2017 Cyberthreat Defense Report

North America
Europe
Asia Pacific
Latin America
Middle East
Africa

« Research Sponsors »

PLATINUM

CODE42 IMPERVA SecureWorks Symantec

GOLD

bitglass exabeam Hewlett Packard Enterprise WEBROOT

SILVER

ENDGAME. foxtechnologies. illusive Soliton sumologic

Table of Contents

Introduction

The first three installments of the Cyberthreat Defense Report (CDR) began the process of looking beyond major breaches and the never-ending evolution of cyberthreats to better understand what IT security teams are doing to defend against them. Let's face it. We all know that ransomware ran rampant in 2016. More valuable to most IT security professionals than the intimate details of the next variant to emerge on the scene are the tactics and technologies other organizations are using to defend against it.

Highlights of what we learned from earlier editions of the CDR include:

- One in four security professionals doubts their organization has invested adequately in cyberthreat defenses (2014).
- Mobile devices and social media applications are IT security's "weakest links" (2015).
- Nearly nine out of 10 organizations are looking to replace or augment their endpoint security tools (2016).

The fourth annual CDR pursues the same objective: not so much to inform the IT security community about what the bad guys are up to (Verizon does a great job there), but rather to relay how their peers globally are currently defending against threats and the investments they expect to make going forward. Based on a rigorous survey of IT security decision makers and practitioners – across not only North America, Europe, Asia Pacific, and Latin America, but for the first time, the Middle East and Africa as well – the CDR examines current and planned deployment of countermeasures against the backdrop of numerous issues and concerns, such as:

- The adequacy of existing cybersecurity investments, both overall and within specific domains of IT
- The likelihood of being compromised by a successful cyberattack
- The types of cyberthreats that pose the greatest risk to organizations today
- The organizational factors that present the most significant barriers to establishing effective cyberthreat defenses
- The operational, tactical, and strategic value that individual security technologies provide

SURVEY DEMOGRAPHICS:

- **Responses from 1,100 qualified IT security decision makers and practitioners**
- **All from organizations with more than 500 employees**
- **Representing 15 countries across North America, Europe, Asia Pacific, the Middle East, Latin America, and Africa**
- **Representing 19 industries**

By revealing these details, we hope to help IT security decision makers gain a better understanding of how their perceptions, concerns, priorities, and defenses stack up against those of other IT security professionals and their organizations. Applied constructively, the data, analyses, and findings covered here can be used by diligent IT security teams to shape answers to many important 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 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? And what about our investments in other/newer areas that are becoming increasingly important, such as providing adequate data protection for cloud applications, leveraging deception technologies to derail advanced threats, and using cyber insurance to address residual risk?
- How does our level of spending on IT security compare to that of other organizations?
- 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?

Introduction

Another important objective of the CDR is to provide developers of IT security technologies and services with information they can use to better align their solutions with the concerns and requirements of potential customers. The net result should be better market traction and success for solution providers that are paying attention, along with better cyberthreat protection technologies for all the intrepid defenders out there.

The findings of this report are divided into four sections:

Section 1: Current Security Posture

The security foundation an organization currently has in place and the perception of how well it is working invariably shape future decisions about cyberthreat defenses, such as:

- Whether, to what extent, and how urgently changes are needed; and
- 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 respondents' perceived effectiveness of their organization's investments and strategies relative to the prevailing threat landscape.

Section 2: Perceptions and Concerns

In this section, our exploration of cyberthreat defenses shifts from establishing baseline security postures to determining the types of cyberthreats and other obstacles to security that concern today's organizations the most. Like the perceived weaknesses identified in the previous section, these concerns serve as an important indicator of where and how organizations can best improve their cyberthreat defenses going forward.

Section 3: Current and Future Investments

Organizations can ill afford to stand still when it comes to maintaining effective cyberthreat defenses. IT security teams must keep pace with the changes occurring around them – whether to the business, technology, or threat landscapes – by making changes of their own.

With respondents' perceptions of the threat landscape and the effectiveness of their organization's defenses as a backdrop, this section sheds light not only on the security technologies organizations currently have in place, but also on the investments they plan to make over the coming year.

