behavior, in combination with their identity and policy, provides improved context.

• Second, determine the context of the workspace in which the observed activity in question is occurring. Policies are contextual based on the entitlements of the individual, the scope of their job function and their environment (where). If an intelligence system can't understand the policy and the difference between the nature workspaces (work to be performed in those areas), then it can't infer intelligent conclusions.

CONVERGENCE APPROACH

Redefining identity involves a broader methodology beyond most contemporary physical security practices of issuing an ID badge, binding a card number to a user and propagating permissions to a static whitelist in a controller. First, recognize that a person's identity and what is understood about them should be the same regardless of the system, their location, or role, hence bifurcated issuance, life cycle, provisioning and controls should be viewed as a legacy proactive to be overcome.

All departments that have an interest in the use of a person's identity attributes, entitlements and behaviors should work together so they all flow from the same authoritative source to ensure timeliness and accuracy but also share audit trail data across stakeholders that have an interest.

Physical security should embrace the larger scope of policies related to job scope, regulatory compliance and controls developed outside their own department to consider how they might reengineer their controls (and road map systems to facilitate when making technology decisions). Meeting with stakeholders to understand the operational processes behind a user's job function, their workspace and the objects within it will provide better consideration as to policy conformance controls.

It should also be recognized that physical security should endeavor to consider a similar scope for how systems grant access to users in the first place. It's common for IT systems to have not only an authentication procedure, but also authorization. The first only judges the identity assertion provided by the user, while the latter considers a wide range of data (event logs or intelligence analysis outputs) to decide if a user should be granted access regardless of the validity of the authentication process. Unfortunately, predominant physical security access control infrastructures don't have these aspects in scope and will be a barrier to "actionable" measures that resemble something transformational, which many security leaders are hoping for.

OUTCOMES

Recognizing that identity best practices are universal and working across stakeholders to establish common operating mechanisms to work toward the same goals of controls, identity hygiene and actionable intelligence result in better security and drive down the costs. When subscribing to the same principles, objectives and dates, there's an opportunity to align people, systems and processes. Physical security infrastructure isn't designed or prepared to accommodate some of these concepts, but there's evidence of innovation from IT vendors that specialize in identity to extend into physical security to handle the identity aspects while providing access control companies focus on core functions related to risk identification, response and command and control, thereby being able to address a variety of stakeholder objectives, including the complexity of OT.

7.1.3 IDENTIFICATION
THE CHALLENGE

Access badges have been the de facto standard for users to prove their identities when requesting access to resources under the domain of physical security. While the radio frequency identification and chip technology underneath have undergone evolution to increase security and broaden use cases as to how the cards can be used, the fundamentals haven't changed much. They're physical tokens (such as a card or fob) that require a personalized process to acquire photos and identity information, validated, printed and distributed. Organizations also need to resource ongoing life cycle events that require name or role changes, lost or damaged card replacement and emergency access.

Conversely, IT generally has the same responsibilities concerning managing identity, authentication and the respective operations concerning user credentials; however, this is generally achieved with greater efficiency. This is partly due to their mostly being digital/virtual, eliminating much of in-person demands, but also the methods used mostly adopt standards so managing different methods across different providers supports heterogeneity. This provides the opportunity to choose a variety of authentication methods that will meet the needs of security level, across different applications and support new use cases. Conversely, while additional factors can be applied to card authentication, the card is still generally required, and the authentication payload underneath remains the same (strengthening confidence that the appropriate person possesses the card but not necessarily the transaction itself).

SHORTCOMINGS & IMPACT

Physical security leaders are increasingly looking for ways to operationalize their credential programs to be less demanding of resources, consumption of physical cards and supplies and reduce burden and downtime of users, which impacts satisfaction and productivity. They also need to solve other challenges discussed in this paper relating to improving controls, detection and building out intelligence. Logs produced by badge swipes are of limited utility in this respect; they only apply when a user actually swipes (usually on ingress and not egress) and generally only apply to access points with readers, leaving significant areas (inside and outside corporate facilities) without insight. In addition, these logs don't generate other types of metadata that would be beneficial to intelligence and authorization models.

CONVERGENCE APPROACH

Countless security leaders are borrowing what other stakeholders in their organizations have already been doing – virtualizing applications, making them portable and streamlining the operations and user experience in the process. Enter mobile credentials – these are neither invented by physical security nor all created equally. Some simply emulate a physical ID card in virtual form. One could argue whether this is convergence or not, though this debate is irrelevant. The significance is the means in which the solution provider has undertaken, by way of innovation, to facilitate the mobile app being able to offer various authentication methods and use cases, generate useful metadata and solve specific challenges that were previously beyond the reach of physical security.

A physical ID badge is generally a single use case device. A point of clarification; Where they've often provided more use cases (café, time and attendance, logical access, etc.) they've really just recycled the badge number as the authentication payload – not really a new application, just repurposed in ways that are not more secure (and arguably violating generally accepted IT governance policy in the process). The overall burden of cost and operations remains while not offering the type of shift that mobile credentials can offer.

Security leaders need to consider the broader implications of adopting mobile credentials. They don't own mobile device policy, mobile device management tools that IT ops use, and aren't experts at assessing mobile application security, which can be strong if done correctly but has a propensity for requiring an exacting approach. Physical security will need to engage with multiple resources from GRC to understand policy that applies to all departments, privacy obligations and IT ops to ensure there's an acceptable means to distribute and update the app.

OUTCOMES

Beyond virtualizing authentication, the mobile device has capabilities built in to process, generate and transmit a range of useful data that wasn't previously available to physical security yet was always desirable. Some aspects of convergence are simultaneously occurring at the reader level. Internet of Things concepts are being baked into next-generation readers which provide a new range of device capabilities but can work with mobile credentials in a smarter way to perform some preauthorization at the edge, convert different authentication methods into a transaction that legacy infrastructure can work with or execute some event-driven automated provisioning updates (or revocation) to offload operational burden.

Leaders that endeavor to venture beyond virtualizing a badge number and photo will introduce physical security to a range of new authentication factors, standards and choices of metadata and should eagerly collaborate with colleagues on how they're making decisions, using the data and forming intelligence to improve controls and detection. Working with cyber analysts would be a good start.

Also, risk managers likely see various risk owners across departments developing more creative and meaningful remediating controls which, in turn, might help identify where unique physical security data (presence of people, telemetry and occupancy) is the missing ingredient to a major (funded) initiative. After all, it's people who violate policy and controls, and relying only on IT's data is equally limiting. Being able to use both data sets (and reconcile with one another) provides incremental value.

