Report.

DNS Security Survey Report.

Securing DNS is increasingly critical for optimal network security.

Two thirds of survey respondents have experienced some form of attack targeted at or using the domain name system (DNS). This has raised heightened concerns about DNS security but full defensive measures have largely not yet been implemented.

Simply put, the domain name system (DNS) makes the Internet usable for humans. It serves as the critical directory look-up function, translating text web addresses to digital Internet addresses used by our devices to connect to websites, email and other Internet applications.

Organizations publish their web addresses in DNS so people can easily find them. If customers can't reach your website because DNS is down, you could suffer financial, reputational, or other forms of loss. If DNS is inoperable, you are invisible on the web.

Because of its criticality to the Internet, DNS may not only serve as an attack target, it may serve as an attack vehicle, given its necessary permissiveness to flow though firewalls to and from the Internet. Network engineers must take heed to consider DNS vulnerabilities and defensive measures to more completely secure their networks.

Key survey findings include:

- Malware and ransomware attacks were experienced by over half of survey respondents, with some indicating reputation and/or financial loss.
- Besides malware and ransomware infiltration, respondents suffered attacks of DoS/DDoS, reflected DDoS, domain hijacking and DNS cache poisoning.
- Every survey respondent indicated at least moderate concern about DNS security, with sixty-one percent expressing moderate concern and thirty-nine percent, huge concern.
- Over fifty percent of respondents have fully implemented basic DNS security controls such as DDoS protections, access control lists (ACLs), query monitoring and role based deployment.
- DNS security extensions (DNSSEC) deployments lag other security measures in terms of implementations with less than sixteen percent of respondents having fully deployed.
- Forty-seven percent of respondents agree or strongly agree with the statement, "I fully understand how DNSSEC functions" while fifty-three percent felt the same about DNS firewall functions.

BT

Introduction

During the autumn of 2017, BT Diamond IP conducted an industry survey regarding DNS security. DNS is a critical ingredient in operating and managing an IP network, not to mention in simplifying user navigation. For these reasons, and due to a rise in diversifying attack vectors that use DNS, network engineers are seeking strategies for securing DNS to more tightly monitor and secure their networks.

To help assess the status of DNS security concern and mitigation strategies, BT Diamond IP recently conducted a web-based DNS security survey. The survey was posted online, and invitations to participate were posted on social media and sent to individuals identified as IT and Operations professionals.

All survey responses were automatically tabulated into the Survey Monkey tool. Any individual skipped questions were not included in tabulations. Percentages shown in charts may not equal 100 percent due to rounding or to questions enabling multiple answers. This document summarizes key findings from our survey.

Given the relative complexity of DNS security technology, survey participants were provided a link to a free DNS Security Strategies whitepaper, which summarized major DNS vulnerabilities and mitigation strategies. For access to this white paper and for more information about DNS security, please consult the *Additional Resources* section at the end of this document.

Level of Concern about DNS security

The level of concern about DNS security was moderate-to-high as indicated in Figure 1. About 39% indicated huge concern while 61% stated they felt moderate concern in this year's survey. Surprisingly, none of the respondents indicated "low concern."

While most security topics generally garner moderate levels of concern, many so-called "ancillary" security threats are more uniformly distributed. Clearly among IT professionals, DNS security is no longer ancillary but mainstream.