Section 4: Practices and Strategies

Establishing effective cybersecurity defenses requires more than simply implementing next-generation technologies designed to detect the latest wave of elusive cyberthreats. In fact, given that most breaches today result from threat actors' exploiting known vulnerabilities or configuration weaknesses, a more sensible strategy may be to reduce one's attack surface first, and then use an overlapping set of detection-focused countermeasures to mitigate the residual risk.

In this final section of findings, we first look at the technologies organizations are leveraging to reduce their attack surfaces. Our microscope then turns to implementation details and the reasons for investing in certain security technologies, along with strategies organizations are employing to address the persistent shortage of skilled IT security personnel.

Research Highlights

Current Security Posture

- **Rising attacks.** Nearly four in five respondents' organizations were affected by a successful cyberattack in 2016, with a full third being breached six or more times in the span of a year (page 6).
- **Optimism reigns.** More than a third of respondents consider it unlikely their organization will be the victim of a successful cyberattack in 2017 (page 7).
- **Mobile devices weakest tech component.** For the fourth consecutive year, mobile devices are perceived as IT security's weakest link, closely followed by other end-user computing devices (page 8).
- **Developing secure apps weakest process.** Secure application development and testing is the security process organizations struggle with the most, followed by user awareness training (page 9).
- **Failure to monitor privileged users.** Only a third of respondents are confident their organization has made adequate investments to monitor the activities of privileged users (page 10).
- **Patch management woes.** Less than a third of respondents are confident their organization's patch management program effectively mitigates the risk of exploit-based malware (page 11).
- **Cyber insurance pulling its weight.** Three-quarters of respondents rate their organization's level of investment in cyber insurance as adequate (page 12).

Perceptions and Concerns

- **Threats keeping us up at night.** Malware, phishing, and insider threats give IT security the most headaches (page 13).
- **Ransomware's bite out of the budget.** Six in 10 respondents said their organization was affected by ransomware in 2016, with a full third electing to pay the ransom to get their data back (page 14).
- **Ransomware's biggest nightmare.** The potential for data loss is the greatest concern stemming from ransomware, while the potential for revenue loss trails the field (page 15).
- **Microsoft leaving the door open?** With two-thirds of respondents not fully satisfied with Microsoft's security measures for Office 365, the door remains open for third-party security solutions (page 16).
- **Employees still to blame.** Low security awareness among employees continues to be the greatest inhibitor to defending against cyberthreats, followed closely by a shortage of skilled personnel and too much data for IT security teams to analyze (page 17).

Current and Future Investments

- **Security budgets still rising.** Despite stabilizing as a percentage of organizations' overall IT budgets, nearly three-quarters of IT security budgets are expected to rise (again) in 2017 (pages 19 and 25).
- **Must-have network security investments.** Network deception solutions are the top-ranked network security technology planned for acquisition in 2017, followed by next-generation firewalls and user and entity behavior analytics (page 20).
- **Shielding endpoints from cyberthreats.** Containerization/micro-virtualization tops the rankings for both endpoint security and mobile security technologies that respondents plan to acquire in 2017 (pages 22 and 23).
- **Application security testing gaining traction.** Database firewalls may currently be the most widely deployed app/data security technology, but application security testing tools top the most wanted list for 2017 (page 24).

Practices and Strategies

- **NAC's reign continues.** Network access control (NAC) remains the top technology for reducing a network's attack surface (page 26).
- **Dumping security data.** While 96% of respondents collect at least some full-packet network traffic data to support their security efforts, nearly three-quarters ditch it within four weeks (page 27).
- **Leveraging CASBs to protect sensitive data.** Preventing disclosure of sensitive data is the leading reason why organizations are deploying cloud access security brokers (page 30).
- **Identity/credential thieves in crosshairs.** Thwarting account hijacking is the top use case for organizations deploying user and entity behavior analytics, followed closely by detecting data exfiltration (page 29).
- **Cybersecurity skills shortage crisis.** An astounding nine out of 10 respondents indicated their organization is suffering from the global shortfall of skilled IT security personnel (page 31).