8 CONCLUSION

Convergence has evolved over time, shifting from industry-driven excitement to a more nuanced understanding. Historical mistakes, like a lack of clear definition and organizational alignment, led to value shortfalls and challenges.
Recently, convergence has made a comeback, moving away from traditional ideas. Now it's driven by end users focused on specific organizational goals. This change highlights the importance of collaboration across departments, systems and people, going beyond just acquiring capabilities.

Today, convergence expands physical security into broader organizational objectives. Urgent business needs, especially during the pandemic, have driven convergence projects in areas like OT, crucial for critical infrastructure relying on industrial control systems. The demand for physical security to play a broader role is rising, seen in compliance mandates recognizing the need for controls over access to systems. This expands the role of physical security to address challenges like IP espionage, contamination prevention and data center security upgrades.

Physical security leaders are at a crossroads, feeling pressure to showcase outcomes and secure funding. Instead of incremental upgrades, they're adapting strategies, drawing inspiration from successful models in other departments. Breaking down industry silos is crucial, as the separation of physical security from IT hinders progress, and there is a need for collaborative engagement across diverse organizational domains.

As convergence gains momentum, the end user's path is found by evolving programs and changing perceptions. End users, vital in running security programs, play a pivotal role in defining convergence through shared challenges and successes. Different industry players will feel varying impacts. Manufacturers need to align offerings with evolving end-user demands, adapting to technologies like AI, mobile and cloud, often

collaborating with specialists from other industries. Convergence intersects with the rising importance of cybersecurity at the board level. As physical security integrates with IT, attention must be given to cybersecurity risks, with regulatory requirements emphasizing executive ownership, risk management and continuous awareness.

Regardless of one's stance, convergence is undeniably present. Industry stakeholders are strengthening positions and exploring new markets. The convergence narrative encourages active participation, adaptation and collaboration, promising a future that continues to break conventional boundaries.

APPENDIX
9.1 TECHNOLOGY
9.1.1 PARADIGM SHIFT ANALYSIS

This section analyzes technology segments and contrasts key differentiators of the most recent shift over the previous one and explores how these changes impact industry practitioners and warrant further consideration.

SOFTWARE

- Increasingly moving toward the cloud
- Applications using development frameworks and libraries
- Designed for native interoperability, supporting open APIs
- Agile development: More focus on near-term market demand via just-in-time approach to releases
- Integration/support for identity repositories

IMPACT

- Governance and security implications
- License models shift from CapEx to OpEx (significant challenge for physical security)
- Faster development pace and more stability
- Less complexity to integrate, with end users placing more emphasis on best-of-breed capability vs. vendor ecosystems

HARDWARE

- Commonly network enabled
- Narrower scope of capability but greater specialization
- Increasingly an edge device in form of Internet of Things (IoT) (uniquely different to manage)
- Increasingly resource-constrained (smaller, less compute power, lower thermal design power)
- Heavier logic processing on the server, with local functions performing specific apparatuses only
- Web interfaces and standard protocols used to access, receive instruction, move or publish data

IMPACT

- Generational leap in environmental visibility user behavior and asset intelligence capability
- Ease of installation, deployment and configuration
- Decreased cost per unit but more frequent refresh cycles and decreased end-of-life span
- Attack surface expands considerably, with significant governance, asset management and cybersecurity implications
- Less complexity to integrate, with less emphasis on vendor ecosystems vs. best-of-breed

INTELLIGENCE

- Increased priority by security leaders to adopt a "data-driven" approach to security
- Shift from reporting and analytics to insights (serve purpose rather than provide utility and process)
- Products collect more data and make assumptions about where it's stored and how it will be used
- Requires increased data collection to utilize for intelligence purposes
- Complimented by sensory, edge devices and applications from outside physical security
- Broader spectrum of spectrum of data increases; employment of AI to assimilate and process data

IMPACT

- Humans aren't good or efficient at assimilating larger sets of data, shifting how resources are staffed
- Requires definition of behavior and threats to detect; will force security programs to refine risk management
- Will necessitate standardization of data and metadata across entire organization to effectively utilize
- Significant pressure to rapidly improve maturity in privacy, security and integrity of data being relied upon
- Shift toward partnering with internal resources in different ways (and external partners with different skill sets)

SURVEILLANCE

- Over the last decade, much has moved from analog to IP (no longer novel)
- IP cameras moving toward an IoT profile
- Increasing prevalence of intelligence capabilities processed at edge or rely on back-end
- Emphasis moves toward detection, shifting from reactive to real-time and eventually predictive
- Advancements in device life cycle management (some using AI) to scale performance and conformance
- Leverage AI to correlate surveillance events to those in other systems to identify greater risk

IMPACT

- Shift from relying on humans to monitor streams to having intelligence detect prioritized events
- Addresses ineffective and disproportionate reliance on humans to monitor streams (doesn't scale)
- Less reliance on having events reported (or missing them) to automated and contextual notifications
- Little distinction between surveillance servers and IoT devices and those under IT's purview
- Significant looming security, privacy and governance requirements
- Urgency to implement high assurance of stream integrity, quality, availability and underlying data

ACCESS CONTROL & PHYSICAL IDENTITY

- Software is evolving is evolving considerably faster than related infrastructure
- Shift from disparate banal event tracing to informative root cause and priority to focus resources
- Moving from seeing the world through access and tamper points to workspace, environment and context
- More meaningful implementation of identity: compliance, behavior, detection and anomalies
- Increased risk vs. event focus starting to innovate detection for targeted and blended threats

IMPACT

- Deeper identity requires integration with IT's life cycle and role structure (not just attribute and status lookups)

- Redefining workspace viewpoints requires collaboration with stakeholders that use them (and incorporate policies)
- Leveraging AI to automate audits, monitor for governance conformance and compliance infractions
- Compelling incentives to transition infrastructure to be connected, sensory and standardized
- Collaborative exchange of physical identity data with cyber analysts for more complete picture respectively

MODALITY

- Applications are increasingly moving to the cloud
- Mobile breeding into physical security to be ubiquitous for access, monitoring and identity credentials
- Virtualization of servers, applications and even traditional hardware functions
- Increasing emphasis to leverage software-defined controls vs relying on hardware and related upgrade frequency
- Dedicated devices are increasingly becoming pervasive (gunshot, temperature, thermal, telemetry, etc.)