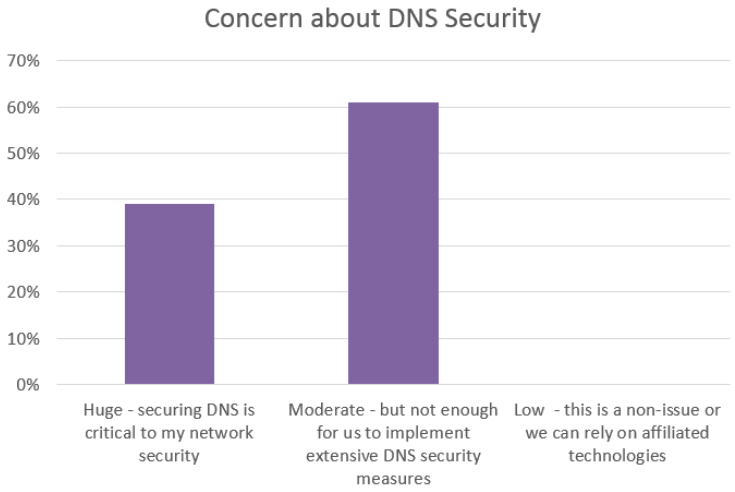

Figure 1: Level of concern regarding DNS security

"I find it really strange that these folk have invested time, money and attention in their web presence, and kind of go, 'Ah the DNS, that's just rubbish.' It's not. DNS is everything. Failing to secure DNS is savage ignorance."

Geoff Huston

APNIC Chief Scientist

http://www.zdnet.com/article/failing-to-secure-dns-is-savage-ignorance-geoff-huston/

DNS Attacks

Figure 2 illustrates the types of attacks that those participating in the survey had experienced over the prior twelve months. Over half of all survey respondents had experienced a malware or ransomware attack, with ten percent of these indicating some financial loss to individuals or the organization. While not all malware and ransomware use DNS, over 90% of malware does use DNS to make contact with the malware author's command and control (C&C) center over the Internet, according to a 2016 Cisco security report†. In this manner, malware installed on infected devices can receive attack instructions, download malware updates, and export sensitive information gathered by the malware. Hence monitoring DNS and firewalling DNS responses can lead to detection and prevention of malware or ransomware activities and proliferation.