Section 1: Current Security Posture

Past Frequency of Successful Cyberattacks

How many times do you estimate that your organization's global network has been compromised by a successful cyberattack within the past 12 months? (n=1,042)

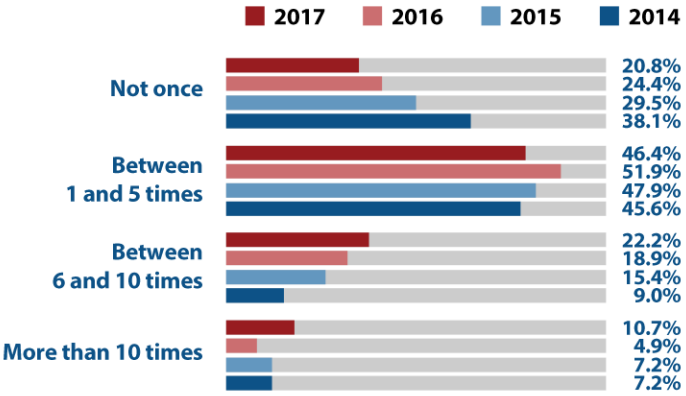


Figure 1: Frequency of successful attacks in the past 12 months.

"The bad (but not surprising) news from our respondents is that they're back to losing ground on this front..."

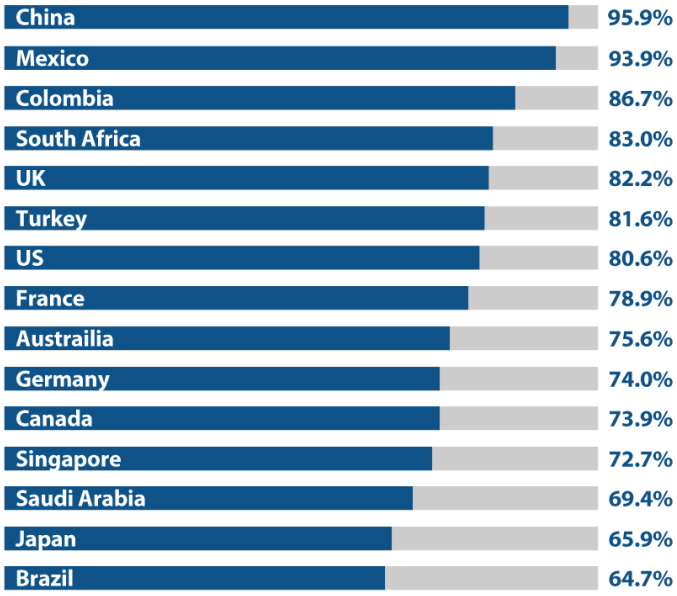


Figure 2: Percentage compromised by at least one successful attack in the past 12 months.

The number of successful cyberattacks that organizations suffer is not only a reflection of the prevailing threat landscape, but also an indicator of the effectiveness of the defenses they currently have in place.

The bad (but not surprising) news from our respondents is that they're back to losing ground on this front (see Figure 1). After holding relatively steady from 2015 to 2016 at approximately 23%, the percentage of respondents hit by six or more successful attacks in the past year jumped nearly 10 points, to 32.9%. All-time highs were also reached for those being victimized "more than 10 times" (10.7%) and at least once (79.2%).

Digging a bit deeper into the data, we can also report that Brazilian organizations are faring the best in two areas: they were most likely to avoid falling victim to a cyberattack even once (35.3%) and least likely (2.9%) to be hit more than 10 times (see Figure 2). A related side note: often portrayed as the greatest source of cyberattacks, China also looks to be the greatest victim – at least according to our data, which shows a whopping 95.9% of Chinese respondents' organizations being hit by at least one successful cyberattack in 2016.

In addition, larger organizations (> 10,000 employees) were hit "6 times or more" at more than twice the rate of their smaller counterparts. This is not particularly surprising when you consider that larger organizations are likely to have a substantially greater attack surface to defend – not to mention the widely accepted perception of being "juicier" targets.

Future Likelihood of Successful Cyberattacks

What is the likelihood that your organization's network will become compromised by a successful cyberattack in 2017? (n=1,056)

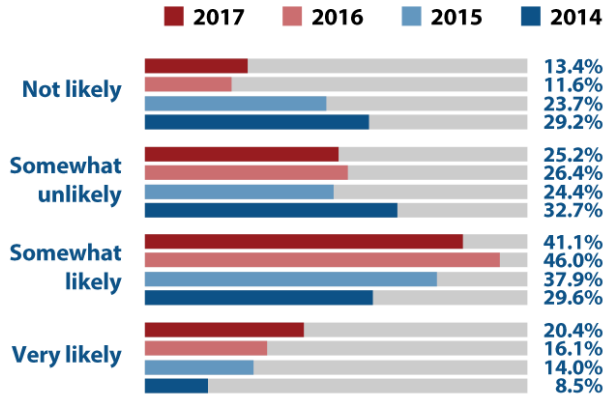


Figure 3: Likelihood of being successfully attacked in the next 12 months.