IMPACT

- Much different and larger attack surface
- More frequently physical applications reside on same devices (mobile) and platforms as IT applications
- Restrictions on east-west data flows may complicate hybrid environments with existing legacy technology
- Require different management models, skills, tools and policies
- Increased collaboration with IT and InfoSec to navigate planning and deployment models
- Increased collaboration with IT and internal GRC to execute proper evaluation, implementation and management

IDENTIFICATION

- Increased demand for higher assurance of identity where users are who they say they are
- Traditional card number as both identifier and authentication payload being scrutinized
- Increased pressure for physical security to leverage IT authentication credentials (OTP, FIDO, etc.)

- Virtualized identity (software-based) offers flexibility and opportunity to operationalize burdensome processes
- Shift toward increased controls of users to align with evolving physical identity goals and policies

IMPACT

- Industry will need to reconcile the absence of authorization layers for identity to implement many controls
- Organizations will need to manage varying forms of identity (badges will coexist with virtualization)
- Authentication payloads will be audited to same standards as IT authenticators, prompting overhaul
- Industry will face pressure to adopt and conform to InfoSec policy to deploy and sustain related implementation

OPERATIONS TECHNOLOGY

- Priority on business transformation driving analog and older systems to be modernized
- Putting analog systems onto a network that were never designed to be on the internet
- Adding and modifying components while repurposing and extending logic

IMPACT

- Not originally designed with adequate cybersecurity; expanded attack surface adds complexity
- Critical nature of OT functions prioritizes need to restrict, manage and audit user access
- Requires risk management maturity and extensive collaboration across domains

9.1.2 CONVERGING CYBERSECURITY WITH A RANGE OF REAL-WORLD CIRCUMSTANCES

SECURING NEW INVESTMENTS
NEW PLACES

Security standards don't get outsourced to the cloud — only the deployment. While there may be specific certifications that InfoSec may require, they can only tell part of the story. Certifications generally set a minimum criterion for consideration but lack specific prescriptive practices to conform to achieve certification. The latter part is up to organizations to perform their due diligence and ensure that providers meet specific expectations as they would if the deployment was internal.

There exists a broad range of topics and considerations that must be covered. InfoSec is fairly well accustomed to this analysis, whereas physical security isn't. For example, cloud providers often have many APIs in order to offer the broadest support possible for the range of customer environments/requirements that they may face, yet each API represents its own unique security risk and needs to be individually assessed. Will physical security set their own standards for API development, reviews and penetration testing of each one — or leave it to those that already undertake this on behalf of the rest of the organization?

It could also be that physical security has opted to adopt a public cloud (software as a service), where other end-user organizations also subscribe to the same service. While some certifications may require the provider to "address" how customer access and data is segregated and secured, very few will detail how. There exists a wide spectrum of performance in this area across the industry, but it is up to end users to inspect what they expect; what's conformant to their standards. Essentially every aspect that would be managed internally now needs to be done with each third party.

NEW WAYS

Outside of cloud technology itself, key decisions across a range of permissions and connections need to be made and managed. A cloud provider has little value if that service (and its data) is locked in a silo, hence there exist reasonable expectations that integration of application logic and respective data to be available to other applications (and vice versa) to be used for broader intelligence endeavors and audit requirements.

Enterprises generally don't allow outside applications to communicate which whatever internal applications they wish, and certainly not directly. They have strict rules and approvals — ranging from specific ports, directing through DMZs or one direction but not the other, etc. (commonly regarded as "east-west traffic").

Adoption of cloud intersecting with requirements of working with internal hosted applications can get complex due to limitations on what might be allowed to communicate with one another (and in what sequence). For example, moving an access control system to the cloud would mean that an external application would need access to controllers, and vice versa, which would be on a secured network, while the cloud likely wouldn't be permitted to speak directly to it. This gets further complicated should it be proposed that the cloud application ingest data from other systems to make better decisions (for example, surveillance data).

A maze of permissions starts to reveal itself as a major impediment to executing the desired next-generation opportunity. Fortunately, IT and InfoSec are fairly accustomed to this entire scope of consideration and planning. Physical security seldom operates their own network and therefore will need to work collaboratively to determine what is permitted and how to accomplish what's intended.

NEW THINGS

IoT devices, purpose-built for specific areas, offer sensory feedback, enhancing physical security with valuable information. Due to their small footprint, low cost and ease of setup, IoT devices are becoming integral to intelligence goals and are set to proliferate in physical security environments. Even users not prioritizing IoT deployment may encounter traditional hardware evolving to resemble IoT devices as they refresh components, especially AI-incorporated IP cameras operating at the edge.

However, IoT devices pose unique cybersecurity challenges. Many are hard-wired and easy to set up without IT department knowledge, and manufacturers often prioritize functionality over vulnerability testing, leading to potential weaknesses. Default passwords and symmetric keys are common, making devices vulnerable from the start.

The variety of IoT devices, protocols and APIs complicates oversight for IT applications, hindering tasks like firmware updates, patching and enforcing password

policies. The risk, often downplayed by physical security experts, lies in attackers exploiting weak systems as initial entry points to access networks or execute objectives, turning seemingly low-risk devices into significant threats.

Beyond hardware, IoT encompasses virtualized forms like mobile devices. While fixed in hardware, mobile devices take on different IoT profiles through apps, collecting sensory data and accessing protocols. Recognizing their versatility, mobile devices should be treated and secured as distinct IoT entities.

SECURING EXISTING SYSTEMS TO A NEW STANDARD

Many systems currently employed by end users aren't "next generation" but are still within their useful life and serve their intended purpose. Physical security practitioners also need to continue to come to terms with properly assessing whether these systems possess adequate security.

There exists consensus that the industry is playing catch-up" with cybersecurity, which is simple in concept but without prescription. Proper context around the situation would distinguish the roles and responsibilities of parties within the manufacturer, integrator and end-user community.

Software vendors that operate a service can iterate the code behind the scenes and push out smaller but frequent updates transparently to end-user environments. Manufacturers who don't employ a service model can make patches available or at minimum look to their next versions being more robust.

However, end users who generally don't have control over the source code of their commercial off-the-shelf systems face evolving threats, expanding attack surface and maturing policies to deal with for years. Unfortunately, within this broad community of third parties, too often resources and priorities vary, expertise isn't yet adequate or processes aren't put in place to provide the consistent performance that's required.