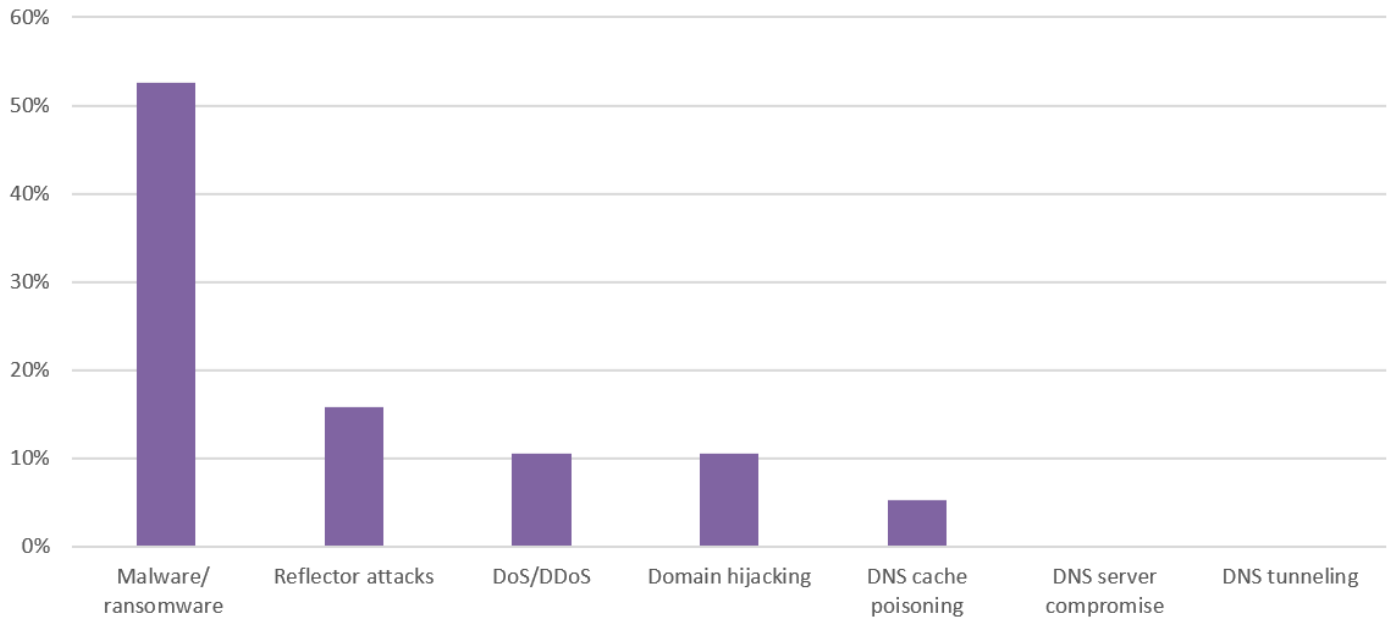

Figure 2: Attacks experienced by survey participants

At eighteen percent, coming in second among attack types, reflector attacks are a form of denial of service (DoS) attack whereby the attacker issues a large quantity of DNS queries using the attack target's IP address as the source IP address of each query. In this way, DNS responses are directed back to the "querier," in this case the attack target's IP address. The attacker may issue large numbers of queries using this tactic to multiple DNS servers and use queries with large answer payloads such as "ANY" or DNSSEC queries to further amplify the attack.

Non-reflector DoS/DDoS attacks came in at eleven percent, tied with domain hijacking. Domain hijacking is an attack that redirects those querying for your domain to an attacker server for resolution. This form of attack may entail infiltrating your DNS servers or your parent zone registrar's DNS servers and can result in unwitting users being

† Cisco Security Report, https://umbrella.cisco.com/blog/2016/01/21/cisco-security-report-more-orgs-should-be-monitoring-dns

redirected to an attacker website posing as your own to gather credentials or other sensitive information.

About five percent of respondents had suffered a DNS cache poisoning attack over the past twelve months. Cache poisoning can occur when an attacker answers a query for a given destination before the “real” or authoritative server responds. It’s not quite that trivial to poison a DNS server cache as other parameters in the response must complement the query, but this attack can likewise hijack unsuspecting users to imposter websites. DNS security extensions (DNSSEC) is the definitive solution to this type of attack.

Interestingly, no survey participants had suffered a DNS server compromise or DNS tunnelling attack. A successful server compromise attack certainly poses a threat not only to the DNS server and its integrity but could also serve as a launch point for other attacks within the organization. DNS tunnelling can be used to export information using the DNS protocol. Since DNS traffic is typically permitted uninhibited through firewalls, attackers find it a convenient transport protocol to exfiltrate information. Many tunnelling techniques have been devised in terms of encoding traffic into what looks like DNS queries and answers, though none of our survey respondents have observed this.

DNS Security Implementations

We asked participants about their implementation status for several DNS security techniques. Due to the diversity of attack vectors against DNS and against other network and computing elements that use DNS, a variety of strategies are required to defend effectively. Many of these strategies also facilitate a defense-in-depth approach when used with other DNS and general network security tactics.