"When asked about the likelihood that their organization's network would be compromised in the coming year, respondents were, for the fourth year in a row, more optimistic than would seem warranted."

When asked about the likelihood that their organization's network would be compromised in the coming year, respondents were, for the fourth year in a row, more optimistic than would seem warranted. Despite nearly 80% indicating their organization's computing environment had been compromised within the past year (see Figure 1), only 61.5% considered it "somewhat likely" or "very likely" that it would happen again over the next 12 months (see Figure 3).

Although the degree of optimism grew a bit over last year – with a gap of 18.5% this year compared to 13.5% for 2016 – overall, the year-over-year data is a close match across the board. Even the percentage of respondents considering it "not likely" that their organization will be breached in the coming year held fairly steady, with only a slight increase from 11.6% in 2016 to 13.4% for 2017.

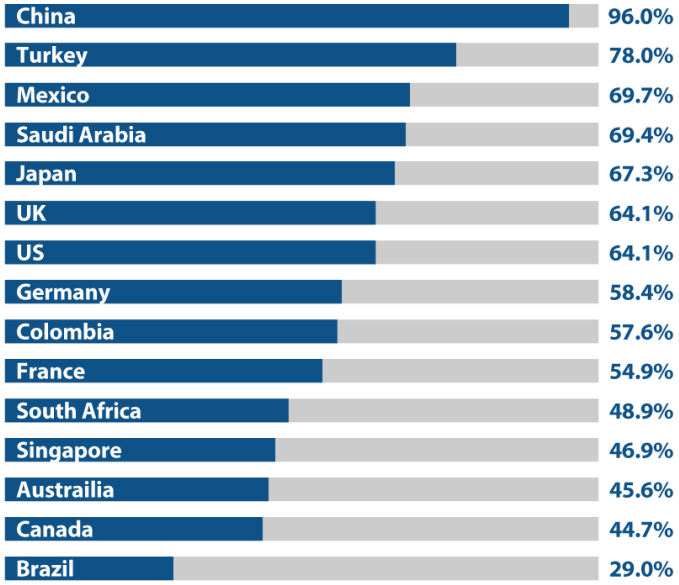


Figure 4: Percentage indicating compromise is "more likely to occur than not" in the next 12 months.

Geographically, the optimism bandwagon – those with the lowest percentages of respondents considering it more likely than not that their organization will be compromised in the coming year – was led by Brazil (29.0%), Canada (44.7%), and Australia (45.6%). On the other hand, China (96.0%) and Turkey (78.0%) were the flag bearers for what we refer to as the "realist camp" (see Figure 4).

A closing remark on this topic: we have absolutely no explanation for why respondents in the government (39.1%) and health care (49.2%) verticals are so optimistic in this regard, but we're glad they've finally found something to be (relatively) happy about.

Section 1: Current Security Posture

Security Posture by IT Domain

On a scale of 1 to 5, with 5 being highest, rate your organization's overall security posture (ability to defend against cyberthreats) in each of the following IT components: (n=1,088)