TECHNOLOGY THAT CAN'T BE ADEQUATELY SECURED

Many end users face aging systems whose design didn't foresee to incorporate the type of protections that today's environment requires and can't be adequately updated or patched. Many end users don't have adequate budgets to replace older systems, never mind contending with newer ones where vulnerabilities emerge that can't be fixed. OT systems can also fall into this category.

9.2 BUSINESS ACUMEN: EXPANDED
9.2.1

MANDATES SHAPE INITIATIVES AND BUDGETS

Executives establish organizational mandates to achieve very specific business performance outcomes. They flow from executives down to stakeholders as priorities to achieve. Stakeholders respond by devising the means in form of key initiatives — outlining specific objectives and future-state outcomes.

Initiatives generally require a variety of resources, While that's typically a challenge for most projects, alignment in these areas gains enough support at the executive levels to form a common incentive model for all participants to reprioritize availability, cooperate and collaborate to achieve success. A working example of this model incorporating recent initiatives that many in the industry experienced due to the pandemic is illustrated in figure 2.
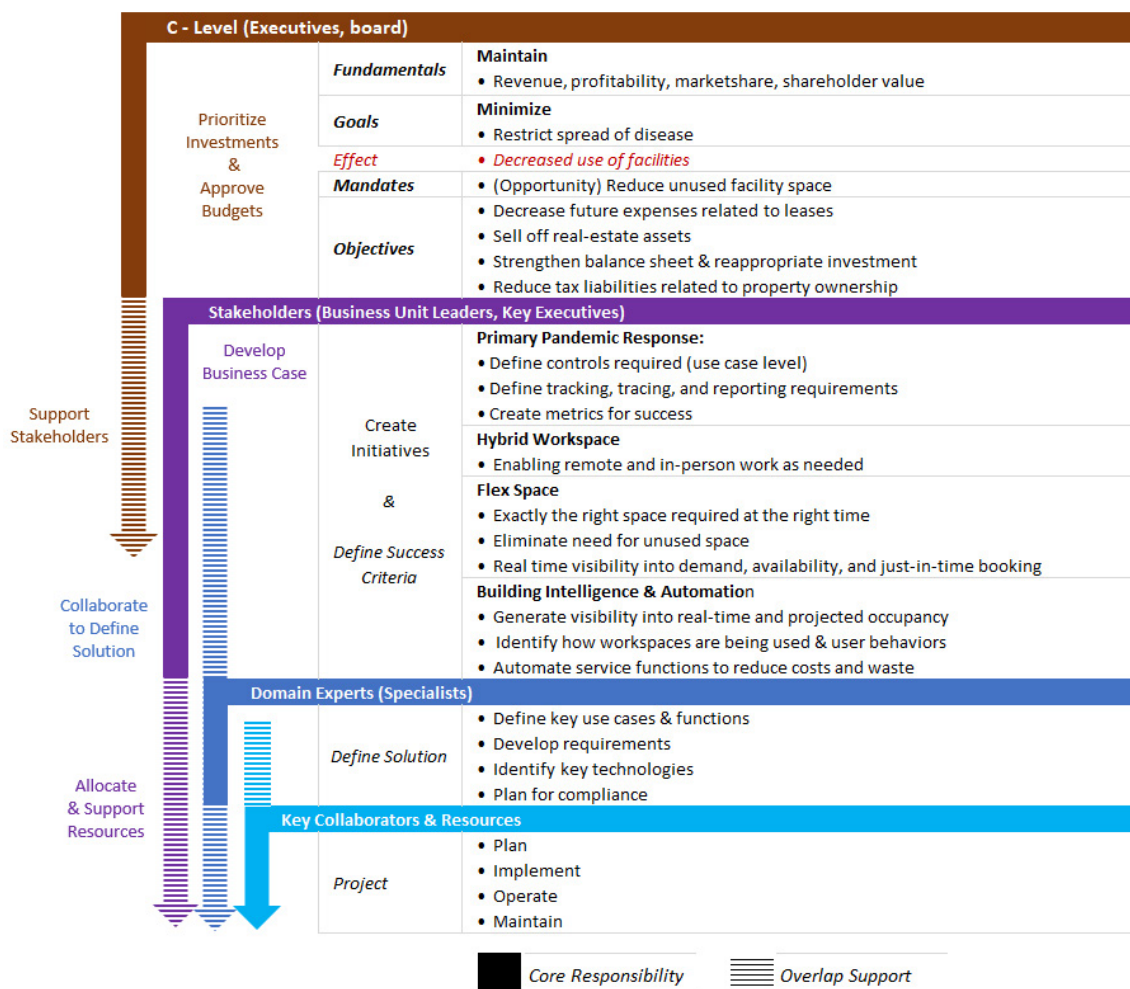
9.2.2

LEADING DRIVERS DEFINING INITIATIVES

While business fundamentals remain constant, how executives chart a strategic course to execute changes based on markets and business environments evolve. The following section outlines contemporary drivers defining key initiatives where physical security is increasingly requested to participate with other stakeholders or represents an opportunity to do so.

BUSINESS TRANSFORMATION

"Business transformation" represents a range of drivers behind these developments within the modern business environment, which is a concept of fundamentally changing business processes, systems, people and technology to better support business strategy and produce measurable results in efficiency and shareholder and customer satisfaction.

Many elements of this concept aren't new, yet with most organizations transitioned to a digital paradigm combined with new technology being purpose-designed to facilitate optimizations, it's an invitation for executives to be more aspirational and likely achievable. It's not surprising that this concept has become a top priority within the C-level community and sets in motion the demands they place on stakeholders, the contributions they make and where budgets are appropriated.

INFLUENCE ON INITIATIVES
- Anywhere efficiencies can be made and advantages can be realized
- Could be modernizing systems, operations, consolidation, speed of production or delivery and optimizing insights
- Incipient "Identity 2.0" initiatives are a good example of this

PANDEMIC

The pandemic presented sudden and significant challenges which stimulated mandates as a response. In turn, demand for solutions catalyzed initiatives which generated specific high-priority projects where physical security plays a critical role.

INFLUENCE ON INITIATIVES (SEE FIGURE 2)
- People tracking, tracing and reporting for regulatory compliance
- Hybrid workspace and flex space
- Building intelligence, efficiency and automation

SUSTAINABILITY

From a traditional standpoint, sustainability might be out of view, but it has corporations investing billions to meet long-term strategic goals. Sustainability is about the overall cumulative effect; therefore, anywhere that can be reduced for measurable impact is not immediately ruled out of scope: reducing carbon, pollution, energy, resources and waste.