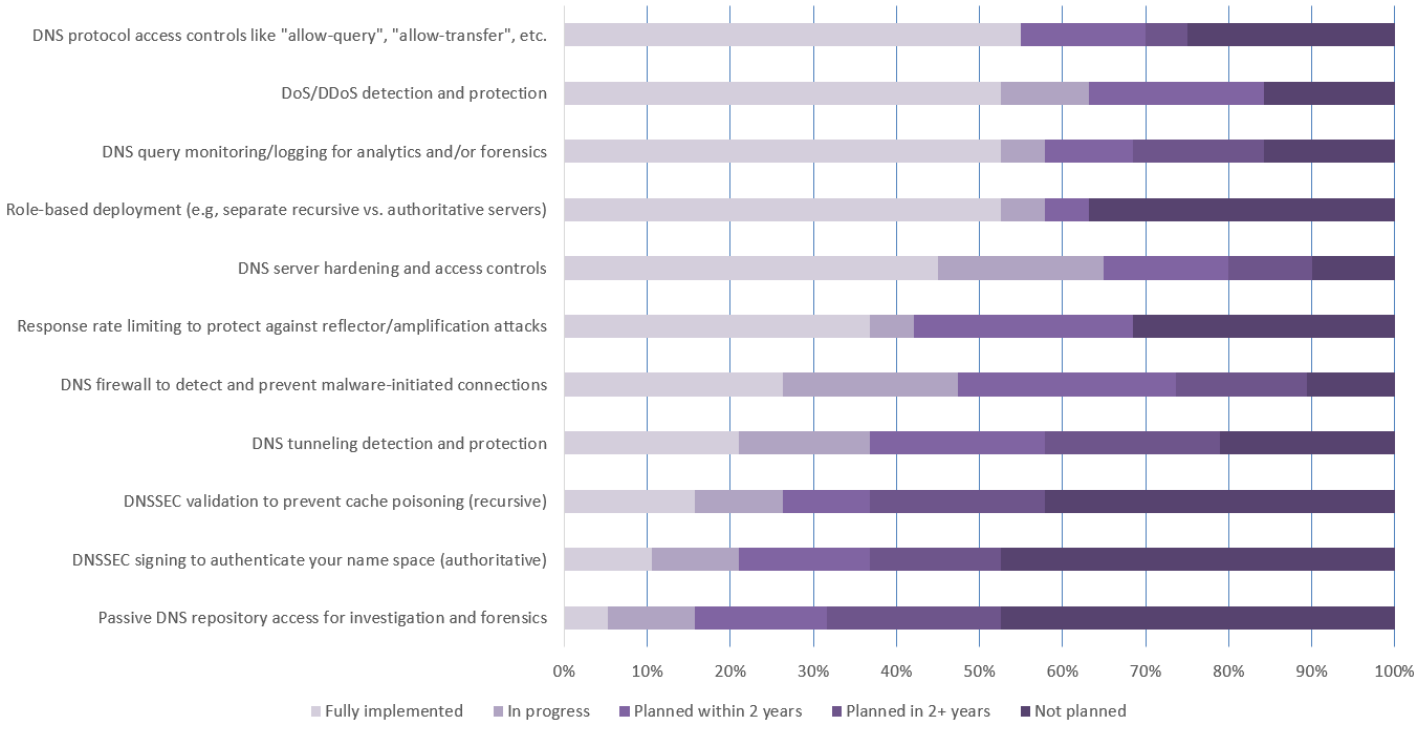

Figure 3: DNS security implementation status

Figure 3 illustrates the status of DNS security deployments, listed by those most fully implemented. Over half of respondents have fully implemented the basic security measures of access control lists (ACLs), DoS/DDoS protections, query monitoring and forensics capabilities and role-based deployment to contain the breadth of an infiltration. DNS server hardening has been implemented by nearly half of survey respondents, though eighty percent plan to implement within two years. About two-thirds of respondents plan to implement response-rate limiting within two years, with over one-third having fully implemented this already. Response-rate limiting can cut down on the impact of reflector attacks by throttling query responses from common IP addresses.

A little over one quarter of respondents have fully implemented DNS firewall functionality, which is an effective approach to detecting and blocking malware attempts to contact C&C centers. DNS firewall policies enable the enforcement of policies to block such queries or to redirect query answers to connect the device to a mitigation portal for remediation. Nearly 75% of respondents plan to implement a DNS firewall solution within two years, which should help in defending against this most prevalent form of DNS attack.

Just over twenty percent of respondents have fully implemented controls for DNS tunnelling, with just over half planning to implement within two years.

The next pair of responses indicate that less than forty percent of respondents plan to support DNS security extensions, DNSSEC, within two years. In fact, over forty percent have no plans at all to implement DNSSEC. DNSSEC supports digital signatures on DNS resolutions, enabling users to authenticate such responses, vastly diminishing the likelihood of possible domain hijacking via cache poisoning. While early implementations of DNSSEC were complex to initialize and maintain, many open source and commercial products automate most or all of the cryptographic setup and maintenance these days. To understand this possible outdated perception, we delved more deeply into DNSSEC as we'll discuss in the next section.

About six percent of respondents utilize a passive DNS service to assist with forensics and diagnoses. A passive DNS service enables one to query the history of a domain for example, in terms of the IP addresses it resolved to in the past, when it was first seen on the Internet, what subdomain exist and so on. This and related history information can provide insight regarding the possible nefarious use of given domains observed in queries on your network.

DNSSEC Opinions

Given the relatively meager deployment of DNSSEC at less than 20% worldwide, we asked survey participants about their opinions about DNSSEC and whether the perception exists that DNSSEC is too complex. Responses are summarized in Figure 4. The top two responses in the chart, ordered by percentage strongly agreeing, indicate a strong recognition of the value of DNSSEC. DNSSEC validation is a function of your recursive/caching servers which issue queries to Internet DNS servers to resolve domain names and in the case of DNSSEC-signed responses, validate the responses. DNSSEC signing is the cryptographic signing of your domain names in your DNS servers which other Internet users may query to locate your web and email servers, etc. and to validate if signed. Over two-thirds of respondents agreed or strongly agreed that DNSSEC can protect name resolution.

