CYBEREDGE GROUP

2015 CYBERTHREAT DEFENSE REPORT

NORTH AMERICA & EUROPE

<< Research Sponsors >>

Platinum sponsors:

BLUE COAT CITRIX®

Gold sponsors:

NetIQ PHISHME tenable network security ThreatTrack SECURITY WEBROOT®

Silver sponsors:

CloudLock CYLANCE

ENDGAME. iSIGHTPARTNERS TRIUMFANT

Table of Contents

Introduction

Survey Demographics

- 814 qualified IT security decision makers and practitioners
- All from organizations with more than 500 employees
- Representing 7 countries in North America and Europe
- Representing 19 industries

Published in 2014, the inaugural Cyberthreat Defense Report began the process of looking beyond headline-grabbing breaches and the nth stage in the evolution of cyberthreats to better understand the perceptions, concerns, and priorities of the IT security professionals charged with defending today's networks. Representative findings from that first report included the revelation that one in four security professionals doubts whether their organization has invested adequately in cyberthreat defenses, the identification of mobile devices as IT security's "weakest link," and the expectation that more than three-quarters of businesses will adopt bring-your-own-device (BYOD) policies by 2016.

The second annual Cyberthreat Defense Report continues this process of striving to inform the IT security community, not about the latest and greatest "baddies" to emerge on the scene, but rather how their peers are electing to defend against them. Based on a rigorous survey of IT security decision makers and practitioners across North America and Europe, the Cyberthreat Defense Report examines the current and planned deployment of countermeasures against the backdrop of numerous perceptions, such as:

☑ The adequacy of existing cybersecurity investments, overall and within specific domains of IT

☑ The likelihood of being compromised by a successful cyberattack within the next 12 months

☑ The types of cyberthreats that pose the greatest risk to a given organization

☑ The organizational factors that represent the most significant barriers to establishing effective cyberthreat defenses

☑ The impact that software-defined networking (SDN) may have on an organization's ability to defend against cyberthreats

By revealing these details we hope to provide IT security decision makers with a better understanding of how their perceptions, concerns, priorities, and – most importantly – current defensive postures stack up against those of other IT security professionals and organizations. Applied in a constructive manner, the data, analyses, and findings that are covered can be used by diligent IT security teams to gain insights into many practical questions, such as:

- ☑ Where do we have gaps in our cyberthreat defenses relative to other organizations?
- ☑ Have we fallen behind in our defensive strategy to the point where our organization is now the "low-hanging fruit" (i.e., likely to be targeted more often due to its relative defensive weaknesses)?
- ☑ Are we on track with both our approach and progress in continuing to address traditional areas of concern – such as strengthening endpoint security and reducing our attack surface – as well as tackling newer ones, such as providing security for mobility and defending against advanced persistent threats (APTs)?
- ☑ How are other IT security practitioners thinking differently about cyberthreats and their defenses, and should we adjust our perspective and plans to account for these differences?

A second objective is to provide developers of IT security technologies and products with some of the answers they need to better align their solutions with the concerns and requirements of their potential customers. The net result should be better market traction and success for solution providers that are paying attention, and better cyberthreat protection technologies for all of the intrepid defenders out there.

cy•ber•threat
/ˈsībərˌTHret/

noun

1. the possibility of a malicious attempt to damage or disrupt a computer network or system (source: Oxford Dictionaries)

2. any type of malicious activity or actor that leverages computers and networks to adversely impact other computers and networks, to include everything from well-known forms of malware (e.g., viruses, worms, and Trojans) to malicious insiders and targeted attacks (source: CyberEdge Group)

Research Highlights

Current Security Posture

- ☑ 70% of respondents are spending greater than 5% of their IT budgets on security. *(Pages 6-7)*
- ☑ 71% were affected by a successful cyberattack in 2014, but only 52% expect to fall victim again in 2015. *(Pages 7-9)*
- ☑ For the second consecutive year, mobile devices (smartphones and tablets) are perceived as IT security's weakest link, closely followed by social media applications. *(Pages 9-10)*
- ☑ Security analytics is the top-ranked network security technology planned for acquisition in 2015, followed by threat intelligence and next-generation firewalls. *(Pages 11-12)*
- ☑ Nearly a third lack tools to inspect SSL-encrypted traffic for cyberthreats. *(Pages 12-13)*
- ☑ Containerization/micro-virtualization technology is the top-ranked endpoint security and second-ranked mobile security technology planned for acquisition in 2015. *(Pages 13-15)*
- ☑ Only 23% of respondents are confident their organizations have made adequate investments to monitor the activities of privileged users. *(Pages 15-16)*

Perceptions and Concerns

- ☑ Phishing, malware, and zero-days give IT security the most headaches. *(Pages 17-18)*
- ☑ 59% of respondents experienced an increase in mobile threats over the past year. *(Pages 18-19)*
- ☑ Inadvertent exposure of confidential data is the top concern with SaaS-based file sharing applications. *(Pages 19-20)*
- ☑ Low security awareness among employees continues to be the greatest inhibitor to defending against cyberthreats, followed closely by lack of security budget. (*Page 22*)
- ☑ Nearly two-thirds of security professionals view SDN as having a positive impact on their ability to defend against cyberthreats. *(Page 23)*

Attack Surface Reduction

- ☑ Network access control (NAC) remains the top technology for reducing a network's attack surface. *(Pages 24-25)*
- ☑ Less than 40% of organizations conduct full-network active vulnerability scans more than once per quarter. *(Pages 25-26)*
- ☑ Only 20% of IT security professionals are confident their organizations have made adequate investments in educating users on how to avoid phishing attacks. *(Pages 27-28)*

Future Plans

- ☑ 62% of IT security budgets are expected to rise in 2015. *(Pages 30-31)*
- ☑ Although BYOD initiatives stalled in 2014, they are expected to nearly double in the coming year—from 30% to 59% of organizations. *(Pages 31-33)*
- ☑ More than two-thirds are looking to replace or augment current endpoint protection tools. *(Pages 33-34)*

Section 1: Current Security Posture

The security foundation an organization already has in place and the perception of how well it is working will influence major decisions about cyberthreat defenses going forward, such as:

☑ Whether, to what extent, and with what degree of urgency changes are needed; and

☑ The most likely candidates to enable those changes (i.e., the specific types of countermeasures that should be added to supplement existing defenses).

Our journey into the depths of cyberthreat defenses begins, therefore, with an assessment of the perceived effectiveness of organizations' investments and strategies relative to the prevailing threat landscape. Insight is also provided on the high-level definition of these strategies based on the technological countermeasures they incorporate.

Cut to the Chase

- 70% of represented organizations are allocating more than 5% of their IT budget to information security
- While 52% of European organizations are allocating more than 10% to security, the same is true for only 35% of North American respondents

IT Security Budget Allocation

Overall, spending on information security products, services, and personnel appears relatively healthy (see Figure 1). Only 9% of respondents indicated their organizations are spending 2% or less of the IT budget on security, while a full 70% signaled an investment level in excess of 5%. A remarkable 21% even claimed to be spending more than 15% of their IT budgets on security.

At first blush, these high spending levels might seem entirely unbelievable – particularly if you were in the security industry 10 to 15 years ago, when allocating 1% to 2%of the IT budget to security was the norm. However, it's precisely this historical under-investing – combined with the board-level attention that infosec now enjoys – which makes the current spending levels not only plausible, but actually necessary and appropriate.

Interestingly, the current data also revealed that European organizations are investing more heavily in information security than those based in North America. While 52% of the European survey population indicated spending more than 10% of their IT budget on security, the same was true for only 35% of North American respondents.

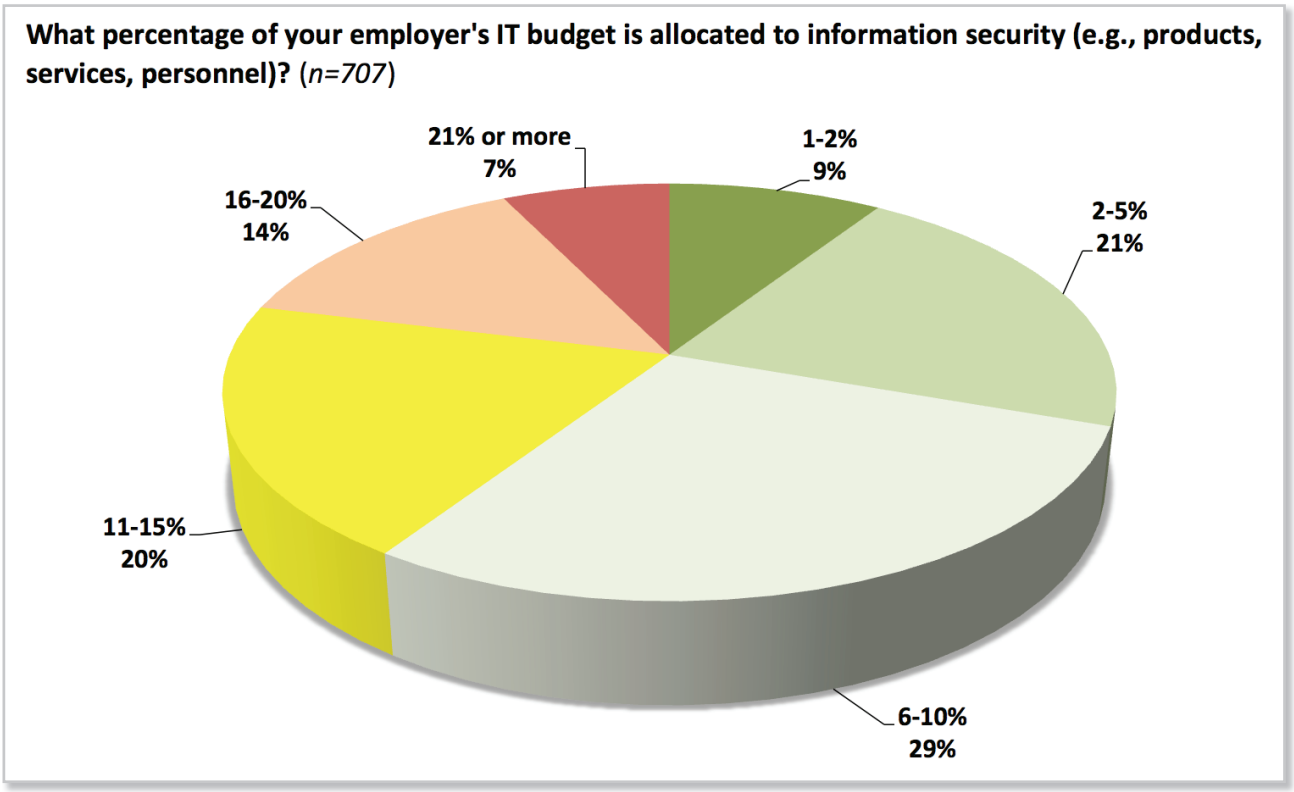

Figure 1: Percentage of IT budget allocated to security

Cut to the Chase

- 71% of represented organizations experienced at least one successful cyberattack in the preceding 12 months (up from 62% the year prior)
- 7% claim they've been successfully breached 10 or more times (unchanged from a year prior)

Past Frequency of Successful Cyberattacks

The need for continued, significant investments in information security is validated by our next set of findings.

In particular, the past 12-month period has seen more than 7 out of 10 respondents' organizations being the subject of a successful cyberattack. This is up from just under 6 of 10 for the respondents polled in last year's survey (see Figure 2).

Other notable findings:

☑ A 67% increase in the percentage of respondent organizations experiencing between 6 and 10 cyberattacks over the past 12-month period; and

☑ No change in the percentage of respondent organizations that were breached more than 10 times in the past year (7%).

From a regional perspective, one significant difference to highlight is that while 35% of North American organizations claimed they did not experience a successful cyberattack over the past year, the same was true for only 20% of European organizations.

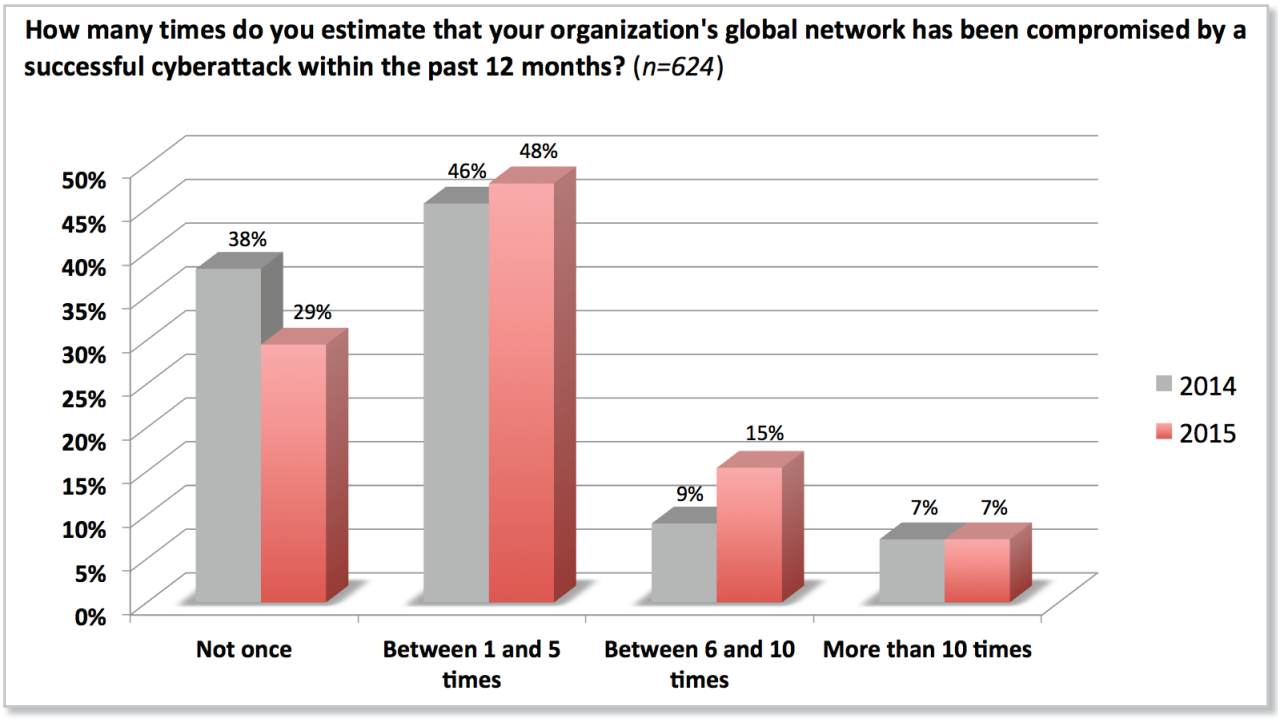

Figure 2: Frequency of successful attacks in the past 12 months

Future Likelihood of Successful Cyberattacks

When asked about the likelihood their organization's network would be compromised in the coming year, respondents were, once again, more optimistic than we would have expected. Despite more than 70% indicating they thought their organization's computing environment had been compromised within the past year (see Figure 2), only 52% considered it "somewhat likely" or "very likely" that it would happen again over the next 12 months (see Figure 3). Respondents do appear to be "waking up" a bit to the realities of the modern threat environment, however, as the 2014 result had only 39% considering it likely their organizations would be compromised in the coming year.