INFLUENCE ON INITIATIVES

- Refresh hardware with lower power and environmentally sustainable material equipment (client).
- Consolidate servers to be centrally located and managed (host). Lean toward cloud and virtualized options.
- Reduce nongreen physical identity badges and consumable supplies (cards, sleeves, inks, etc.)

RISK

From the organization's standpoint, security is the technology and operational solution to a risk problem. The question for executives is whether the likelihood and impact exceed their appetite to "self-insure" and decline to remediation measures.

INFLUENCE ON INITIATIVES

- Approved risk remediation can assert swift plan of action and budget and resource allocations
- Depends on metrics used and residual risk scores to applied specific risks (see CH 5 for more details)
- Risks that have elements of physical security (observed defect or need to improve for target risk level)

GOVERNANCE

Organizations will undertake initiatives in this category due to interpretation of potential fines, legal consequence, business operations or compromised integrity of specific controls. Think of this category as a set of core principles to operate by, some imposed by regulators, while others might be self-imposed (like business continuity).

INFLUENCE ON INITIATIVES

- Regulatory compliance: Varies depending on industry, geography and context of business operations
- Can range from OSHA (safety) to SEC filings, federal and state laws and certifications (SOC 2, etc.)
- Can also be from internal measures (critical controls, deeper prescriptions than compliance requirements)

9.2.3 DISCUSSION: ALIGNING PROJECTS WITH INITIATIVES AND SHAPING WITH CONVERGENCE

To this point, we've discussed how physical security may identify where to find overlap and focus key contributions; however, much of the time to achieve security objectives leaders will need to find a home for capabilities they've already identified and gain support. In this section, let's look at how technology which has been traditionally focused for a single purpose is increasingly being applied to the broader organizational objectives using a convergence model.

IDENTIFICATION

When the pandemic hit, physical security leaders had few tools to provide the level of insight that stakeholders were demanding. Badge swipes weren't reliable enough, some people didn't swipe in, most never swiped out and data at best revealed a user's momentary interaction with the access point but not the rest of their behaviors with the environment between swipes.

Executives needed to know how many people were at a facility, not just a daily count, but at any given time, and in addition, their proximity to one another, or specific assets, and even areas that might not have been set up with traditional badge readers. While improvements in badge technology are often recognized for their security improvement, and mobile credentials are viewed for their convenience, the pandemic revealed how they can play a more strategic role.

MOBILE CREDENTIALS

Mobile credentials might be the ideal example of a technology that can be prepared to serve the demand of convergence. Devices are already in users' hands, and use cases change based on applications installed on them, are portable and have a variety of radios available to use for communication, alerts and geolocation.

Mobile credentials can easily provide the geolocation of people, or more precisely with the addition of beacons to their precise location. Some readers were introduced that also contained a beacon to triangulate users throughout the facility without additional hardware. Some organizations converged capabilities with IT to leverage new frequencies built into their routers that could track users' phones anywhere within the network (as they pass by) to provide broader coverage.

Some organizations discovered that if mobile badges could reveal their specific locations, then the location and distance between two (or more) people could also be known. With the appropriate infrastructure, it could be deduced that two people were in a closer distance to one another that was permitted. The same could be done with specific areas or objects (violated access to specific spaces or were in proximity to specific equipment). The reverse could also be achieved – if someone was more than a certain distance from their chaperone or their authorized work area to identify policy violations.

In addition, at a time when it was undesirable to have users converge on site to sign in, perform enrollment or be issued a badge, mobile credentials can be leveraged to achieve all these aspects remotely. Users can take their own photos and upload them, and administrators can revoke, issue replacements or even modify virtual badges with new capabilities, authentication methods or core identity elements (name or role change, etc.).

SURVEILLANCE

While surveillance gets noticed for becoming ubiquitous with IP and increasingly AI, the real story that's often overlooked is how these serve as a platform for opportunity as well as new challenges which get lesser attention. The days of people watching cameras for what they want to know are fading into the background, while innovative technology performs much of the work that humans can't possibly accomplish. For example, if an organization has 1,000 cameras and only five operators watching them at any given time – well, most aren't being watched.

Surveillance cameras are gaining various sensing capabilities, ranging from thermal to perceive temperature or specific heart signatures to listening for sound, human and object detection. AI can analyze the streams in real time to perceive people, the direction they are heading, different type of objects and the interaction between them, achieving much of the work at scale that humans are often inadequately resourced to do.

IDENTITY IS CRITICAL

In recognizing objects, people and movement, detection is limited without proper context. Machine algorithms need a basis for interpreting inputs, and understanding their relationship is crucial. To identify abnormal behavior, clear definitions of "normal," "acceptable" and "permitted" are essential.

Identity is pivotal. AI can identify a person near a control station, but without information about their role and entitlements, it can't determine if they should be there. Traditional access control systems lack this detail and are becoming outdated. Leveraging possibilities requires understanding a person's identity, the identity of things and their relationship to the organization, all defined by policy.

Advances in identity management platforms, inclusive of physical security (from IT to OT), augment security considerations. For example, an access control system without specialization may evaluate access attempts based on expected authentication, falling short of an executive's broader concerns.

Consider a CFO's responsibility for financial controls. An intelligent identity management system can prevent unauthorized modifications to inventory counts, ensuring proper oversight and audit. Without IT and access control systems being aware of related actions, automated evaluations won't occur.

Contrast two funding proposals for the CFO. One invests in improving physical security systems partnered with IT for identity intelligence, aligning with prioritized financial controls. The other focuses on security improvements but lacks similar outcomes. Convergence of goals and solutions is more likely to gain support.

9.3 RISK: EXPANDED

9.3.1 CORE COMPONENTS OF ESRM

Too large of a topic to cover within a chapter, this section covers the core fundamentals of enterprise security risk management that significantly apply to the physical security industry to consider for adoption to use convergence to achieve greater success.

An ESRM program provides the governance and mechanisms by which participants to engage, perform assessments and executive effective decision making. The framework is defined, documented and structured to facilitate collaboration of

different stakeholders and practitioners across various domains, backgrounds and cultures. Key elements include the following:

ASSET CLASSIFICATION

Beyond the value of the asset, the objective is to understand the critical nature of the asset to the rest of the business and determine impact it would have on adjacent business functions, objectives and consequences.