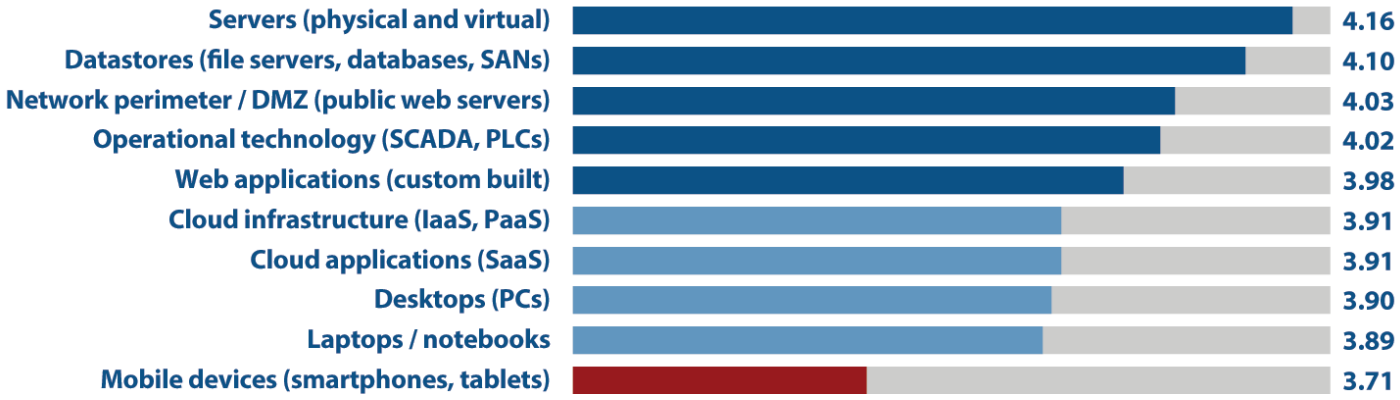


Figure 5: Perceived security posture by IT domain.

Data on the perceived ability to defend against cyberthreats in different IT domains (see Figure 5) helps inform priorities for future spending on security technology and services.

While respondents expressed relatively high confidence in their defenses for both physical and virtual servers, our results found client devices of all types – but especially mobile devices –present the greatest security challenge to today's organizations. This result makes perfectly good sense to us: IT can be expected to be better at securing resources over which it has greater control (e.g., servers) than those it does not (e.g., mobile devices).

Other findings of interest:

- Respondents are relatively confident in their organization's defensive capabilities for both data storage systems and operational technology (e.g., networked process controllers).
- There is only a small difference in the perceived security posture for homegrown web applications compared to cloud-sourced applications (SaaS).
- 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).

"...our results found client devices of all types – but especially mobile devices –present the greatest security challenge to today's organizations."

In addition, it would be remiss of us not to mention that the findings from this year were nearly identical to those from last year – well, sort of. To clarify, while the order in which the different IT domains are ranked is virtually unchanged from last year – with only the entries for web and cloud applications flip-flopping – the weighted scores received by each domain are, in fact, notably different. For the second year in a row, these scores jumped across the board, this time by an average of more than 0.13.

We know, we know; that's not really much of a gain. But this is security, after all. We need to take our gains wherever we can get them! Now if we could just turn the tide on that pesky percentage of respondents' organizations having been breached in the past year.

Section 1: Current Security Posture

Assessing IT Security Functions

On a scale of 1 to 5, with 5 being highest, rate the adequacy of your organization's capabilities (people and processes) in each of the following functional areas of IT security: (n=1,086)

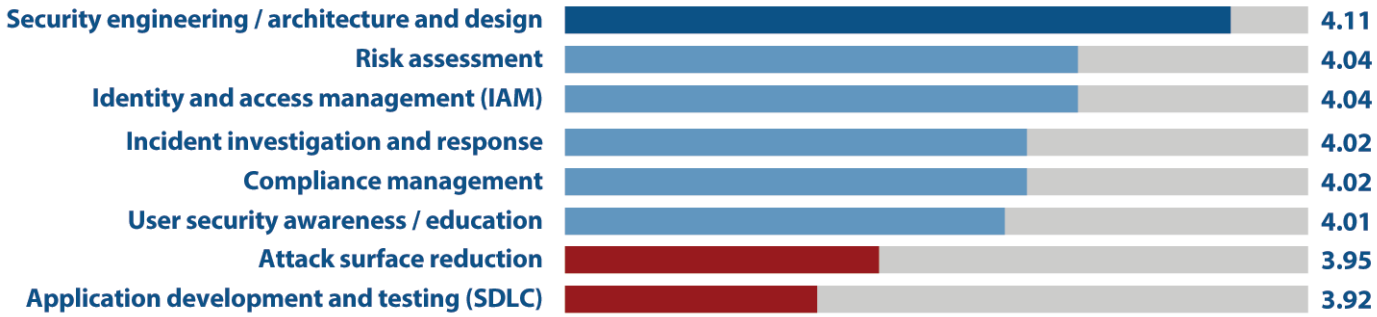


Figure 6: Perceived adequacy of functional security capabilities.