Overall, Europeans (58%) are slightly more pessimistic (or, perhaps "realistic") than their North American counterparts (49%) regarding the likelihood of their respective organization being successfully attacked in the coming year.

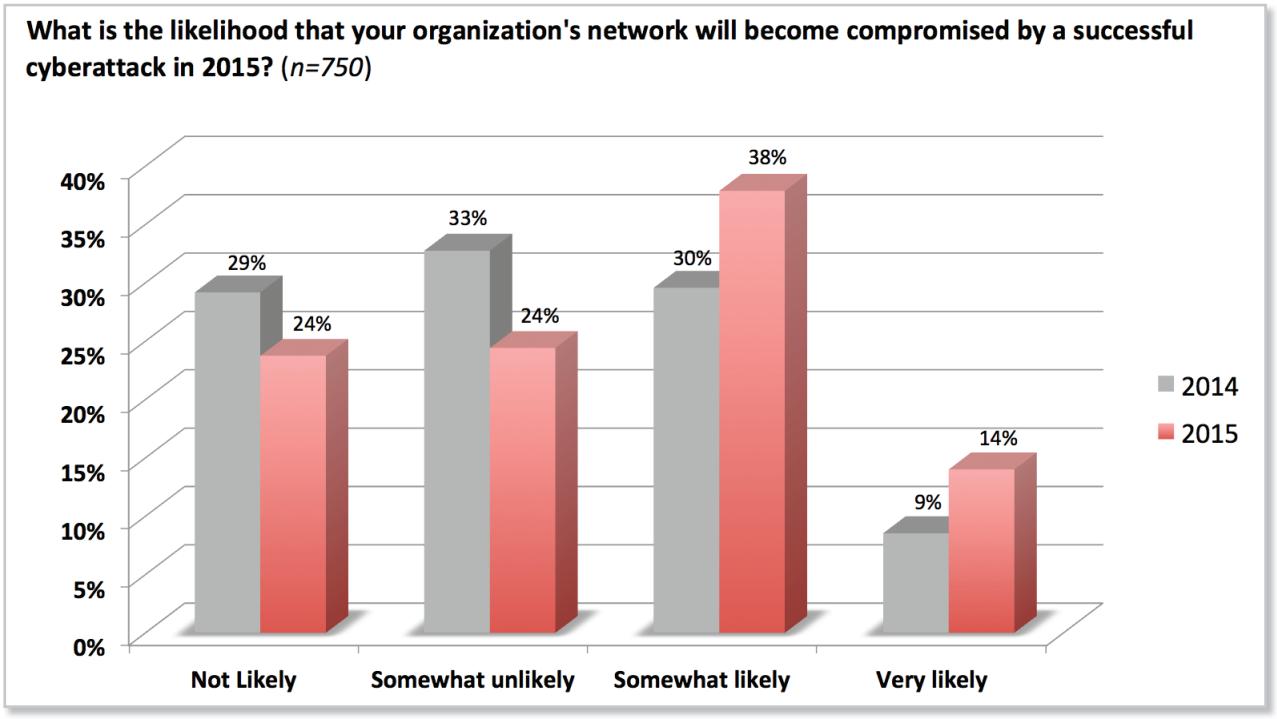

Figure 3: Likelihood of being successfully attacked in the next 12 months

Security Posture by IT Domain

Data on the perceived ability to defend against cyberthreats in different IT domains (see Figure 4) starts to shed some light on potential areas for future spending on security technology and services.

"Client devices of all types – but especially mobile devices – present the greatest security challenge to organizations."

While respondents expressed relatively high confidence in their defenses for both physical and virtual servers, client devices of all types – but especially mobile devices – were found to present the greatest security challenge to today's organizations. This finding makes perfectly good sense to us, at least from the perspective that you'd expect IT to be better at securing resources over which it has greater control (e.g., servers) compared to those that it does not (e.g., mobile devices).

As to why respondents should have the same degree of confidence defending virtual servers as they do physical servers, we can only conclude: (a) that to a large extent "a server is a server," and (b) that any experiential difference protecting virtualized infrastructure is offset by the relative ease with which countermeasures can be programmatically implemented for virtual systems compared to physical ones.

Additional findings of interest:

☑ Establishing adequate protection for/from social media applications such as Facebook and Twitter remains a relative weak spot in organizations' defenses;

☑ There is no significant difference in the perceived security posture for homegrown web applications compared to cloud-sourced applications (SaaS); and,

☑ Similarly, there is negligible perceived difference in the ability of respondents' organizations to protect different flavors of cloud services (i.e., IaaS/PaaS vs. SaaS).

From top to bottom, the findings were nearly identical to those from last year's report.

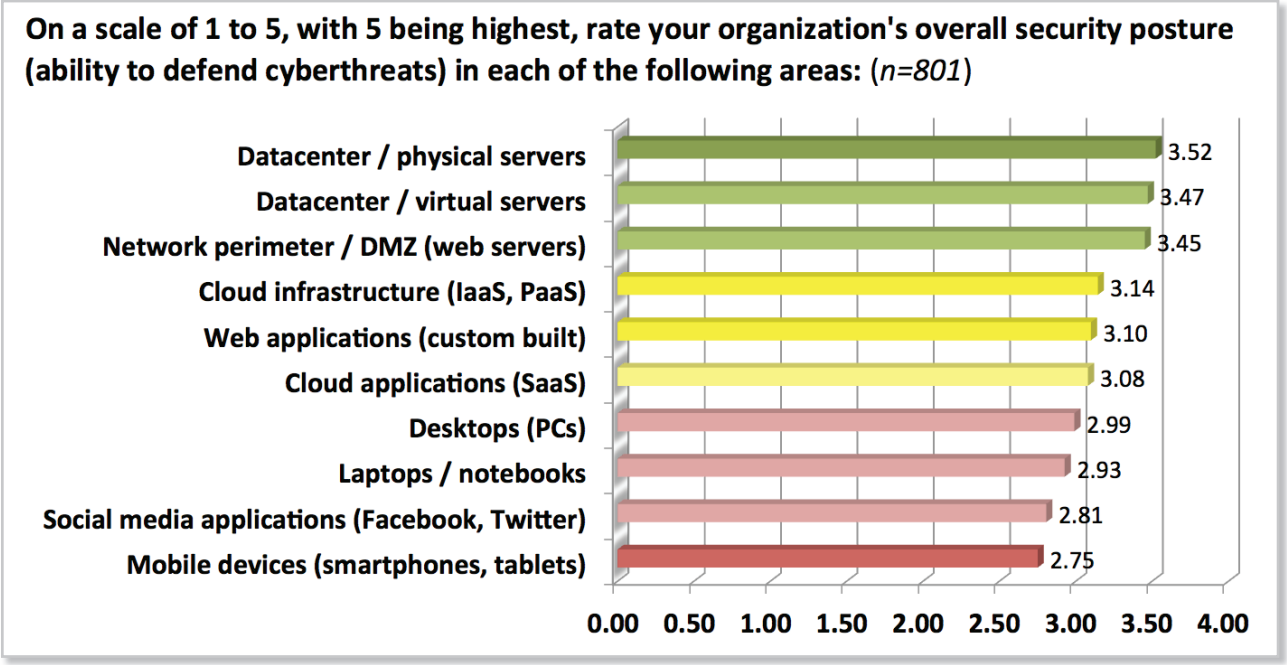

Figure 4: Perceived security posture by IT domain

"Security analytics, equipped with full-packet capture and analysis capabilities, is the top-rated network security technology planned for acquisition in 2015."

"The use of a dedicated threat intelligence service to reinforce existing defenses and better plan future security strategies and investments is rapidly reaching mainstream status."

Network Security Technology Deployment Status

Participants were requested to designate a deployment status – currently in use, planned for acquisition within 12 months, or no plans – for a specified list of network security technologies. (Endpoint and mobile security technologies are addressed in a subsequent section.)

Table 1 provides a visual and numerical representation of the responses. Percentages in green correspond to higher frequency of adoption and/or acquisition plans. Percentages in red correspond to lower adoption and/or acquisition plans.

Notable findings:

- ☑ Network AV, IDS/IPS, and secure email gateways are the most frequently deployed defenses (and, not surprisingly, have the least capacity for growth).
- ☑ Security analytics, equipped with full-packet capture and analysis capabilities, is the top-rated network security technology planned for acquisition in 2015.
- ☑ NGFWs are also earmarked as a top candidate for investment over the coming year (nearly matching their first place designation from last year).
- ☑ The use of a dedicated threat intelligence service to reinforce existing defenses and better plan future security strategies and investments is rapidly reaching mainstream status, with 32% signaling intent to adopt such a solution in 2015.
- ☑ With security analytics, network behavior analysis (NBA), and security information and event management (SIEM) all near the top of the leader board for the coming year, it seems clear that many organizations are continuing, as they did last year, to beef up their capabilities for monitoring and analyzing network traffic for the presence of cyberthreats.

Our closing thought for this table is that we are a bit surprised to see only a ~50% adoption rate for both web application firewalls (WAFs) and advanced malware analysis technology. Given the prevailing conditions over the past several years – namely the shift to targeted application-layer attacks and steady rise of APTs – we expected adoption rates would be higher for both of these essential defenses.

Which of the following network security technologies are currently in use or planned for acquisition (within 12 months) by your organization to guard all network assets against cyberthreats? (*n=810*)

	Currently in use	Planned for acquisition	No plans
Network-based anti-virus (AV)	76%	16%	8%
Intrusion detection / prevention system (IDS/IPS)	69%	22%	9%
Secure email gateway (SEG)	69%	18%	13%
Secure web gateway (SWG)	63%	22%	15%
Denial of service (DoS) / distributed denial of service (DDoS)	59%	22%	19%
Security information and event management (SIEM)	56%	26%	18%
Next-generation firewall (NGFW)	54%	32%	15%
Web application firewall (WAF)	54%	28%	17%
Advanced malware analysis / sandboxing	53%	27%	21%
Data loss/leak prevention (DLP)	51%	31%	18%
Network behavior analysis (NBA) / NetFlow analysis	47%	30%	22%
Security analytics / full-packet capture and analysis	45%	33%	22%
Threat intelligence service	43%	32%	25%

<-- Less Frequency ---------- More Frequency -->

Table 1: Network security technologies in use and planned for acquisition

Inspection Capabilities for SSL-encrypted Traffic

Participants were asked to indicate whether their organizations have the necessary tools to inspect SSL-encrypted traffic for cyberthreats (see Figure 5).

"Nearly one-third of our respondents were unconvinced that they have the necessary tools at their disposal to adequately inspect SSL-encrypted traffic."

Although the majority (68%) expressed a measure of confidence in this regard, nearly one-third of our respondents were unconvinced that they have the necessary tools at their disposal to adequately inspect SSL-encrypted traffic. This figure is a cause for concern, at least to us. In an age of network communications where SSL/TLS encryption has become standard fare, the inability to decrypt and analyze traffic for threats "coming along for the ride" – or data on its way out the door – leaves a gaping hole in one's defenses.

No statistically significant differences were observed by region (i.e., North America vs. Europe).

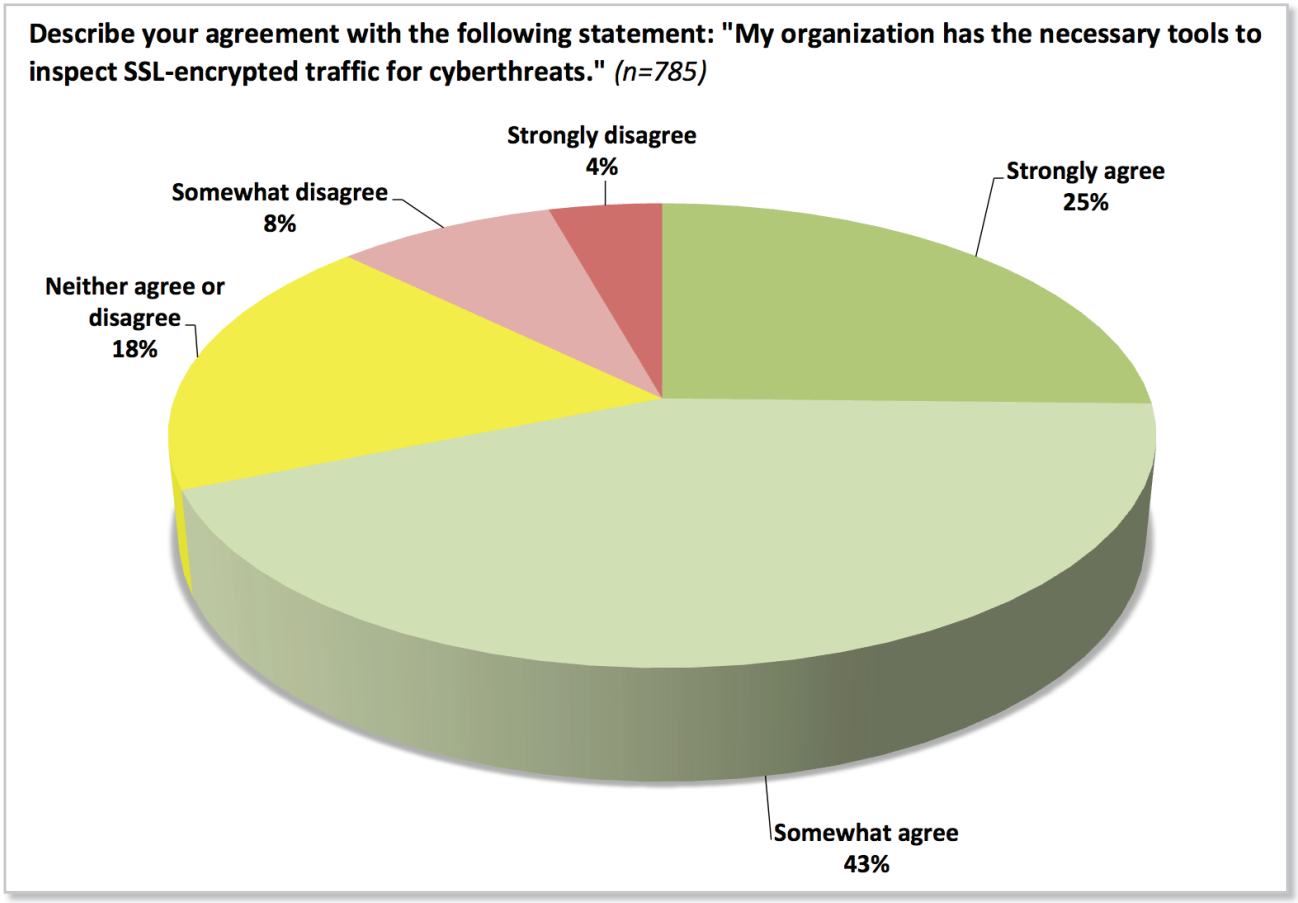

Figure 5: Tools for inspecting SSL-encrypted network traffic

"As security teams come to better understand the automation, control, and time-saving benefits possible with self-remediation technology, we fully expect adoption of related solutions to increase."