DEFINED RISK OWNERS

Clear owner of specific risk(s). Since the ESRM endeavors to focus beyond the event itself and its impact on the greater business, it's generally appropriate to designate risk owners to be outside of security and within the affected business function.

COMMON METHODOLOGY

Combined sets of principles, practices and procedures so that all departments, who possess diverse backgrounds and skills, are operating by the same standards concerning risk.

TREATMENTS

In the risk world, the overall remedy to a specific risk which includes proposed changes to operations, procedures, controls and technology to lower the residual risk rating.

STANDARDIZED ACTIONS

There are three choices; address risk, defer it or do nothing.

STANDARDIZED RISK RATINGS

Organizations must be able to summarize risk priorities. A rating system is used the represents a progressive scale which ranges from acceptable risk to those which exceed desired risk. Generally, these are uniquely defined by each organization to consider business climate, context of business objectives and appetite for risk.

For example, it could be a 1 through 5 system, where a level 1 could represent a single event that would impact the organization by $200 million or more in a given quarter. Conversely, a Level 5 might be less than $1 million. In many cases, risks that are convincingly demonstrated to meet Level 1 get fast-tracked, whereas Level 3 might get deferred, while a Level 5 likely won't be addressed.

STANDARDIZED ASSESSMENT SCORING

Assessments are performed at two levels: 1) by specialists to understand the specific mechanisms that comprise of the risk, and 2) the application of ratings in three areas of confidentiality, availability and integrity. Generally, organizations will set tolerances across these three areas.

QUANTIFIABLE METRICS

Risk ratings rely on underlying intelligence about the risk which can be quantified, ultimately producing insights about the measurable impact that doing nothing would have and how this may otherwise look if defied treatments were approved and applied; the latter is referred to as "residual risk." The concept is that most risks can't be entirely eliminated but are lowered to varying degrees, perhaps to acceptable levels.

SHARED RISK REPOSITORY

Shared risk repository means visibility of all risks across departments to facilitate transparency, providing an opportunity for various experts to assess risk and contribute toward proposed treatments. The application can range from a spreadsheet to a dedicated system. Regardless of application, it needs facilitate the documentation of risk elements (owner, ratings, proposed treatments, status, etc.) and be accessible by participants to enter, search and review risks across the organization.

DOCUMENTED DECISION PROCESSES

Organizations need a reliably uniform process by which all participants can apply the same logic to make decisions about risk to avoid departure from core values, lead to inconsistent outcomes and discontent among participants.

RISK LEADERSHIP

Risk is multifaceted, cutting across various business departments, people, operations and skills. It's very difficult for a participant who's already dedicated to a specific business function to identify all the connections that a risk has to other risks, operations or various proposed treatments that are in common with one another.

It's critical that a dedicated risk leadership function exists to ensure that indirect reporting structures adequately participate and make these connections to promote the appropriate focus, context and resources to ensure a high level of competency, consistency and scope across the entire risk portfolio.

OVERSIGHT

Generally performed by committee to facilitate the governance of the program, determine its effectiveness, repudiate practices or adopt new ones.

CLEAR REPORTING STRUCTURE

ESRM reports somewhere high enough to gain support such a model and appropriate visibility so executives can make informed decisions.

SHARED THREAT INTELLIGENCE

Share threat intelligence with one another (and supported processes)

9.3.2 ESRM USE CASE: OT

Operations technology is an area where convergence is becoming commonplace, if not a requirement to solve complex challenges driven by the C-suite. Organizations that have industrial controls systems that are very old (pre-internet) still perform their primary purpose, yet it would be more advantageous (or required) to achieve expanded functionality.

From a business standpoint, there would be greater value to modernize a water treatment plant system where it could be continuously monitored that its pumps are working sufficiently, automate quality testing and apply conditional logic based on results for rapid engagement if protocols need to be initiated (versus manual testing with long gaps between knowing what might be going on across dispersed unmanned stations).

The dilemma for most OT initiatives is to decide between spending massive amounts of money for a new system and "modifying" it at a fraction of the cost to do things that it was never designed to do in the first place. However, older industrial systems weren't designed to perform these modern functions or even be exposed to the internet – and the threats that go along with it. Hence, these considerations are done not in a vacuum specific to function or security, but rather a crossfunctional team of people to devise proposed improvements, assess the risk and determine the feasibility.

- Stakeholders to define the specific outcomes (could be compliance, efficiencies or otherwise)
- Business and process experts to define the functional solution aspects
- OT application users that understand how the OT system is used for situational context

- OT system technology experts familiar with the specific application, code, implementation and its limitations
- Technology domain experts to confer on technical modifications which may be possible
- Security architects to assess overall security topography and potential compliance
- Application and network security engineers to assess attack surface and vulnerabilities
- Privacy, legal and editor reviews for compliance with policies (or consider changes)
- Physical security to review and contribute toward controls objectives to limit people to access or use near vulnerable areas of the system or processes)
- Treatments are defined and documented (proposed improvements)
- Assessments were performed to determine existing and potential security posture (examining potential actors, their motivations, investigating the methods that may be undertaken to closely examine what defensive countermeasures can be applied to result in meaningful controls)
- CRO to review, coordinate and correlate risk elements with other departments, proposed treatments and resources to ensure visibility and optimization
- Quantifiable metrics are derived (cost of improvements and treatment) and define potential impact from risk occurrence
- Residual risk ratings are applied (remaining risk after proposed treatments are applied)
- A risk rating is applied to the residual risk to represent business context and property
- Decision-making methodology is applied, potential impact (define impact before and after treatment)
- Course of action determined

As represented, this type of effort is driven from the top down but ultimately is a risk equation developed by a diverse team and structure to help executives decide if the modified system that may be inferior to that of a brand-new system – but can the risk be kept at a level that is both "acceptable" to the business and adequately managed? The output generated from this process enables executives to calculate a risk versus reward decision in context of the contemporary business environment that they manage.

9.3.3 BEST PRACTICES FOR RISK CONVERGENCE – EXPANDED

For many physical security leaders, engaging with a broader spectrum of people, backgrounds and risks within an ESRM will be quite different for them. It will require considerable application of the core pillars of convergence to be successful in contributing to other stakeholders and in turn gaining support for risks whose desired treatments are closer to the physical security leaders' desired improvements.