As any security professional worth her salt knows, technological countermeasures are only one piece of the puzzle when it comes to establishing effective defenses. People and processes are important, too. Accordingly, this year, we decided to explore the softer, non-technical aspects of the security equation.

"...Surprising to us is the level of confidence expressed across the board..."

Weighted scores of respondents' perceived adequacy of their organization's capabilities for some of the most significant functional areas of IT security are shown in Figure 6. Surprising to us is the level of confidence expressed across the board, as reflected by the 4.01 average weighted score for all areas, or, in other words, "mainly adequate."

Far less surprising is the appearance of user education/awareness and secure application development/testing at the bottom of the rankings. The former is consistent with the later finding of users being the greatest inhibitor to achieving effective defenses (see Figure 16), while the latter is symptomatic of the long-standing struggle of "security" to gain a seat at the application development table.

Section 1: Current Security Posture

Monitoring Capabilities for Privileged Users

Describe your agreement with the following statement: "My organization has invested adequately in privileged account/access management (PAM) technology to monitor activiites of users with elevated or privileged access rights." (n=1,089)

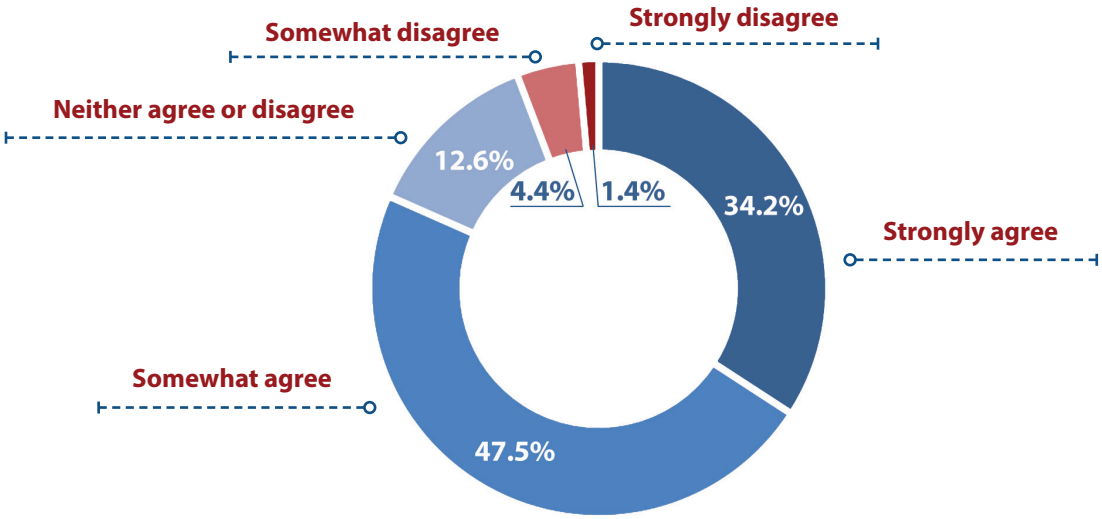


Figure 7: Adequacy of privileged user monitoring.

Participants were asked to indicate whether they believe their organization has invested adequately in technology to monitor activities of users with elevated or privileged access rights (i.e., privileged users). At the same time that only one-third (34.2%) of respondents are confident regarding their organization's ability to monitor privileged users, it's encouraging to see that only 5.8% feel their organization is negligent in this critically important area (see Figure 7). But therein lies the rub, too. This is a critical area, period.

With privileged accounts, we're quite literally talking about having access to the keys to the kingdom: the ability to take down application servers and networks, gain access to reams of sensitive data, or surreptitiously plant malcode on any device in the computing environment. And it's not just a rogue privileged user from within your ranks whom you need to worry about, but also any threat actor who manages to obtain credentials to one or more privileged accounts. So, is it really a good thing that nearly half of our respondents (47.5%) only "somewhat agree" their organization has made adequate investments in monitoring privileged users? Suffice it to say, in our opinion, there's still plenty of room for improvement.

"...it's encouraging to see that only 5.8% feel their organization is negligent in this critically important area..."