Endpoint and Mobile Security Deployment Status

The same approach used to assess network security technologies was repeated to gain insight into deployment status and acquisition plans for both endpoint and mobile security technologies. Let's begin with the former (see Table 2).

Not surprisingly, antivirus technology tops the list of already installed endpoint defenses. Disk encryption and application control trail by modest margins, but still enjoy an adoption rate of nearly two-thirds among respondent organizations.

At the other end of the spectrum, with the lowest current uptake, are containerization and micro-virtualization technologies. The news is not all bad in this case, however, as these solutions – which generally operate by providing an isolated workspace on the endpoint that is regularly reset to a known good/clean state – show the greatest promise for acquisition over the coming year.

Disappointing, in our opinion, is the rather low usage rate cited for endpoint self-remediation technologies. As security teams better understand the automation, control, and time-saving benefits possible with self-remediation technology, we fully expect adoption of related solutions to increase.

Which of the following endpoint security technologies are currently in use or planned for acquisition (within 12 months) by your organization to guard desktops, laptops, and servers against cyberthreats? (*n=788*)

	Currently in use	Planned for acquisition	No plans
Anti-virus / anti-malware (signature-based)	82%	14%	4%
Disk encryption	64%	22%	14%
Application control (whitelist/blacklist)	63%	22%	14%
Advanced malware analysis / sandboxing	53%	26%	21%
Data loss/leak prevention (DLP)	51%	29%	20%
Digital forensics / incident resolution	46%	29%	26%
Self-remediation for infected endpoints	42%	28%	30%
Containerization / micro-virtualization	34%	31%	35%

<-- Less Frequency ---------- More Frequency -->

Table 2: Endpoint security technologies in use and planned for acquisition

Shifting to the mobile security landscape, the fact that no single technology has been embraced by greater than 55% of respondent's organizations signifies a market that is still in a relatively early phase of development – or, at least one where there is still plenty of opportunity for new and innovative solutions!

"… the fact that no single technology has been embraced by greater than 55% of respondent's organizations signifies a market … where there is still plenty of opportunity for new and innovative solutions!"

Other notable findings from Table 3:

- ☑ The use of VPN connections, particularly to on-premises gateways (55%), repeats as the technology with the greatest rate of adoption (was 60% in 2014).
- ☑ Mobile device and mobile application management (32%) echo last year's results (30%) as the technology most likely to be acquired over the coming year.
- ☑ Results indicate marked growth in the uptake of antivirus/anti-malware solutions for mobile platforms, which went from a 36% rate of use in 2014 (last place) to 45% in 2015 (middle of the pack).

☑ There is considerable interest in acquiring containerization and micro-virtualization technologies to help with mobile device security – as was also the case for other types of endpoints (see Table 2).

Which of the following mobile security technologies are currently in use or planned for acquisition (within 12 months) by your organization to guard mobile devices (smartphones and tablets) and corporate data accessed by mobile devices, against cyberthreats? (*n=739*)

	Currently in use	Planned for acquisition	No plans
VPN to on-premises security gateway	55%	24%	21%
Mobile device / application management (MDM/MAM)	50%	32%	18%
Network access control (NAC)	50%	27%	23%
Mobile device file / data encryption	47%	29%	24%
Mobile device anti-virus / anti-malware	45%	29%	26%
Virtual desktop infrastructure (VDI)	44%	28%	28%
VPN to cloud-based security gateway	43%	25%	32%
Containerization / micro-virtualization	29%	31%	40%

<-- Less Frequency ---------- More Frequency -->

Table 3: Mobile security technologies in use and planned for acquisition

Monitoring Capabilities for Privileged Users

Participants were asked to indicate whether they believe their organizations have invested adequately in technology to monitor activities of users with elevated or privileged access rights (i.e., privileged users). While nearly one-third are decidedly skeptical about their organization's capabilities in this area, another major chunk of the respondent population – just shy of half – are no better than lukewarm in this regard (see Figure 6).

These findings align well with other anecdotal evidence on the topic, but still sound a bit too optimistic – at least to us. Making greater investments in solutions for privileged identity management would seem to be precisely "what the doctor ordered," given the repeated indications that credential theft and reuse attacks remain among the greatest threats facing today's organizations (just take a peek at any issue of the Verizon Data Breach Investigations Report over the last handful of years). The bottom line is that as they continue to beef up their capabilities for monitoring and analyzing network traffic to help identify elusive

cyberthreats (see “Network Security Technology Deployment Status”), today’s organizations would also be well served by placing greater emphasis on the challenge of identifying the misuse of privileged accounts –by rogue administrators as well as external threat actors who have managed to compromise such accounts.

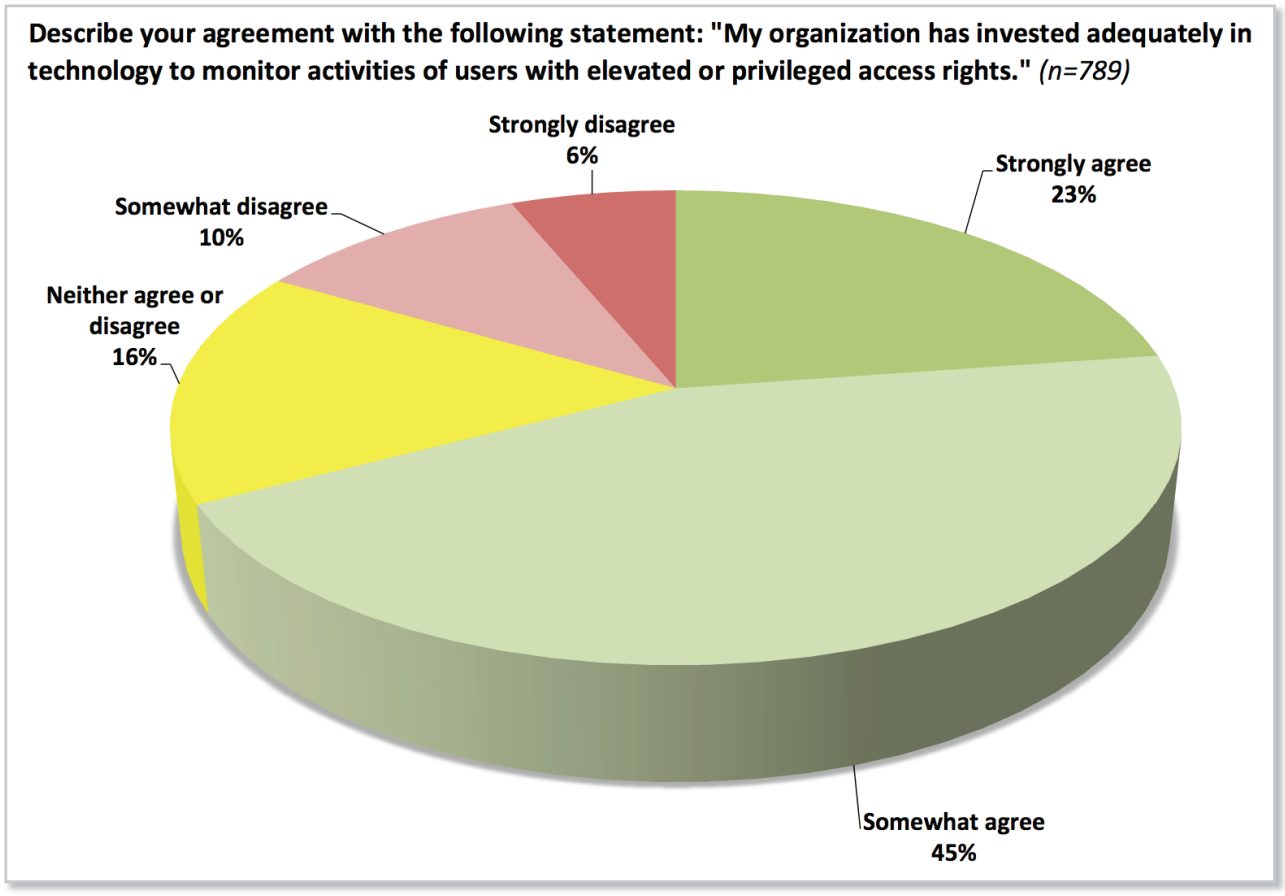

Figure 6: Adequacy of privileged user monitoring capabilities

Section 2: Perceptions and Concerns

The exploration of cyberthreat defenses now shifts from establishing baseline security postures to determining the types and sources of cyberthreats that concern today's organizations the most. Like the perceived weaknesses that have already been identified, these concerns serve as an important indicator of where and how it best makes sense for organizations to improve their cyberthreat defenses going forward.

This section of the report also investigates the reasons for obtaining third-party threat intelligence, the perceived security impact of software-defined networking, and the factors that most often inhibit today's organizations from establishing adequate cyberthreat defenses.

Cut to the Chase

- Malware and phishing / spear phishing are of the most concern to respondents
- Drive-by downloads, watering hole attacks, and DoS/DDoS attacks are of the least concern

Types of Cyberthreats

After tying with malware for the top spot in last year's report, this time around phishing/spear phishing finds itself in sole possession of the title for the type of cyberthreat that concerns our survey respondents the most (see Figure 7). Malware and zero-day attacks trail by only a small margin, as the composition of the top four entries remains unchanged from a year ago. New entrants – drive-by downloads and watering hole attacks – register the least concern, along with denial and distributed denial of service (DoS/DDoS) attacks.

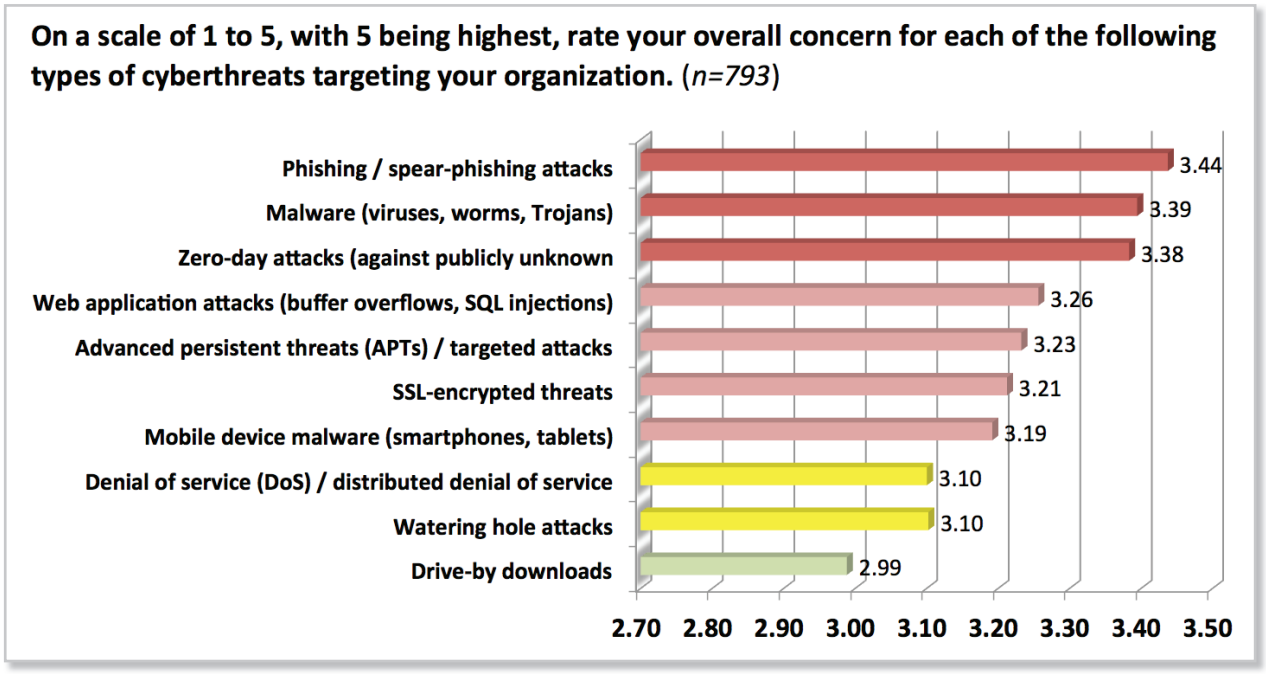

Figure 7: Relative concern by class/type of cyberthreat

"... this time around phishing/spear phishing finds itself in sole possession of the title for the type of cyberthreat that concerns our survey respondents the most."

However, this high-level summary only tells part of the story. Examining the raw (unweighted) data a bit more closely yields a few additional observations:

- ☑ Behind phishing, the class of threats most frequently receiving the designation "extremely concerned" was zero-day attacks.
- ☑ Drive-by downloads and mobile device malware were the threat classes most often receiving the "not concerned" designation.
- ☑ For each class of threats, "not concerned" was chosen by at least 6% of the respondents.
- ☑ Across the board, the combined percentage of respondents answering "not concerned" or "mildly concerned" was considerably greater than one might expect, ranging from a low of 22% for malware to 34% for drive-by downloads.

Mobile Devices in the Crosshairs

When asked to characterize how the volume of threats targeting their organization's mobile devices (e.g., smartphones and tablets) changed in the past 12 months, a whopping 6 out of 10 respondents indicated there had been an increase (see Figure 8). This trend – along with the modest adoption rates for mobile security technologies (see Table 3) – helps complete the picture that explains why mobile devices are considered the weakest link in most organizations' defenses (see Figure 4).

Survey Insight

6 of 10 respondents indicated an increase in the volume of threats targeting their organization's mobile devices over the past year.

On a regional basis, slightly more European respondents (64%) observed an increase in the volume of mobile device threats than did their North American counterparts (57%).

Overall, only 6% of respondents saw a decrease in the volume of mobile device threats over the past year.