KEY TRANSITION AREAS

In the course of practicing convergence successfully, many physical security leaders will need to transition from practices that are deeply embedded across the physical security industry that will prove to be unsuitable within the broader risk community with which they now need to engage.

DISTINGUISH EVENTS AND RISKS

Physical security has generally designed their programs around the desired events to be detected and how to prepare and respond and establish requisite documentation so they can be cited and executed with scale and consistency. These are important aspects when physical security is responsible for many situations where life safety is a pervasive element compared to other risk domains.

Physical security has largely designed risk perspectives around event handling, resulting in documenting them inside standard operating procedures that security operations center (SOC) operators can reliably follow. The SOPs are commonly utilized as the source of risks to be prevented or mitigated.

The industry has generally failed to recognize that risks are caused by events, yet the two aren't synonymous with one another. An event is just an event. Its risk may be high or low. The nature, location, people involved, assets in scope and how critical business functions may be impacted determine the "risk" for that unique circumstance.

Physical security needs consolidate their risks to a central repository where they can be appropriately managed within a risk framework that appropriately considers requisite elements of risk beyond what event management and response can contribute, preferably converging on existing practices that are already employed by the rest of the organization.

ADEQUATE DESIGN OF CONTROLS IMPACTS RESIDUAL RISK

In response to events that are commonly applicable to physical security, the industry has developed generally accepted controls. While these can serve as baseline deterrence measures, they can't be automatically construed as the most appropriate controls without considering the unique threat model associated with a specified risk. Hence, if the quality of a treatment is dependent upon it being purposely devised to reduce a specific risk and is not adequately performed, the residual risk rating is likely to be flawed, thereby impacting the overall risk rating for consideration. This can change the course of conversations, urgency and outcomes regarding proposed initiatives.

Physical security leaders need to consider designing controls in a manner that aligns with the same practices that are undertaken by the rest of the organization who utilizes a risk framework.

QUANTIFIABLE METRICS TO CONVEY IMPACT

A significant part of a risk framework is the ability to make risk-based decisions. The ability to do so relies heavily on having the appropriate information. While the metrics, ratings and treatments are critical components, they must be accompanied by a solid understanding of the impact the risk would precipitate if it wasn't addressed.

Many events associated with physical security are challenging to measure, but it is increasingly possible to apply metrics looking at the same situation from a risk and business perspective. The former provides the context by which the organization wants to understand the impact, and the latter provides the relevance by which to measure it.

For example, life safety is often the most challenging aspect to quantity – placing a value on someone's life is both difficult and undesirable; however, relevant and acceptable metrics can be devised without directly solving the issue proposed. Rather, an employee's contribution toward specific business functions may not be realized, productivity may be lost, and investments may be required to search for a rehire and train them. Some employees may be highly specialized, which depends on the impact and extends the timeline, all of which can be measures in terms of time, cost, and misdirected resource allocation.

Physical security leaders need to find ways to measure identified risks in ways that provide relevant insight so that risks can be fully appreciated within the established decision-making process.

DEALING WITH DECLINED SUPPORT

It's both likely and entirely appropriate that most proposed risk treatments will be declined; however, when executives choose to defer risk, the organization is essentially self-insuring the risk. It's critical that this there exists policy which recognizes that deferral doesn't mean "indefinite."

A generally accepted and effective mechanism within ESRM frameworks to address this is by using a "waiver" process. When risks are declined or deferred, they don't just go away. Rather, policy dictates that a process is automatically employed where risks can only be deferred for a specific period of time and a process for risk owners to revisit decisions that were made. This becomes a very effective tool for security practitioners who are heavy on risks to manage but in short supply of support to address their respective burden. For example, waivers have different lengths depending on criticality; some might be revisited every three months and others annually. In practice, deferring a specific risk a dozen times probably gets noticed by auditors and at some point, either needing better explanation or to be prioritized to be addressed.

In addition, who deferred the risk as well as their reasons become a matter of record. In turn, security leaders can focus on where the organization has agreed to support security initiatives (or inversely directed them).

9.4 GOVERNANCE: EXPANDED

9.4.1 CORE COMPONENTS OF GOVERNANCE AND CONVERGENCE CONSIDERATIONS

PRIVACY

First, privacy and security are intertwined but not the same. Security considers the protection of assets, systems facilities, information and data and the means which an organization undertakes to do so. Privacy on the other hand is about how the organization goes about disclosing, using, sharing and controlling sensitive information.

Usually, privacy is more related to user data. For example, while trade secrets of an organization are confidential, improper disclosure doesn't usually affect the privacy

of a person, their identity or data. Therefore, unless data has some user element, its protected as an asset but might not be subject to privacy. Conversely, those that do may require both to comply with policy that defines how to treat such data and execute security to it remaining private.

CONTEXT FOR PHYSICAL SECURITY PRACTITIONERS
While user data and privacy aren't a new topic for IT, physical security hasn't been subject to the same oversight (regular system and process audits); however, it's an area of increasing concern and complexity for physical security leaders.

As physical security leaders lean in to become more data-driven and develop predictive models, the tools they consider using (AI, machine learning, etc.) require a broader scope of data to process, consider and provide more relevant outputs. Hence, the demand for increased collection of user data can be at odds with regulations, internal policy or current competency levels to adequately secure and maintain its privacy.

Physical security leaders will need to work in unison with compliance, privacy and security stakeholders to ensure that the same policy is being utilized. Some types of data are new considerations that IT never had to deal with (such as surveillance data, physical behavior analysis, physical attributes and object that can infer identity, such as license plates)will require working with the privacy officer and legal counsel to decide the risk of collecting certain information that might not (yet) violate any laws and make addendums to policies.

DATA SECURITY GOVERNANCE
In the past, physical security was used data for functional reasons (to perform badging, enrollment, queries, device events, etc.). As physical security practitioners increasingly rely on data to detect events, rely on the provided context and designate course of action on such basis, low data integrity can undermine this advantage. Consider the scope of the definition of information security, availability, integrity and privacy.

CONTEXT FOR PHYSICAL SECURITY PRACTITIONERS
If the data isn't available, changed or corrupted, then the intelligence apparatus being relied upon can't do its job. If the data is corrupted or modified, then any AI function that relies on this data as input can provide outputs that are inaccurate or even opposite. For example, what if direction and location were key elements of a detection

scenario? If the location data was corrupted or a bad actor modified the telemetry data, the AI would likely product different results (assuming that a would-be threat was in another location or moving away than the defined area or direction that meets the specific criteria).