Other notable findings:

- With approximately half of the respondents from each country expressing confidence in their organization's investments in this crucial area, Mexico (51.5%), Colombia (48.1%), and Brazil (47.1%) were revealed as relative hotbeds for privileged account/access management. In contrast, Singapore (16.3%), France (21.6%), and Japan (22.9%) were exposed as relative weak spots.
- Government (33.8%) and education (27.0%) had the highest rates of respondents with neutral or unfavorable perceptions of their organization's investments in this area, while finance (10.9%) had the lowest.
- The perceived adequacy of privileged account management investments tracked upward with size of organization (as measured by employee count).

Patch Management Capabilities

Describe your agreement with the following statement: "My organization's patch management program adequately mitigates risks associated with exploit-based malware." (n=1,080)

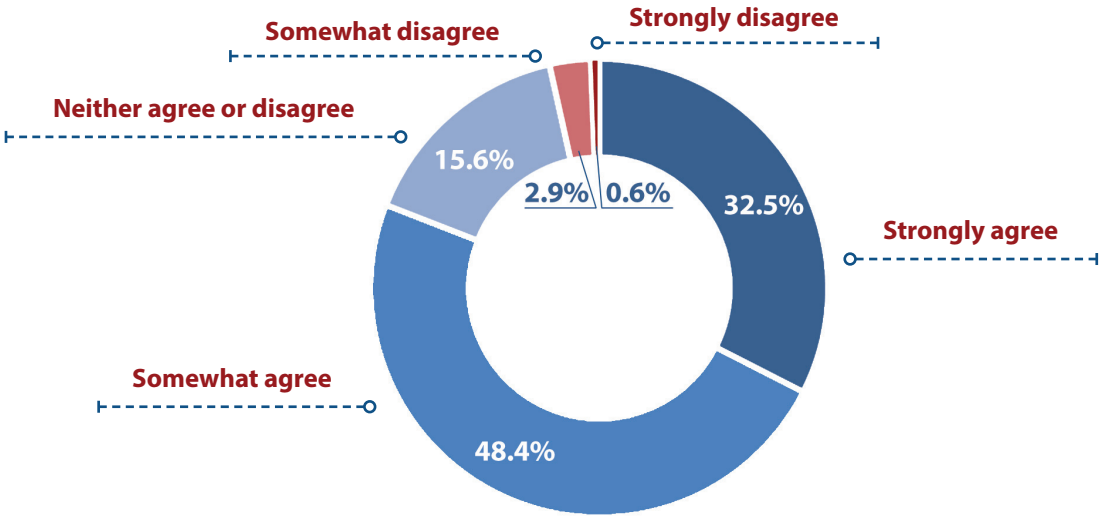


Figure 8: Adequacy of patch management program.

Having an effective patch management program is a surefire way to reduce an organization's exposure to malware and other types of cyberthreats targeting software vulnerabilities. So, what did we find when we asked participants about the adequacy of their organization's efforts in this important area?

Taking a quick glance at Figure 8, it's easy to jump to the conclusion that everything's pretty much squared away in patch management land. After all, more than four in five responded with "strongly agree" or "somewhat agree," suggesting that their organization's patch management program is relatively effective. In addition, only 3.5% responded with "somewhat disagree" or "strongly disagree," which we interpret as pointing to the presence of significant deficiencies in their organization's program.

"...nearly half of our respondents only "somewhat agree" with the adequacy of their organization's patch management program..."

But wait. If that's truly the case, then why, when we take a sneak peek ahead to Figure 10, do we see "malware" highlighted as the type of cyberthreat that most concerns responding organizations? Sure, not all malware works by exploiting vulnerabilities that a truly effective patch management program would eliminate. We suspect, however, that a bigger part of the disconnect here has to do with the nearly half of our respondents who only "somewhat agree" with the adequacy of their organization's patch management program. To us, this particular response suggests there's still plenty of room for improvement.

- Consistent with our findings for privileged account management capabilities (see Figure 7), Mexico (48.5%) and Colombia (46.9%) led the way for countries with the most respondents expressing confidence in their organization's investments in this area. In contrast, Japan (10.4%) and Singapore (16.3%) were exposed as relative weak spots (once again).
- Government (36.5%) and education (25.9%) had the highest rates of respondents with neutral or unfavorable perceptions of their organization's investments in this area, while telecom/technology (14.0%) had the lowest.