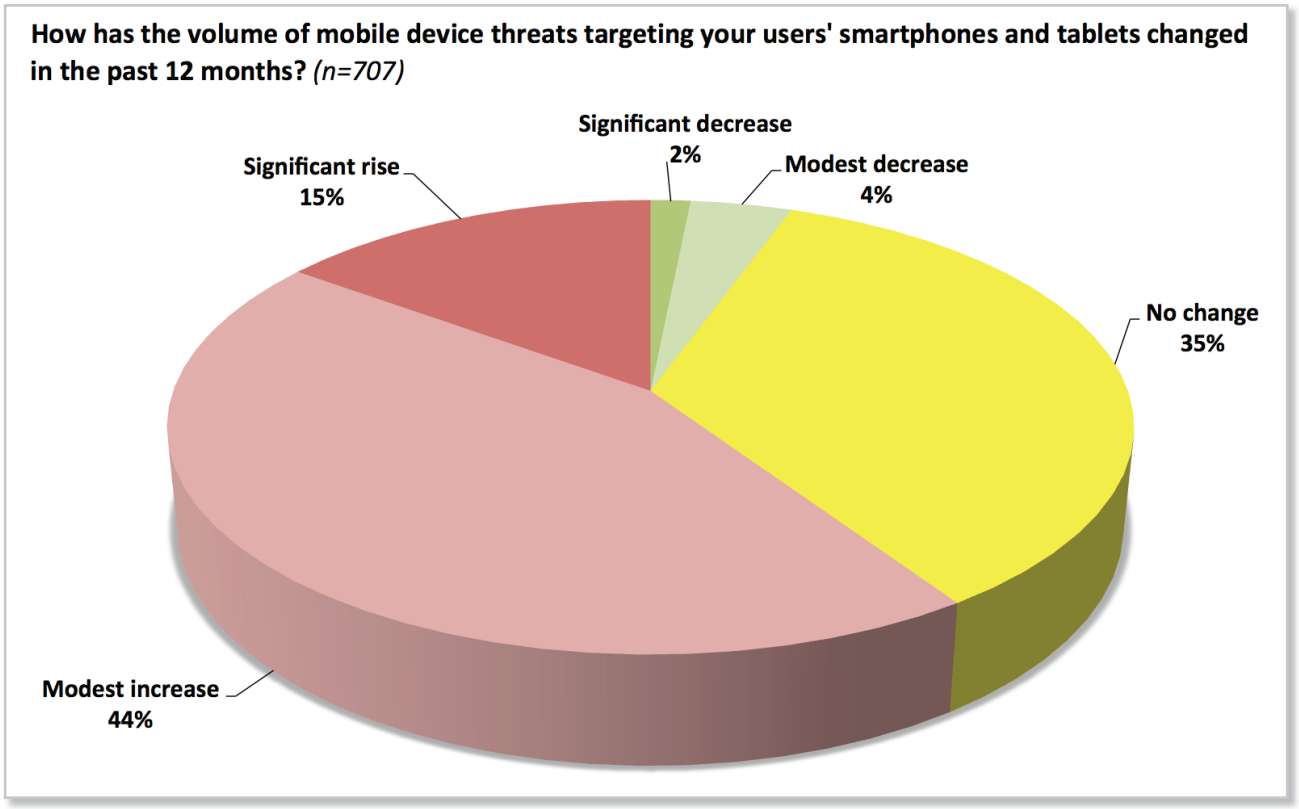

Figure 8: Change in volume of threats to mobile devices

SaaS-based File Sharing Applications

Respondents were asked to rate their concern for different issues associated with employee use of SaaS-based file sharing applications on a scale of 1 to 5, with 5 being the highest. The results, in the form of weighted averages, are depicted in Figure 9.

Although inadvertent exposure of confidential data elicited the greatest concern to garner the top spot on our chart, we would be remiss if we failed to point out that:

- ☑ The total spread in weighted responses between the issue of least concern (data exposure stemming from compromise of the SaaS provider) and the one of greatest concern (accidental data sharing) was not all that significant (0.17).
- ☑ Overall, the average degree of concern expressed (~3.35) was fairly modest, which would seem to suggest either that organizations have already deployed controls to address these risks, or – more likely in our opinion – that this set of issues has not

Survey Insight

Accidental disclosure of sensitive data was cited as the greatest concern associated with employee use of SaaS-based file sharing applications.

yet achieved priority status for most security teams (at least relative to the other challenges on their plates).

Looking at the raw data, it is also interesting to note that maintaining regulatory compliance was the option most often receiving the designation "extremely concerned." The fact that this issue still only ranked in the middle of the pack overall points to the presence of a large, off-setting group of organizations where the influence of data privacy and security regulations is, at best, minimal.

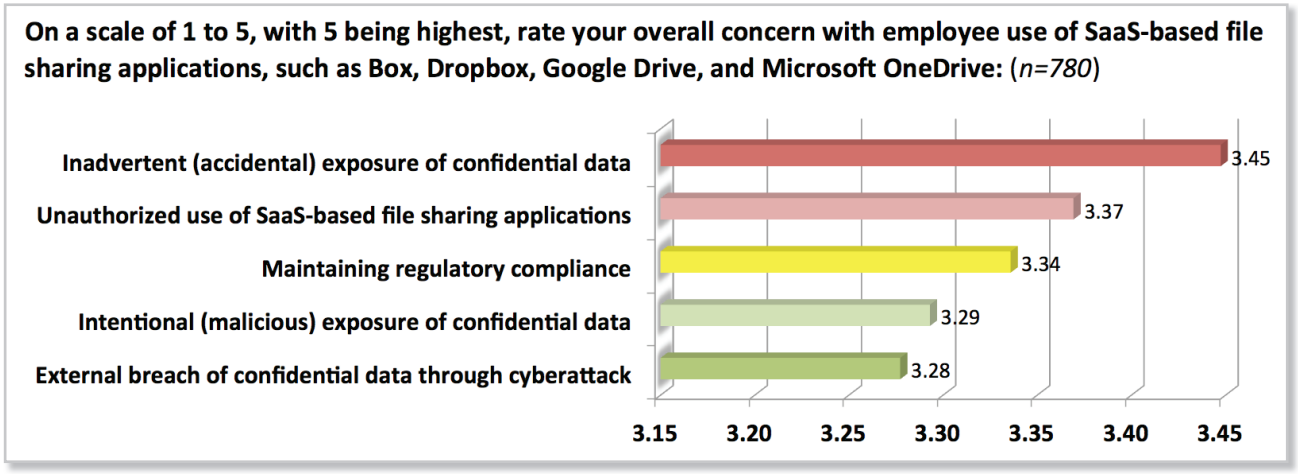

Figure 9: Concerns with employee use of SaaS-based file sharing applications

Threat Intelligence Practices

The objective of our next query was to ascertain the extent to which and the specific ways organizations are using supplemental (i.e., third-party) threat intelligence services to bolster their cyberthreat defenses.

The apparent adoption rate of 87% for threat intelligence *must* include not only the use of third-party services, but also the piggy-backed, second-party intelligence that typically comes along with leading network security technologies – for example, the signature/protection updates, threat notifications, research portal, and such that accompany leading IPSs. Otherwise, the figure is entirely unbelievable, especially given: (a) that standalone threat intelligence offerings are a relatively new/emerging segment of the market; and (b) that the finding from Table 1 indicates a more realistic adoption rate of 43%.

Survey Insight

Currently, threat intelligence is being used primarily for detecting and blocking threats, and less for investigating their occurrences and causes.

The interesting part here is the confusion itself, which points to the need for greater delineation regarding the sources (and probably value propositions, too) of supplemental threat intelligence on the part of associated vendors (and ourselves).

Turning to the use cases for threat intelligence (regardless of source), automatically blocking threats (67%) narrowly edged the second-place response of just using the supplemental information as a basis for detection (61%). Fewer respondents (43%) indicated their organizations use this information to assist with troubleshooting and forensic activities. Overall, these findings are consistent with both our second-party postulation and the relative immaturity of the market segment, as they point more to the use of threat data feeds (e.g., new signatures or updated lists of bad IP addresses and URLs) than context-rich information (e.g., pertaining to individual groups of threat actors, recent tendencies, and vertical industry specialization).

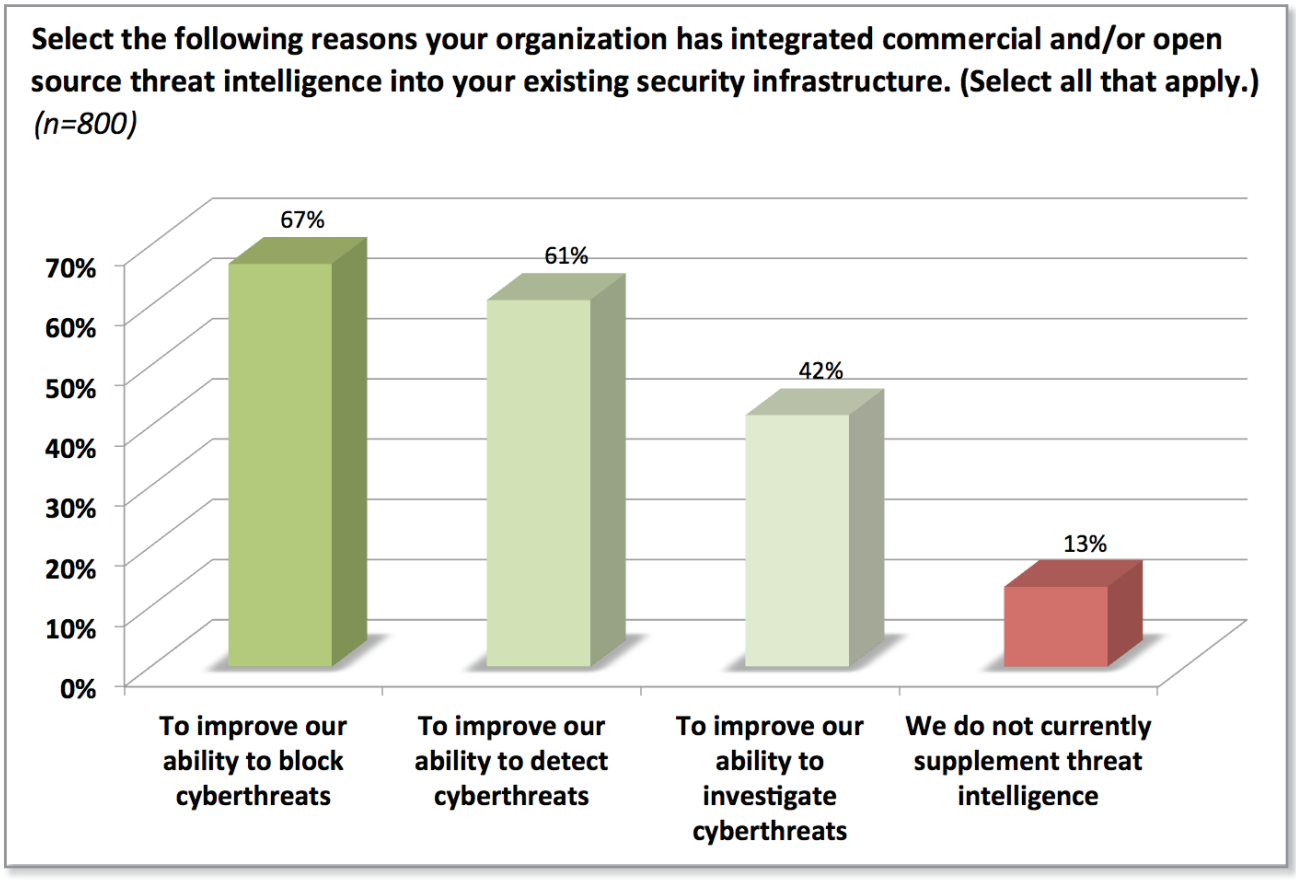

Figure 10: How threat intelligence is being leveraged

Barriers to Establishing Effective Defenses

Establishing effective cyberthreat defenses is by no means easy to do. If it were, one would expect far fewer successful cyberattacks and greater confidence on the part of IT security practitioners with regard to the likelihood of future breaches (see Figures 2 and 3). Part of the issue is undoubtedly the ever-evolving threat landscape. Hackers have a seemingly endless capacity to advance their wares – not to mention that, as defenders, organizations can only guess at hackers' next moves.

"Turning to the survey data, for the second year in a row 'low security awareness among employees' tops the charts …"

But what about other factors? What are the other obstacles that IT security teams must overcome and, more importantly, which of them are most significant?

Turning to the survey data, for the second year in a row "low security awareness among employees" tops the charts, with "lack of budget" and "too much data to analyze" close behind in the second and third positions, respectively (see Figure 11).

Overall, the primary conclusion to be drawn from this data is that for today's security teams, getting their job done is less about overcoming a dearth of effective tools and contextual data or having difficulty justifying investments, and more about getting users to stay out of trouble, having sufficient budget in the first place, and being able to plow through all of the data already available to them. Security vendors, can you take a hint?

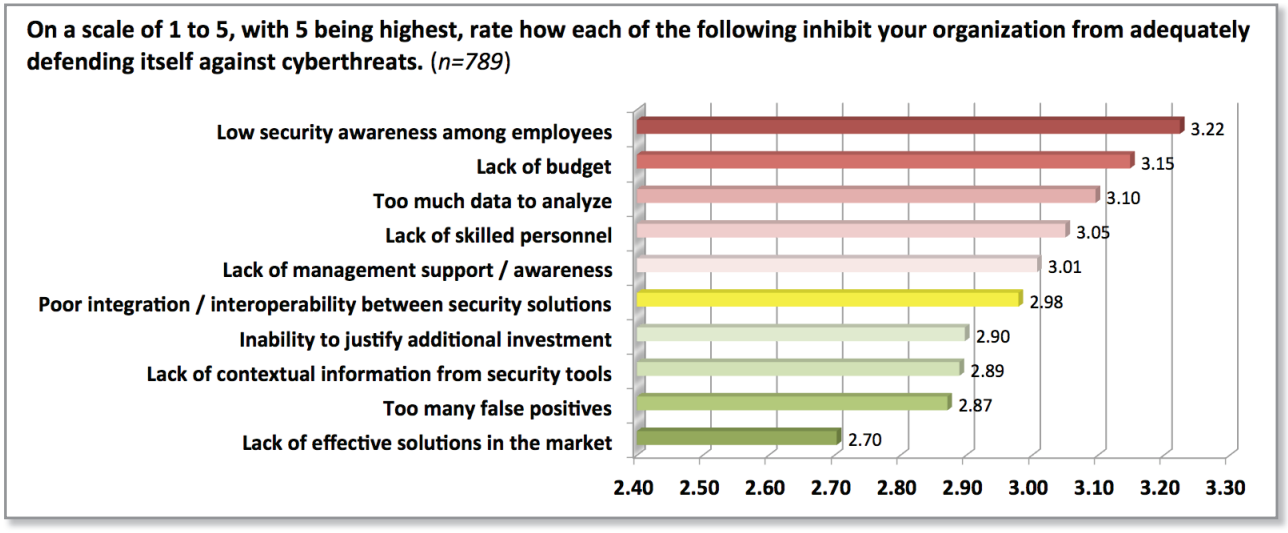

Figure 11: Inhibitors to establishing effective cyberthreat defenses

Survey Insight

Respondents are decidedly bullish on the security impact of SDN, with ten times as many convinced it aids their organization's defenses compared to those that believe it has a deleterious effect.

Impact of Software-defined Networking

Software-defined networking (SDN) – along with its close cousin, network virtualization – has the potential to revolutionize not only network infrastructure and network services delivery, but also many aspects of network security. Easily establishing micro-segmentation and providing the ability to "pipe in" necessary services regardless of their physical location are just two examples.