Little changes can have significant repercussions; therefore, even those physical security practitioners that aren't yet prioritizing cybersecurity measures but have intelligence ambitions should realize that the two are tied together and that convergence measures are the means.

DEVICE MANAGEMENT

Devices need to be managed throughout the entire life cycle, from sourcing (vetting and chain of custody) to decommissioning securely. On the IT side, they generally have reasonably more maturity because they've designed a practice around building it on top of governance, which standardized every step of the device's life cycle.

CONTEXT FOR PHYSICAL SECURITY PRACTITIONERS

Historically, a greater emphasis on managing users rather than devices has persisted in physical security. Conversely, IT has generally accepted and well-defined practices for a broad range of devise to ensure their availability and integrity. Consider that physical security might not be able get firmware version of devise, path it, change cryptographic keys or even have a key management policy contrasted by that of IT that would consider such devices noncompliant and not allow them on their network in the first place.

IT was compelled long ago, but similarly, as their applications became more numerous, network-enabled and connected to many things in and outside the four walls. Devices needed to be trusted and could only be achieved through strong principles, standards and methods. Increasingly, the rest of the organization won't trust physical security devices or the information that they produce or want to be connected to them.

Especially as physical security technology looks more like that of IT, physical security leaders should expect that auditors will increasingly take a closer look at devices and how they are managed (through the lens of the IT ops methodology) and prepare accordingly by using convergence as means to harmonize practice and road map capability.

ASSET MANAGEMENT

Tracking is important for servicing assets efficiently and accurately managing budgets, forecasts and proposals. A big part of this is having visibility into how much such assets have depreciated, accelerated or left. Most IT organizations have defined programs and processes to collect information about all their applications and devices. Generally, they track the location of those IT assets along with who or what is using them, the devices' commission start and end dates, warranty, models, versions, etc.

CONTEXT FOR PHYSICAL SECURITY PRACTITIONERS

Physical security hasn't focused on creating formal and detailed asset management programs that include every system, device and article of equipment. And if they were doing technology asset management, the systems they employed weren't designed for asset management, were siloed from other components and systems and generally fell short of the specific tasks specific to asset management.

In many cases, without clear visibility, finance and auditors will just jointly agree on the life expectancy of an asset which may not be appropriate (much longer) for the type of device, forcing physical security to ponder justifying accelerating depreciation or holding onto noncompliance assets for much longer.

Physical security leaders should consider working jointly with IT, auditors and finance to devise a plan to utilize an existing asset management system or another acceptable means to accomplish objectives.

CONTROLS

Controls are the means of implementing safeguards and countermeasures to carry out what is expected to support desired circumstances. Controls can be designed to manage technical parameters, facilitate process or enforce operating procedures and are a critical component to good governance.

CONTEXT FOR PHYSICAL SECURITY PRACTITIONERS

An example of controls might be the reliance on security guards posted to enforce visitor policies; however, humans can make mistakes. Therefore, in addition to observation, some technical controls are using telemetry-based identity and sensors to track people's movements to interpret whether they are in permitted areas and within the expected range of the sponsor. Alerts can be sent directly to dispatch or the sponsor's manager to act. This is an example of multiple controls working

together to ensure that a consistent result is being achieved and further facilitating actionable operating procedures. Without effective controls, a security program's aspirations can't be realized.

AUDIT

Audit is a validation function of "inspecting what you expect." Audits should endeavor to reflect the scope and expectations defined in the governance program, test controls and inspect environment for nonconformities with defined regular frequency. Without best practice validation, it's likely that various aspects won't be discovered, addressed or improved, which can lead to significant consequences ranging from breaches, shortcomings in preparedness and regulatory infractions.

CONTEXT FOR PHYSICAL SECURITY PRACTITIONERS

Regardless of how well security systems, processes and controls are designed or people are trained and staffed, security needs to know that what's anticipated is actually occurring. Most physical security departments perform visual audits themselves to ensure that the proper equipment, people or procedure is in place. However, they're generally not focused on testing specific controls or with appropriate frequency.

Physical security leaders should partner with IT, InfoSec and the GRC functions to roadmap including physical security with professional audits that concern critical infrastructure and operations (at minimum). In turn physical security should train auditors on the context of physical security risks being managed, key compensating controls and systems functions to enable them to come up to speed conceptually and bring their core competency to bear.

DETECTION

A crucial aspect of a security program is the ability to detect specific events, behaviors and threats. A governance program translates executive management's risk tolerance into specific control measures for alignment. Detection should focus on a) noncompliance with policies or procedures, b) noncompliance of user or device privileges or c) anomalous behaviors by authorized or unauthorized individuals.

Physical security leaders need to shift from merely monitoring events to understanding their context in prioritizing risk, implementing controls and identifying abnormal behaviors. Prioritized risk and controls incorporate defined events, ensuring they are not overlooked but are given meaningful consideration.

This shift requires adopting advanced technologies that move beyond single event detection, utilizing purpose-designed risk equations with multiple inputs. This approach provides security practitioners with insights into risk relevance, root causes and actionable information, requiring fewer resources. Convergence practices should be considered, adopting detection principles from other stakeholders and leveraging their expertise and resources, even if different technologies are used.

Cyber analysts, with their experience in building multiple point reference intelligence models, can be valuable collaborators. This collaboration can result in the sharing of useful data, enhancing the capabilities of both physical security and cybersecurity analysis.

CONTEXT FOR PHYSICAL SECURITY PRACTITIONERS

Physical security leaders should transition away from focusing their detection capabilities solely on event monitoring to those that go further and understand what such events means in context of prioritizing risk, implement controls and anomalous behaviors not considered to be "normal." Note, prioritized risk and controls incorporate defined events and hence aren't overlooked but are accounted for with great meaning.

This will require implementing more advanced technologies which go beyond single event detection and are framed by a purpose-design risk equation of multiple inputs which can provide security practitioners their risk relevance and root cause and lead to more actionable insight with fewer resources. Convergence practices should be considered to undertake similar detection principles as other stakeholders, perhaps even borrowing some of their expertise and resources, even if different technology is used for execution.

Certainly, cybersecurity analysts have significant experience building multiple point reference intelligence models and can be an invaluable resource in this journey, which often leads to a collaboration of useful data that each has that can be valuable to the other.

PRODUCED WITH SUPPORT FROM

Ai-RGUS
NO CAMERA LEFT BEHIND™

Alert Enterprise

Avangrid

safetrust