Jumping to the bottom of the chart, we readily recognize the cause of the inertia in failing to deploy DNSSEC. Less than twenty percent of respondents agreed or strongly agreed that DNSSEC signing or validation is easy to maintain. This perceived burden is the major obstacle to DNSSEC deployment. In reality, DNSSEC is relatively easy to configure and manage with recent vintage open source and commercial products as mentioned previously. But part of the issue is a chicken-and-the-egg problem where configuring DNSSEC validation does little if few zones are signed and configuring DNSSEC signing does little if few resolvers validate. Nevertheless, the manageable incremental effort to configure DNSSEC would seem worthwhile for those seeking secure resolutions to authenticate resolutions and validate the absence of man-in-the-middle manipulation of resolution data.

We asked plainly if participants fully understood how DNSSEC works. The answer to this question yielded a near uniform response equally for each choice, illustrating a lack of consensus, though favoring the affirmative.

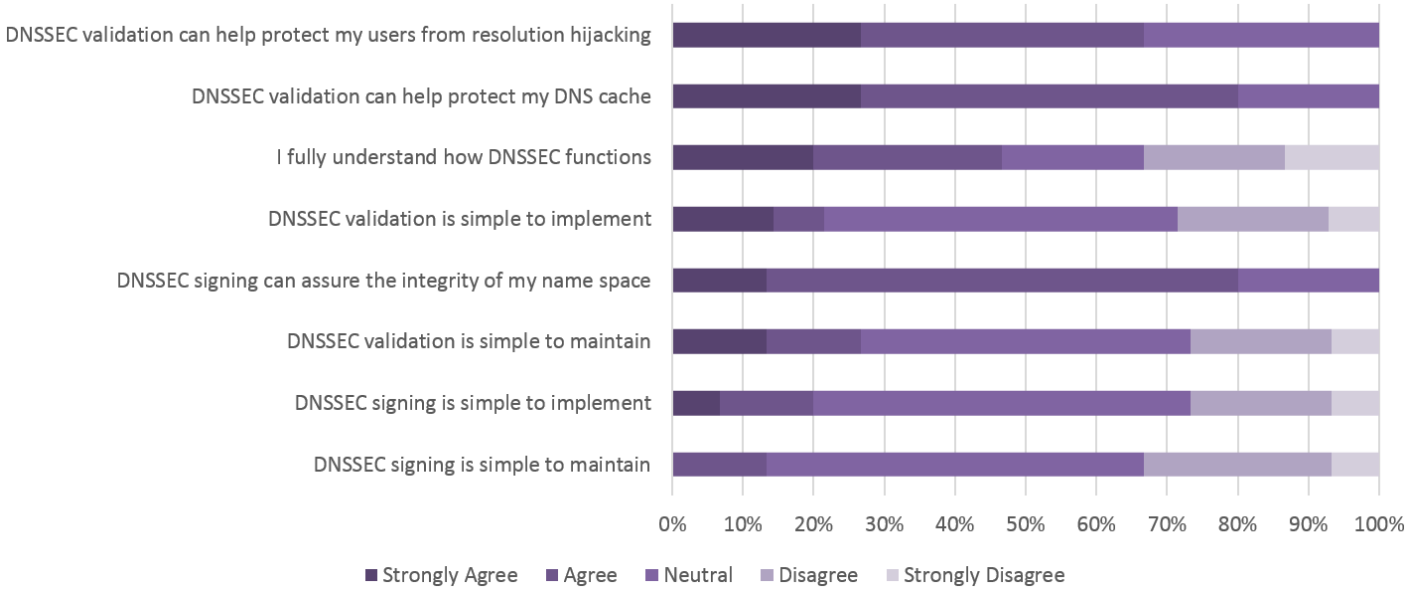

Figure 4: DNSSEC opinions

DNS Firewall Opinions

DNS firewall technology was first devised by the Internet Systems Consortium (ISC) and first implemented in its open source BIND DNS software in 2010. A DNS firewall examines DNS query responses and enables the administrator to define triggers for which corresponding response policies may be applied. Configured on a regular DNS server as response policy zones (RPZs), this functionality enables the identification of a potentially malware-infected device by virtue of its DNS queries.