According to the data, our survey respondents see the security-oriented value of SDN, too. When asked to characterize how SDN impacts their organization's ability to defend against cyberthreats, those indicating it has a positive impact (63%) outnumbered those on the negative side of the fence (6%) by more than 10 to 1 (see Figure 12).

Is it surprising that nearly one-third of our survey population remain on the fence, neither agreeing nor disagreeing that SDN helps their cyberthreat defense efforts to a meaningful extent? Not really, especially considering that the transition to SDN is neither quick nor straightforward in many cases, often resulting in delayed realization of promised benefits.

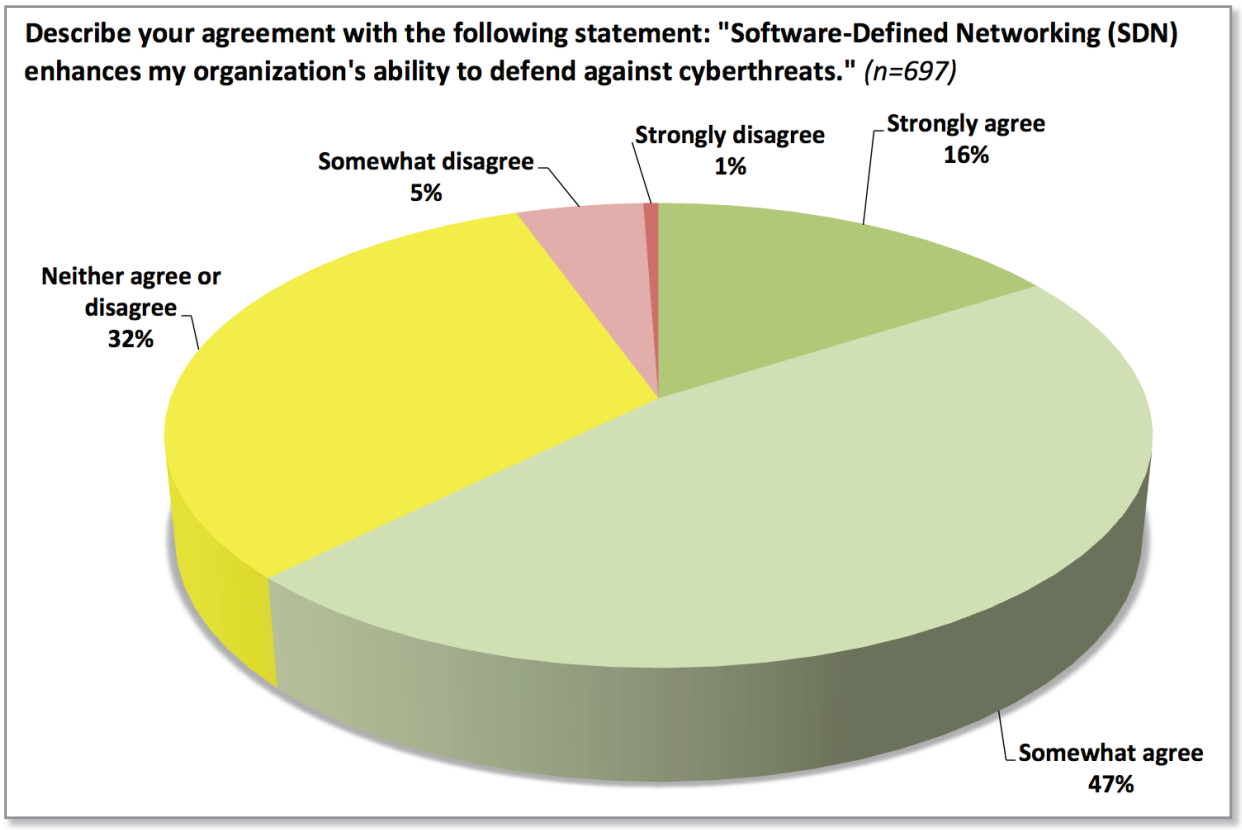

Figure 12: Perceived impact of software-defined networking on cyberthreat defenses

Section 3: Attack Surface Reduction

Establishing effective cybersecurity defenses requires more than simply implementing "next-generation" technologies designed to detect the latest wave of elusive cyberthreats to hit the streets. Given the well-known fact that the vast majority of cyberattacks still focus on exploiting known vulnerabilities, it can even be argued that a more practical strategy to mitigate cyberthreats is to first reduce one's attack surface, and then use an overlapping set of detection-oriented countermeasures to mitigate the residual risk.

Options available to organizations that help with the first part of this strategy – reducing their attack surface – include tactics such as:

- ☑ reducing the number of open ports and services on Internet-facing systems;
- ☑ using next-generation firewalls to granularly control network and application access;
- ☑ eliminating all unnecessary protocols and services running on endpoints, servers, and other internal systems; and,
- ☑ leveraging identity and access management solutions to implement a least-privileges policy.

This section of the report examines a few other relevant tactics and tools that can also be applied in this regard, including full-network scans for vulnerable systems, continuous monitoring, and employee awareness training for phishing detection.

"Identified earlier as playing a prominent role in organization's mobile security strategies, network access control (NAC) technology was also selected by respondents as the top technology for reducing their network's attack surface."

Technologies for Attack Surface Reduction

Identified earlier as playing a prominent role in organizations' mobile security strategies (see Table 3), network access control (NAC) was also selected by respondents as the top technology for reducing their network's attack surface (see Figure 13). Trailing by a small margin were penetration testing and vulnerability assessment solutions, which were cited as being regularly used by 61% and 53% of organizations, respectively.

Lagging even further behind, security configuration management (48%) and file integrity monitoring (34%) did not manage to achieve the mark of being deployed in at least half of our respondents' organizations.

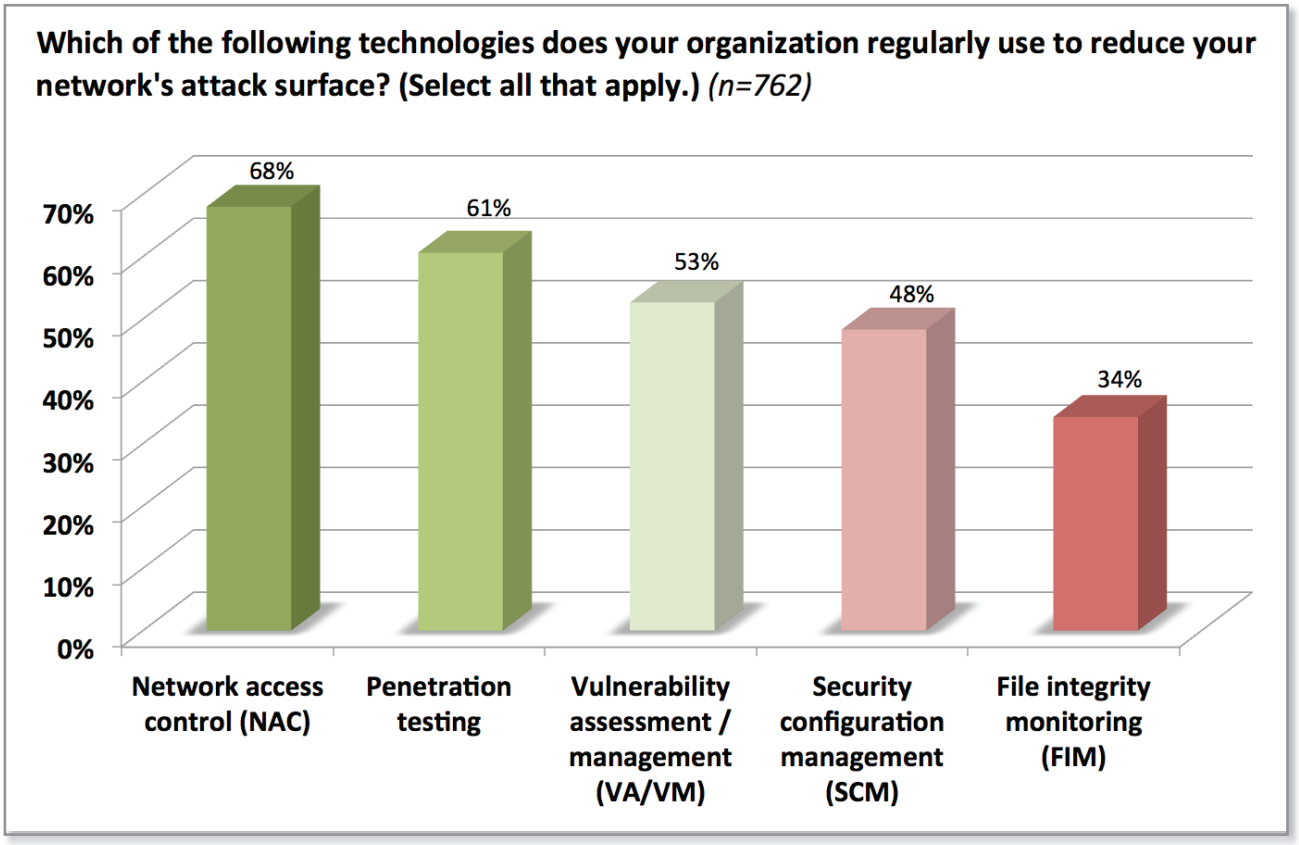

Figure 13: Technology choices for attack surface reduction

Inexplicably, the data also indicates that only 32% of European organizations utilize vulnerability assessment technology for attack surface reduction. This compares to 62% for North American respondents.

Frequency of Network Vulnerability Scans

Respondents were asked how frequently their organization conducts full-network, active vulnerability scans (as opposed to scanning individual devices or enclaves, or using passive vulnerability scanning technologies that, by design, are always on). Similar to last year's, the results are somewhat mixed (see Figure 14).

On one hand, we consider it a positive sign that nearly 4 in 10 organizations are conducting full network scans at least monthly, if not more often. This result represents a significant commitment to cybersecurity and likely indicates greater understanding of the tremendous value of continuous monitoring.

Cut to the Chase

- 39% of responding organizations scan monthly, weekly, or daily
- 33% of responding organizations conduct full-network vulnerability scans less often than quarterly

On the other hand, it is discouraging to see a full third of organizations taking advantage of this powerful countermeasure less often than quarterly.

Once again, approximately 30% of organizations are scanning quarterly, just meeting the minimum requirement for compliance with many of the prevailing regulations and standards (such as the Payment Card Industry Data Security Standard, or PCI-DSS).

No statistically significant differences were observed by geographic region.

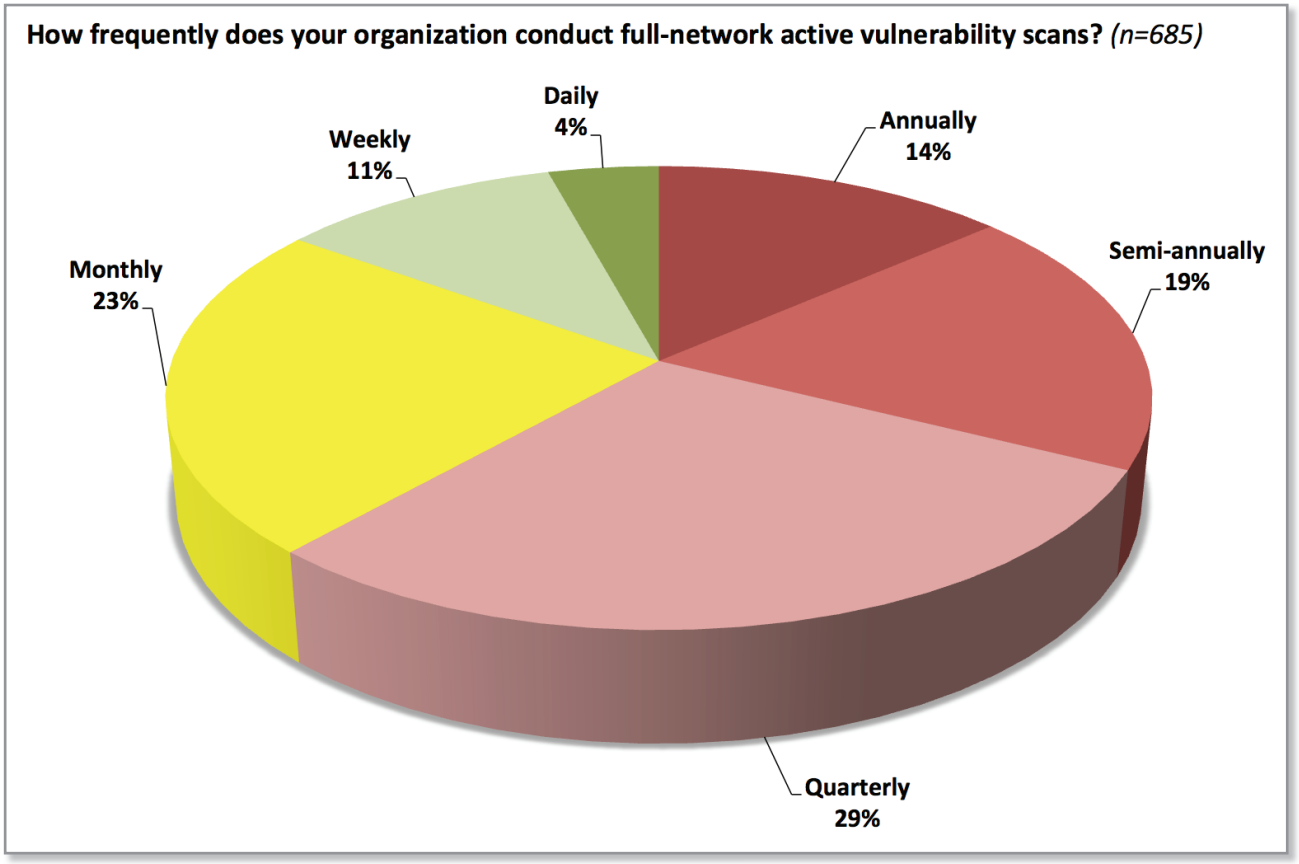

Figure 14: Frequency of full-network active vulnerability scans

Continuous Monitoring Practices

Continuous monitoring is achieving widespread recognition as a best practice – if not an essential one based on the pace with which new cyberthreats are being launched at today's organizations. The survey results concur: for each of four key attack surface reduction technologies, at least 62% of respondents indicated their organization has implemented continuous monitoring (either alone or in conjunction with periodic, ad hoc scanning/monitoring).

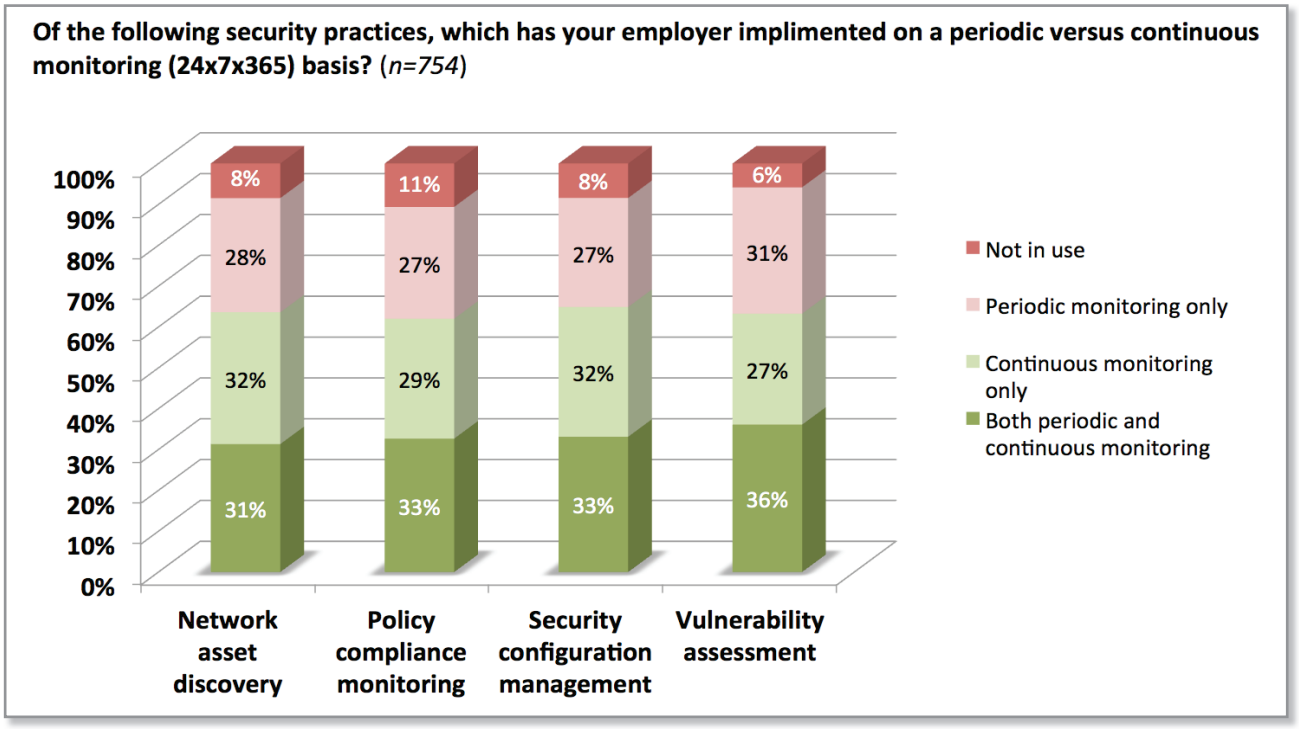

Figure 15: Periodic versus continuous monitoring

Focus on Phishing

Phishing and spear phishing are clearly a significant concern for today's organizations (see Figure 7). It's a familiar story, but a large part of the problem in this case is the inability of associated technical countermeasures to keep up. Even without the high-fidelity targeting enabled by the social media-fueled dispersion of personal information, the increasingly intelligent "engines" used to generate volumes of highly refined phishing messages are more than good enough to deliver a steady stream of "bites." Just like it is with the rest of cyberthreat arms race, the associated detection technologies are always a step (or two) behind.

"… the increasingly intelligent 'engines' used to generate volumes of highly refined phishing messages are more than good enough to deliver a steady stream of bites."

To help offset this differential, best practice calls for educating employees about this type of attack in particular. But how are today's organizations actually doing in this regard? According to our data, the answer is "not so great."

When asked whether their organization has invested adequately in security awareness training for phishing attacks, more than 4 out of 10 respondents were doubtful (see Figure 16). With another 4 out of 10

respondents agreeing only “somewhat” with the adequacy of their organization’s training in this critical area, that leaves less than 20% of respondents expressing confidence that their colleagues have been sufficiently schooled to avoid being “caught.”

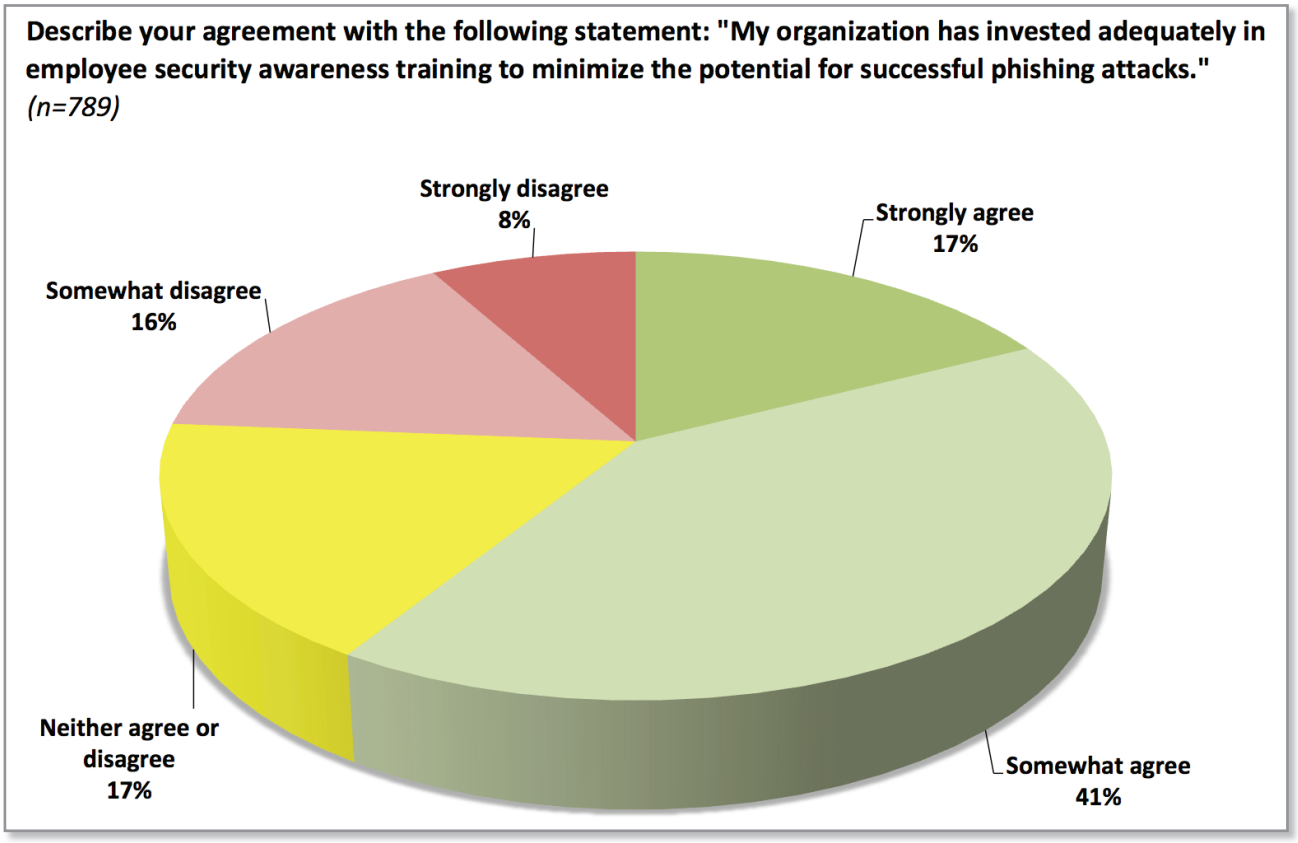

Figure 16: Perceived adequacy of employee training for phishing attacks

Host Remediation Strategies

Once vulnerable hosts become infected, how are organizations pursuing remediation? On a global basis, the survey results indicate only a modest preference for tools that enable remote execution of a package intended to restore infected hosts to a clean state (see Figure 17).

However, just over one-third of respondent organizations continue to pursue the more pedestrian, time-intensive approach of manually performing remediation – an approach, by the way, which carries with it an increased “time of exposure” and, therefore, increased potential for data theft and other forms of damage.

Survey Insight

European organizations are nearly twice as likely as their North American counterparts to use automated, remote execution tools for remediation of malware-infected hosts.

The more expedient "wipe and re-image" technique lags behind the others, with only 25% of global respondents identifying it as their organization's preferred approach for host remediation.

Noteworthy, too, is the strong preference by European organizations for automated, remote remediation (used by 59%), as well as their seeming lack of interest in the wipe and re-image alternative (used by only 11%).

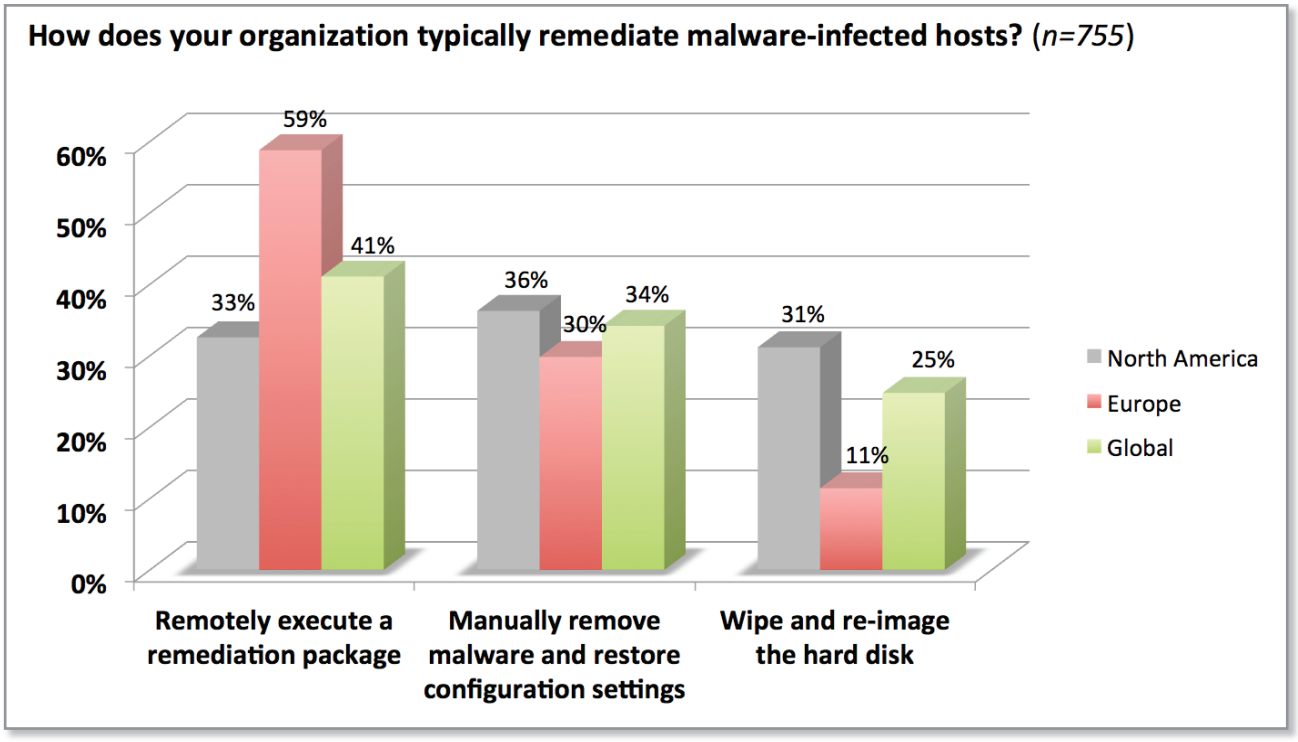

Figure 17: Preferred host remediation practices

Section 4: Future Plans

Organizations can ill afford to stand still when it comes to maintaining effective cyberthreat defenses. IT security teams must keep pace with the changes around them by making changes of their own. Some of their intentions in this regard were already revealed in an earlier section of the report, where we covered the network security, endpoint, and mobile security technologies planned for acquisition in 2014. This section further explores their plans for the future.

IT Security Budget Change

Among the biggest factors contributing to an IT security team's ability to effect change is its budget (see Figure 11). Thankfully, for the second year running, our data shows that IT security budgets are in excellent shape, with more than 90% of organizations continuing to invest in cyberthreat defenses at least at the same level they did in 2014 (see Figure 18).

"For the second year running, our data shows that IT security budgets are in excellent shape."

Other notable findings:

- ☑ Globally, roughly 60% of IT security budgets are expected to rise in 2015 – with European organizations (68%) out-pacing North American ones (58%) in this regard. This compares to only 48% of organizations that expected their budgets go up in the previous year.
- ☑ Only 20% of those anticipating a budget increase expect it to be 10% or greater.
- ☑ Overall, only 8% of IT security budgets are predicted to be in decline – with only 5% of European organizations expecting to take a cut.
- ☑ Of those expecting to see a budget cut, only 1 out of 4 believe the cut will be 10% or greater.

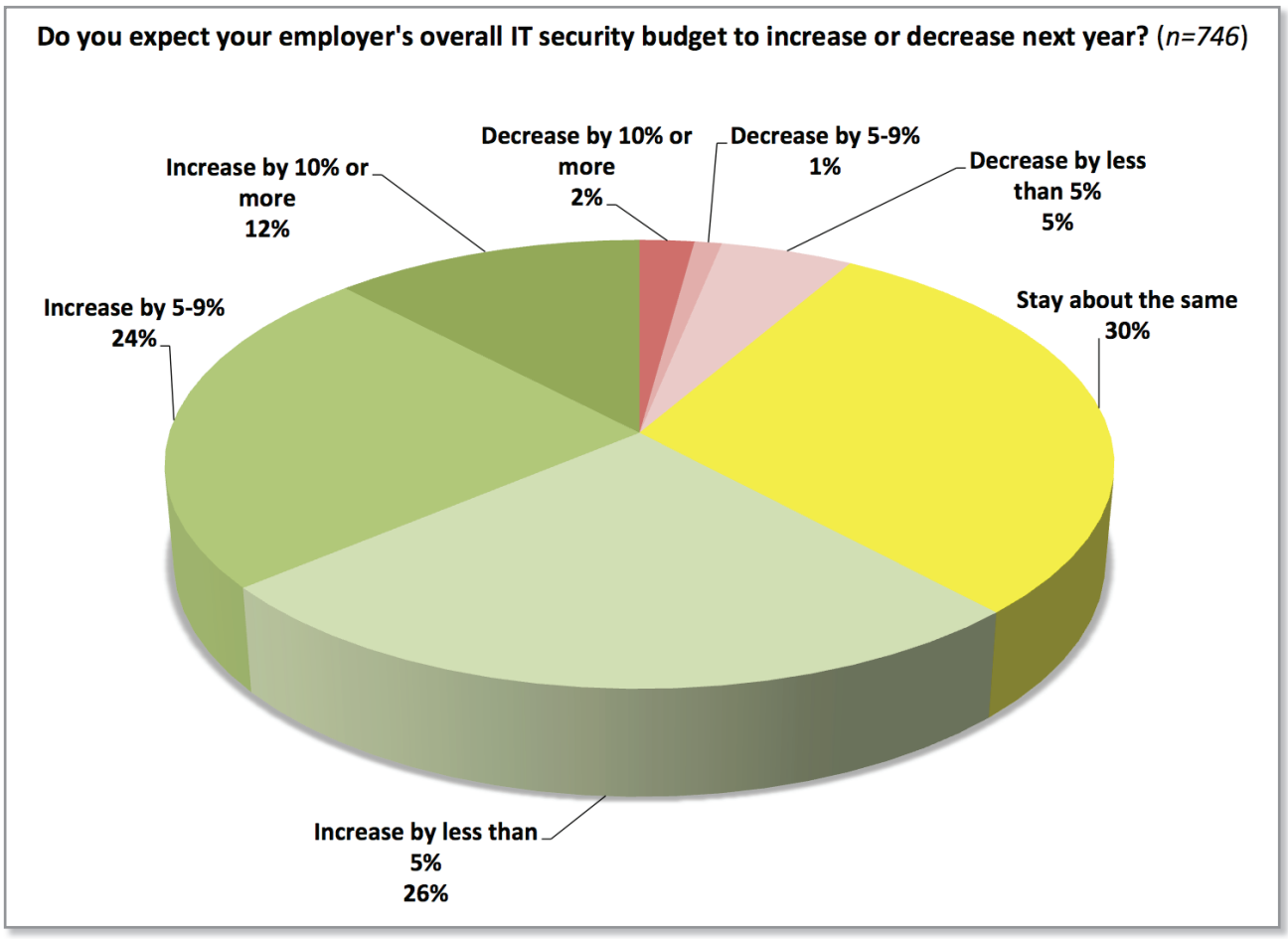

Figure 18: IT security budget changes for 2015

Survey Insight

Adoption of BYOD policies may have run into a speed bump but is still expected to take off. Within two years, more than three- quarters of responding organizations anticipate having BYOD policies in place.