Queries to known or suspicious malware domains or to authoritative DNS servers of questionable reputation based on the domain operator, IP address space, or other criteria can be used to define response policies. A policy may be triggered based on a variety of criteria in the DNS response and may amount to dropping, redirecting or passing through the query response to the querying client. DNS firewall technology adds a defensive layer to outbound

communications from within an organization with DNS queries generally preceding direct IP network connections and thus complements in-band defensive measures such as those implemented in network firewalls.

We asked survey participants similar questions as we did regarding DNSSEC, and responses are summarized in Figure 5. While most respondents confidently confessed to understanding of how DNS firewalls function, the majority were less confident regarding operational issues of implementation, configuration, and maintenance in responding as neutral to such questions. Nevertheless, no respondents disagreed that DNS firewalls are simple to implement or maintain.

Implementation and maintenance complexity in fact depends on one's approach. One may configure one's own policies, individually identifying suspicious domains and implementing corresponding policies, and/or one may subscribe to a free or commercial DNS firewall feed to automate the updating of DNS firewall policies several times a day. A hybrid approach using both techniques is also possible. Regarding the use of a firewall subscription, two-thirds of respondents were neutral about relying solely on a third party firewall feed and regarding the ability to customize feeds.

Two thirds of respondents agreed or strongly agreed that DNS firewalls can help identify the presence of malware and can protect users from malware. No one agreed with the statement that a DNS firewall is not needed if a network firewall is deployed, confirming agreement with our earlier suggestion that DNS firewalls complement network firewalls.