The BYOD Invasion (Revisited)

We've already established that mobile devices are the biggest security pain point for most of today's organizations (see Figure 4). A significant portion of this pain stems from the consumerization of IT and its manifestation in the form of business-driven support for BYOD policies. With BYOD, IT security teams are forced to contend not only with an increasingly diverse array of devices – all with different native security capabilities and widely varying support from third-party security software – but also with the fact that control over these devices must be "shared" with their owners.

So when do organizations expect to have to deal with the challenges of this brave new BYOD world? The answer, it turns out, is a bit complicated (see Figure 19). Although our findings from last year are nearly identical to those from this year's survey, this continuity presents a problem. In particular, based on the 2014 results, we

should now be seeing a significant bump in the number of organizations that have “already implemented” BYOD policies – to the tune of an increase of approximately 26%, leading to a total for “already implemented” in 2015 that is north of 50%. However, things clearly didn’t unfold that way.

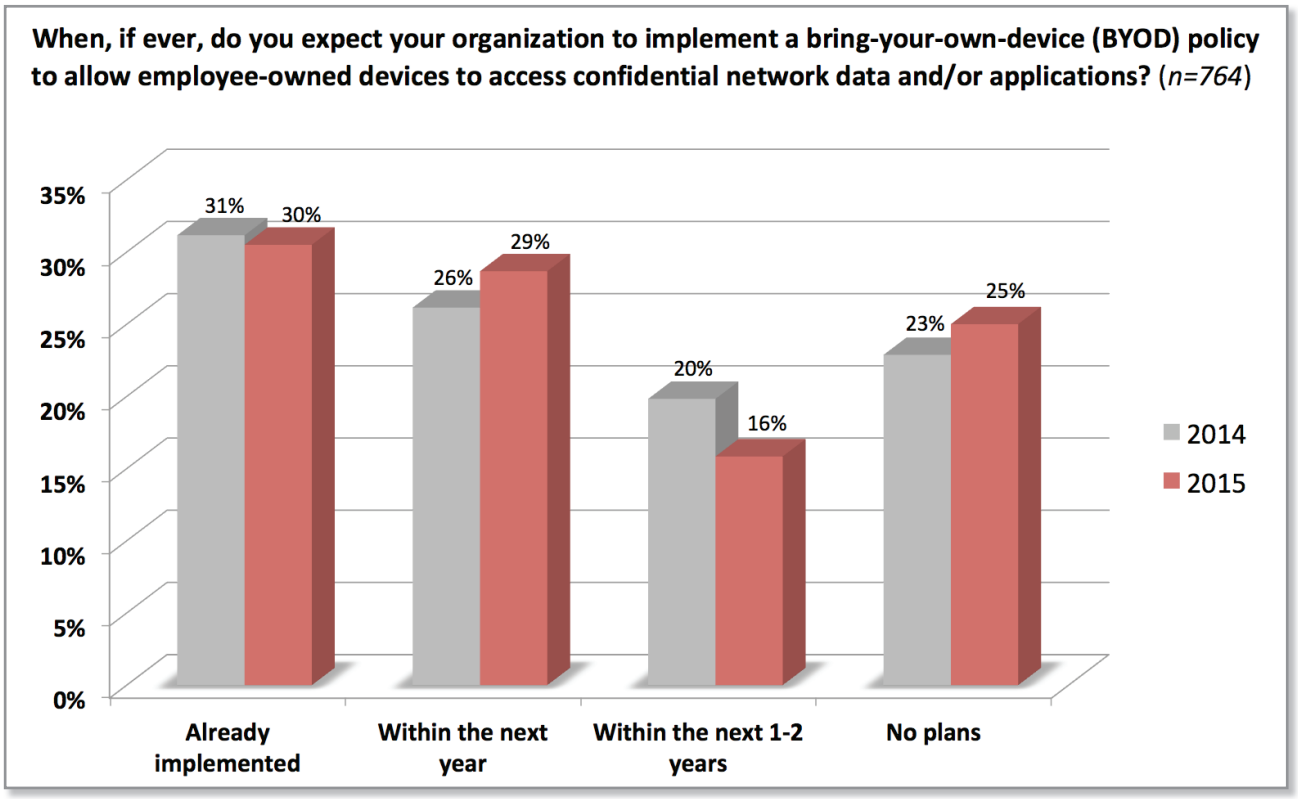

Figure 19: Timeframe for implementing BYOD policy

Instead, the data suggests a “pause” in BYOD implementations – perhaps due to the second wave of BYOD adopters’ sensibly taking a “time out” to first sort out the related technology landscape and implement associated defenses (see Table 3). One can always hope, right?

Whatever the reason is, though, the data also indicates that the virtual pause button will soon be released, with 45% of respondents expecting their organizations to adopt BYOD policies within the next two years.

On a regional basis, the data indicates that European organizations (19%) lag those in North America (36%) when it comes to already having implemented BYOD policies. It also shows, however, that they expect to fully make up this difference (and then some) within the coming year, as they head toward a total adoption

rate of 61% by 2016. This compares to an expected adoption rate of 58% by 2016 for North American organizations.

Endpoint Protection Plans

It's clear that the challenges facing today's IT security teams do not stop at mobile devices, but also extend to other types of endpoints, such as desktops and laptops (see Figure 4). Part of the issue is, and always will be, the potential for ill-advised user actions – such as opening suspicious email attachments, revealing their systems passwords, and of course, visiting questionable websites. Compounding matters is the steadily eroding effectiveness of signature-based countermeasures in the face of advanced malware – featuring polymorphism and an ever-growing array of evasion techniques.

"Two-thirds signaled they would be evaluating new solutions for endpoint anti-malware protection, up from 56% last year."

Given this situation, we asked participants about their organization's intent to evaluate new anti-malware solutions for endpoints. The results reinforce our earlier findings that endpoints remain a significant problem area for most organizations (see Figure 20). Two-thirds (67%) signaled they would be evaluating new solutions for endpoint anti-malware protection, up from 56% last year.

Telling, too, is the 50% increase over last year's result in the percentage of respondents indicating their organization's intent to replace, rather than augment, existing solutions.

The findings are even more dramatic for European respondents. A whopping 78% indicated plans to evaluate new endpoint security products, with 44% looking to replace instead of augment existing solutions. In comparison, North American respondents registered 62% and 28% for evaluating and replacing, respectively.

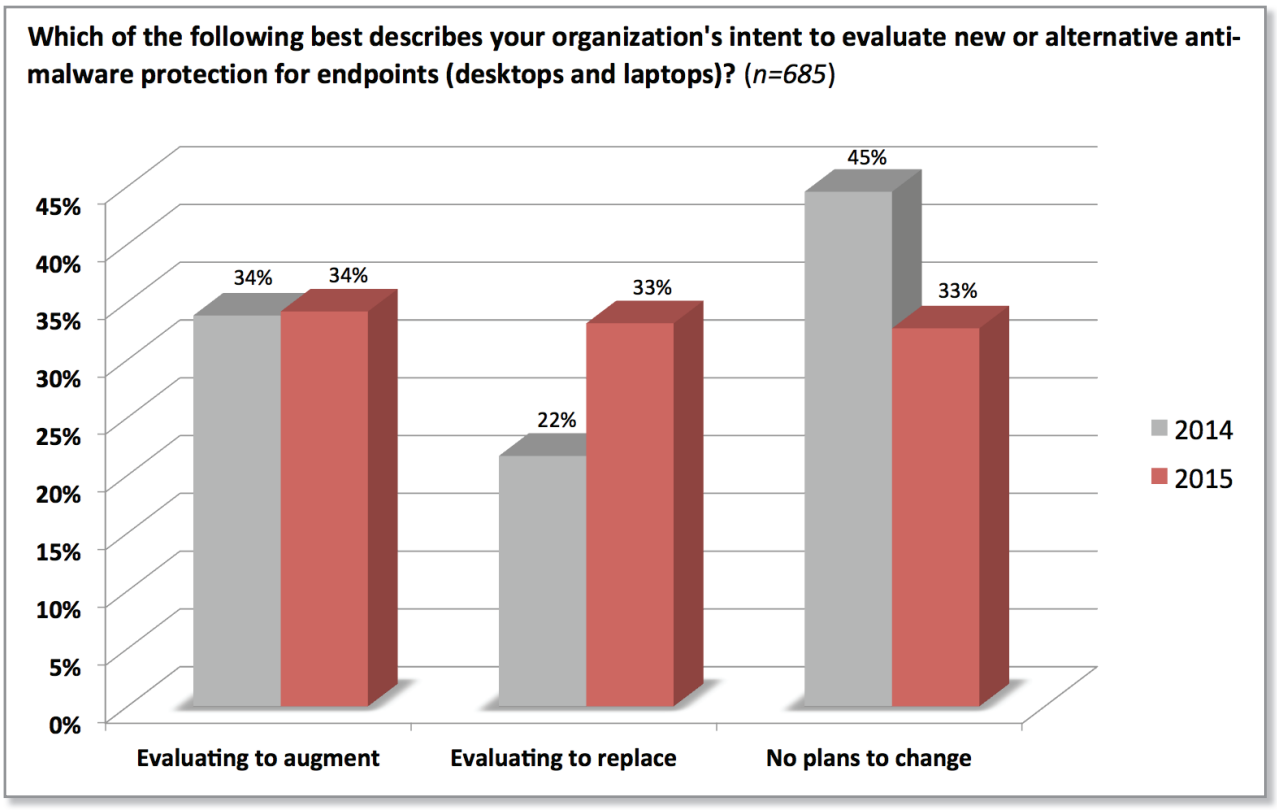

Figure 20: Plans for replacing or augmenting endpoint protection software

The Road Ahead

It certainly wouldn't be surprising to see today's IT security professionals suffering from "doom and gloom" syndrome. Not only are the networks and systems they're tasked to defend in a constant state of flux, but also the barbarians at the gate are well organized, funded, and armed – not to mention persistent. Moreover, while the bad guys need only find a single chink in an organization's armor, success for the home team often hinges on being able to defend against a plethora of vulnerabilities and threats they don't even know about.

As the 2015 Cyberthreat Defense Report reveals, too, at many organizations there are still plenty of chinks requiring attention. For example:

- ☑ Along with social media applications, endpoint computing devices of all types – but especially mobile ones such as smartphones and tablets – are recognized as relative weak spots in most organizations' defenses (see Figure 4).
- ☑ Although they are among the leading solutions planned for acquisition in the coming year, many of the "next-generation" technologies most likely to be effective against advanced malware and targeted attacks, such as security analytics, network behavior analysis, and cyberthreat intelligence services, show fairly modest adoption rates (see Table 1).
- ☑ More than a third of today's security teams lack the tools needed to inspect SSL-encrypted traffic for cyberthreats – or the exfiltration of sensitive data (see Figure 5).
- ☑ Only one-quarter of IT security professionals are confident that their organizations are doing enough to monitor privileged user accounts for signs of misuse and/or compromise (see Figure 6).
- ☑ Adoption rates for key technologies and practices instrumental in reducing a network's attack surface – such as security configuration management and conducting full-network vulnerability scans more often than quarterly – remain fairly modest (see Figures 13 and 14).
- ☑ Less than 20% of IT security professionals are confident in the level of investment made by their organizations to educate employees about phishing attacks (see Figure 16).
- ☑ A full two-thirds of organizations recognize that the anti-malware solution currently being used to defend their endpoints is not providing adequate protection (see Figure 20).

Instead of being daunted by these challenges, however, it appears that today's IT security professionals remain relatively optimistic, or at least confident in their abilities, as only half expect their organizations to fall victim to a successful cyberattack in the coming year (see Figure 3). Of course, it doesn't hurt matters that security budgets are both healthy and rising (see Figures 1 and 18). Having additional funding at their disposal should enable enterprise security teams to not only fill known gaps in their organization's defenses but also start to get ahead in the game, perhaps.

Looking beyond the scope of the 2015 Cyberthreat Defense Report survey, here are some "areas of interest" where we believe proactive attention and judicious investment have the potential to yield significant returns in terms of an organization's ability to defend against both current and future generations of cyberthreats.

- ☑ **Next-generation endpoint defenses.** The issue isn't that traditional, signature-based endpoint solutions are broken; rather, it's that what they do – primarily detect known malware – is no longer sufficient. Fortunately, the market is responding with a new wave of innovation for endpoint defenses. Next-generation solutions that deserve consideration for augmenting legacy endpoint security tools fall into several evolving categories, including: host-intrusion prevention 2.0 (where system-level "traps" and "check points" are set/monitored to detect the relatively modest set of exploit mechanisms most malware relies upon); containerization/micro-virtualization (where isolated, short-duration "workspaces" shield the endpoint from contracted infections and reset to a known clean state upon completion of each user session); real-time file classification and execution control (where advanced machine learning algorithms make real-time permit/deny decisions regarding file execution); and big data correlation (where advanced endpoint instrumentation is coupled with an out-of-band analysis engine).
- ☑ **The evolution of cyberthreat intelligence services.** Basic threat intelligence services are far from useless. Feeds that deliver malware signatures, URL reputation data, and intrusion indicators directly and immediately improve the effectiveness of commonly deployed threat detection and prevention technologies. Other, mid-level feeds that include basic information on the prevalence, sources, and targets of malware and attack activities help expose patterns and may even reveal how to remediate compromised systems. However, even greater value can be derived from the still-coalescing top end of this rapidly growing market segment. The high-level feeds delivered in this case are fully customized to individual customers' requirements and include forward-looking analysis of threats, actors, and methods that can be used not only for tactical purposes – such as immediate adjustment of configured countermeasures – but also to inform an organization's longer term security strategy (i.e., 2+ years out).
- ☑ **Micro/hyper-segmentation.** Segmentation for the purpose of establishing and enforcing differentiated policies has long been a standard security practice. The only catch is that doing so at other than a very coarse level has, at least until recently, been impractical due to compounding infrastructure cost and complexity. Most major cloud computing platforms overcome these challenges, however – for example, by natively incorporating their own software firewalls around every virtual machine. In turn, SDN and still emerging software-defined security enable extension of similar practices into non-cloud (i.e., physical, on-premises) networks. The result is a not too distant future where every networked resource can be treated to its own, individual security zone – an architecture (if you will) that makes it exceedingly more difficult for hackers and automated threats to expand their footprint once they gain access to an environment, and, by the way, also makes it far easier to detect anomalous activity.

- ☑ **Software-defined security.** Following close on the heels of SDN, software-defined security holds the promise of revolutionizing security infrastructure and operations alike. In the case of the former, the physical location of network security devices will become irrelevant as security teams gain the capability to logically pipe in required security services at any point in any application flow / communication path, as needed. As for security operations, the ability to leverage APIs to increasingly automate and orchestrate routine functions will free up security personnel for tasks that require greater expertise, such as security architecture, development of organization-specific analytics, and incident response.

For further insights on these and other emerging areas pertinent to IT security, be sure to tune in for the third annual Cyberthreat Defense Report, currently scheduled for release in the first quarter of 2016.

Appendix 1: Survey Demographics

Of our 814 qualified survey participants, 69% specified United States of America or Canada as their country of residence. The balance of the survey population is spread across five European countries—United Kingdom, France, Germany, Spain, and Italy.

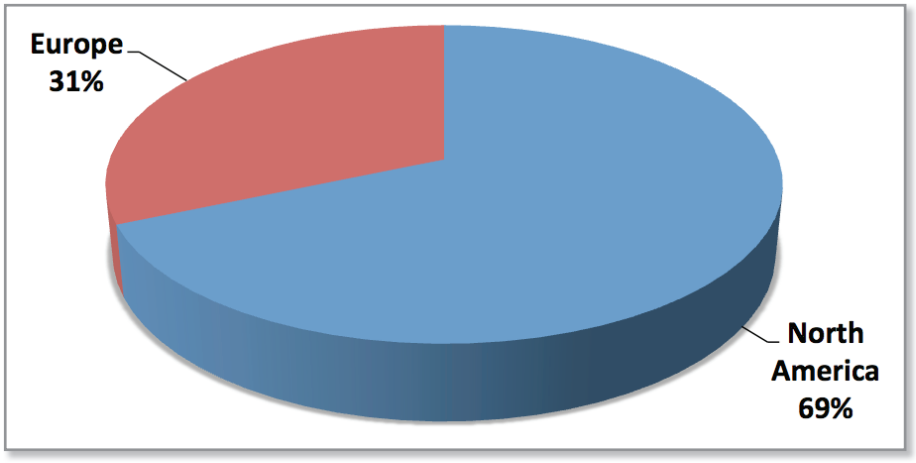

Figure 21: Survey participation by geographic region

As for the roles of our survey participants, nearly one-third hold senior positions (CIO, CISO, or IT security manager/director) with IT security responsibilities. Another quarter are IT security administrators/operations staff, while the remainder are split almost evenly among IT security architects, auditors, and personnel identifying their position within IT security as "other."

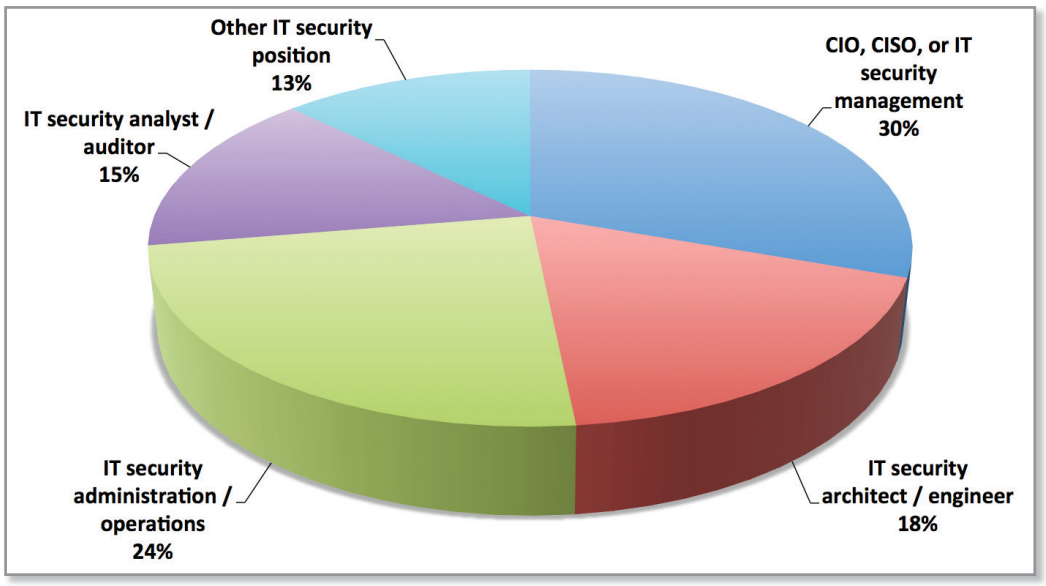

Figure 22: Survey participation by IT security role

Just over one-third of the survey respondents are from enterprises with more than 10,000 employees. The largest segment of the survey population (53%) is from organizations with between 1,000 and 10,000 employees. Only 12% of participants are from smaller organizations of between 500 and 1,000 employees.

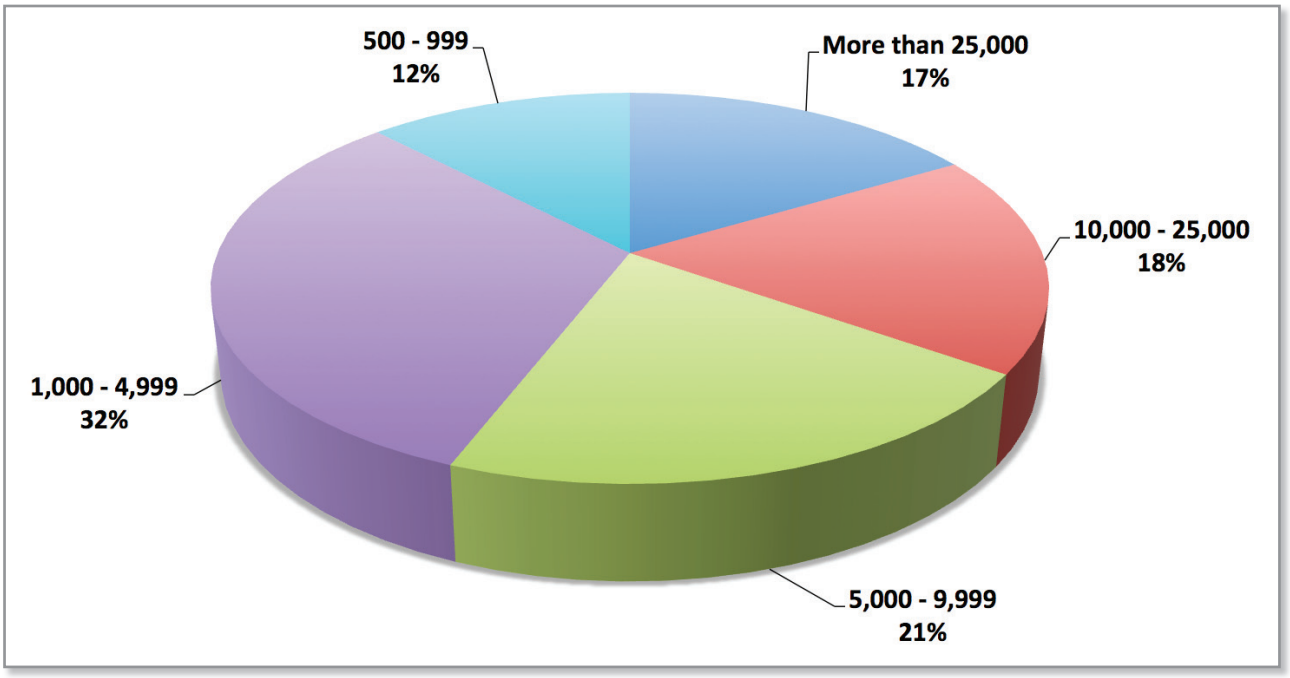

Figure 23: Survey participation by organization employee count

Distribution of survey participants by vertical industry is fairly broad, with representation across 19 industry segments. The top six segments – telecom/technology, manufacturing, education, financial services, government, and healthcare – account for nearly 70% of all respondents. No single industry accounts for more than 15% of participants.

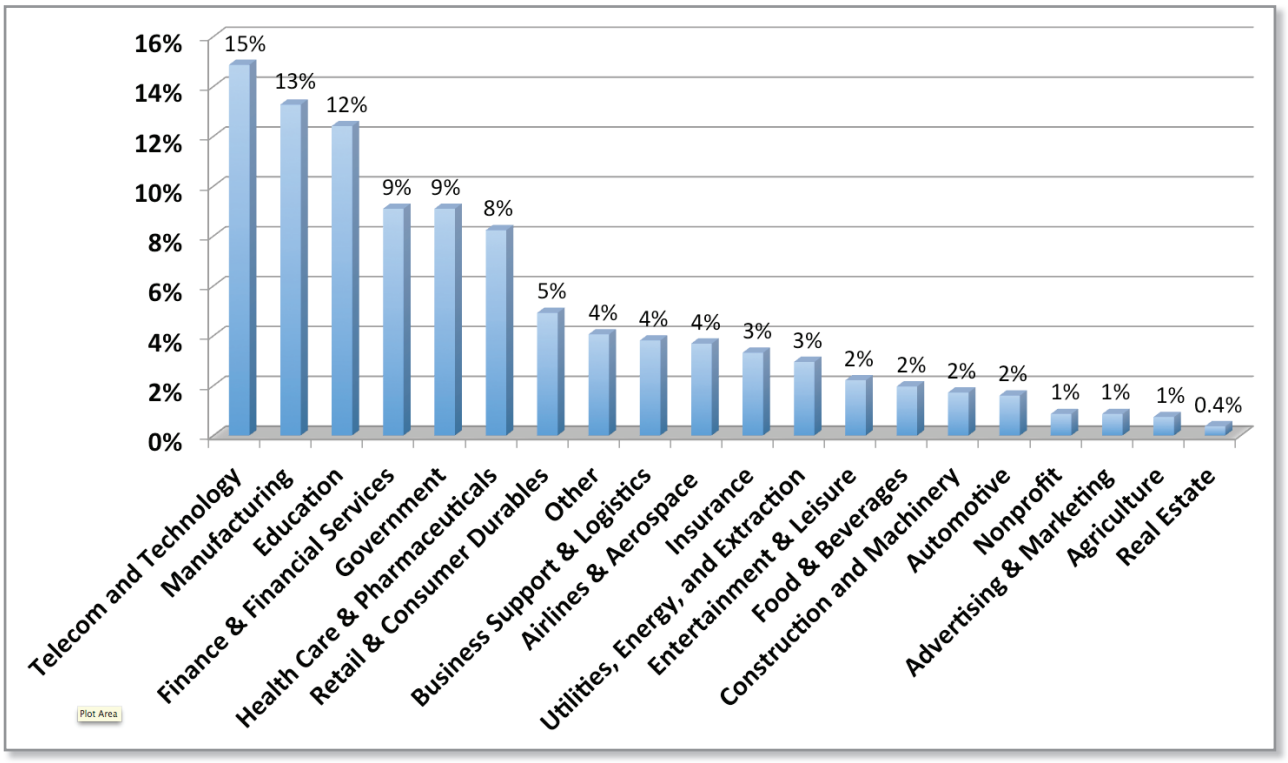

Figure 24: Survey participation by industry

Appendix 2: Research Methodology

CyberEdge Group developed a 27-question (10-15 minute) web-based survey instrument in partnership with its sponsoring vendors. The survey was promoted to information security professionals across North America and Europe in December 2014 through multiple IT security media outlets. Amazon.com gift certificate incentives were offered to the first 100 qualified participants to complete the survey in full.

Non-qualified survey responses from non-IT security professionals and from participants employed by an organization with fewer than 500 global employees were discarded. Most survey questions (aside from demographic questions) included a "Don't know" choice to minimize the potential for respondents to answer questions outside of their respective domains of expertise.

All qualified survey responses were inspected for potential survey "cheaters," meaning survey takers that responded to questions in a consistent pattern (e.g., all "A" responses, A-B-C-A-B-C responses) in an attempt to complete the survey quickly in hopes of receiving the survey incentive. Suspected cheater survey responses were deleted from the pool of responses.

The sample size ("n") for each set of survey question responses varied for multiple reasons. In all instances, "Don't know" responses were excluded from analysis. In some instances, survey takers completed a portion of the survey but then dropped off prior to completion.

Appendix 3: About CyberEdge Group

CyberEdge Group is an award-winning research, marketing, and publishing firm serving the needs of information security vendors and service providers. Our highly experienced consultants have in-depth technical expertise in dozens of IT security technologies, including:

- ☑ Advanced Threat Protection (ATP)
- ☑ Application Security
- ☑ DoS/DDoS Protection
- ☑ Endpoint Security
- ☑ Intrusion Prevention Systems (IPS)
- ☑ Managed Security Services Providers (MSSPs)
- ☑ Mobile Device Management (MDM)
- ☑ Network Behavior Analysis (NBA)
- ☑ Security Analytics / Network Forensics
- ☑ Next-generation Firewall (NGFW)
- ☑ Patch Management
- ☑ Penetration Testing
- ☑ Privileged Identity Management (PIM)
- ☑ Secure Email Gateway (SEG)
- ☑ Secure Web Gateway (SWG)
- ☑ Security Configuration Management (SCM)
- ☑ Security Information & Event Management (SIEM)
- ☑ Virtualization & Cloud Security
- ☑ Vulnerability Management (VM)

For more information on CyberEdge Group and our services, call us at 800-327-8711, email us at info@cyber-edge.com, or connect to our website at www.cyber-edge.com.

CYBEREDGE GROUP

www.cyber-edge.com

info@cyber-edge.com

800.327.8711

@CyberEdgeGroup