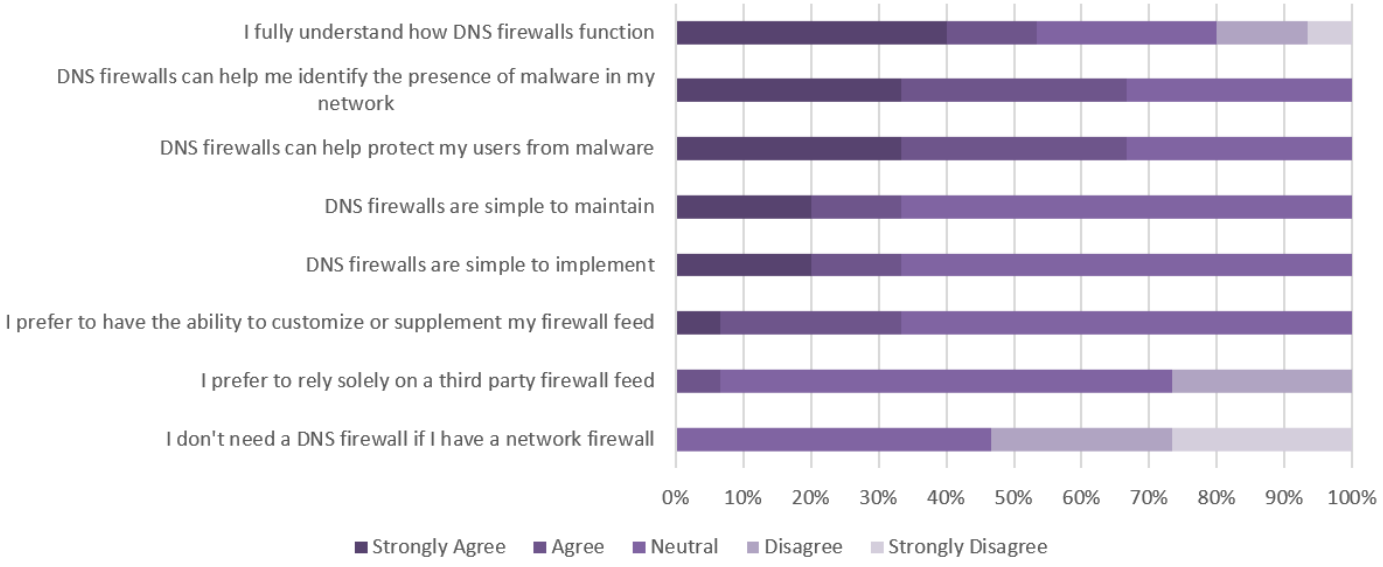

Figure 5: DNS Firewall Opinions

Survey Demographics

Figure 6 illustrates key demographics for respondents from this survey. The types of organizations from which respondents hailed included a roughly equal distribution of multinational and regional enterprises, educational institutions and "other" which includes governments, consultancies and small enterprises. About seven percent of respondents work at a service provider. In terms of network size managed by respondents, nearly half support networks of up to ten thousand IP addresses, while one quarter manage between ten and one hundred thousand. Twenty percent managed up to one million addresses and seven percent over one million.

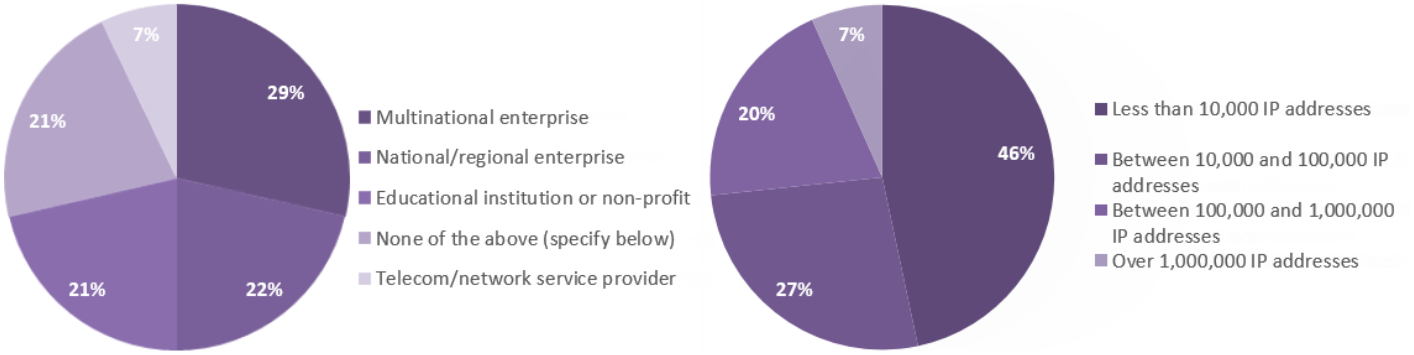

Figure 6: Survey participants' organization type (left) and network size (right)

Conclusions

IT and operations engineers and managers are concerned about DNS security. They realize the vulnerabilities that DNS presents both as a critical network service and as a requisite network protocol requiring open transport throughout their networks and through network firewalls. Despite this recognition, implementation of DNS security measures is modest. Basic controls have largely been implemented by the majority, though preferably all would take such measures. Other more sophisticated controls such as DNS firewalls and DNSSEC have yet to be largely implemented by most despite acknowledged value in securing networks. Perceptions of complexity for DNSSEC and uncertainly regarding DNS firewall configuration and maintenance have inhibited enthusiastic deployment as yet. Please refer to the resources below to learn more and to allay these concerns.

Additional Resources

If you're wondering how to get started with securing your DNS or if you'd like to learn more about DNS security, here are a few resources for more information to get you started.

- http://www.bt.com/diamondip - BT's Diamond IP main page summarizing BT's IPAM, DHCP and DNS, including DNS security products and services.
- http://www.globalservices.bt.com/uk/en/products/diamondip/whitepapers – Free white papers for download including *Protect Against Malware with DNS Firewalls*, *DNS Security Strategies*, *Securing Name Resolution with DNSSEC* and more.
- https://www.internetsociety.org/deploy360/dnssec/ - Internet Society DNSSEC resources including overviews, case studies, training and white papers.
- DNS Security Management book by BT Diamond IP authors, published by Wiley IEEE Press, September, 2017.

Find out more at:

+1 610 321 9000 www.bt.com/diamondip