Section 1: Current Security Posture

Adequacy of Cyber Insurance Coverage

Describe your agreement with the following statement: "My organization has invested adequately in cyber insurance." (n=1,073)

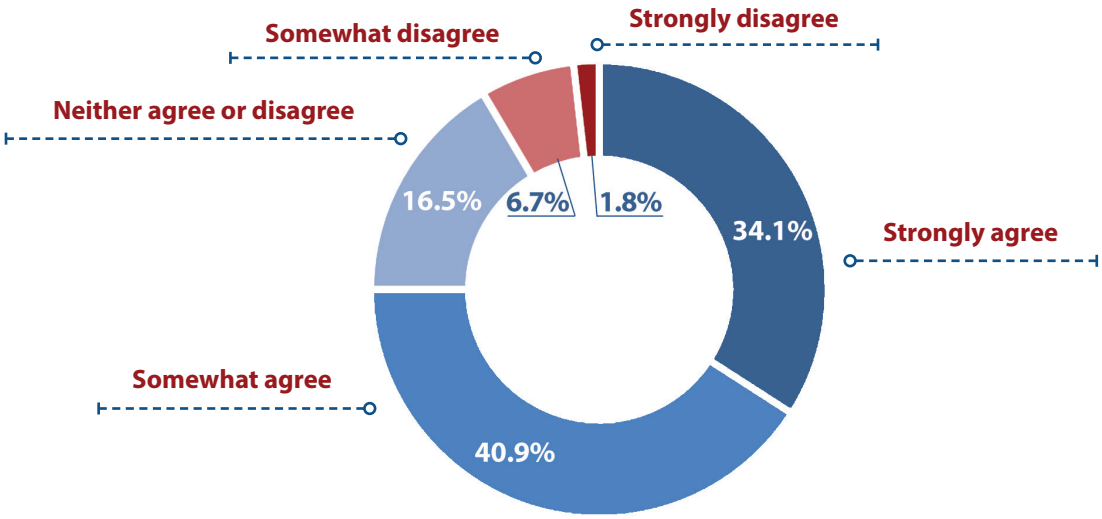


Figure 9: Adequacy of cyber insurance coverage.

To round out this first section, we introduced a new question to gain some insights into the use of cyber insurance as a mechanism to help mitigate the risks posed by cyberattacks. The general appeal of cyber insurance is certainly easy to understand. After all, breaches are becoming more likely/common (see Figure 1) at the same time that the costs related to attacks continue to rise (Ponemon Institute's 2016 Cost of Data Breach Study put the average cost of a data breach at $4 million USD, which is up 29% from 2013).

That said, with a market size of only about $2 billion in 2015, cyber insurance's use as a risk management tool is far from universal. The most common obstacles we've heard about are the strict/onerous reviews of existing policies and practices that are required to obtain coverage, combined with general uncertainty regarding overall value (i.e., cost versus adequacy of coverage and potential payouts).

"On a global basis, a full three out of four agreed with their organization's approach in this area..."

So what did our respondents think about the adequacy of their organization's investment in cyber insurance at this point? On a global basis, a full three out of four agreed with their organization's approach in this area, while less than 10% disagreed (see Figure 9).

Other notable findings:

- Geographically, Mexico (97.0%), Brazil (88.3%), and Colombia (87.9%) topped the charts for respondent agreement with their organization's cyber insurance practices, while Germany (63.5%) and France (64.8%) trailed the field.
- Government (40.6%) and education (35.5%) had the highest rates of respondents with neutral or unfavorable perceptions of their organization's investments in this area, while telecom/technology (15.5%) and finance (18.4%) had the lowest.
- The perceived adequacy of cyber insurance investments tracked steadily upward with size of organization, from a low of 73.9% for smaller outfits (500-999 employees) to a high of 87.6% for the largest ones (25,000+ employees).

The bottom line: cyber insurance is here to stay and adoption rates are only going to increase as the actuarial data involved continues to solidify.

Section 2: Perceptions and Concerns

Types of Cyberthreats

On a scale of 1 to 5, with 5 being highest, rate your overall concern for each of the following types of cyberthreats targeting your organization. (n=1,090)

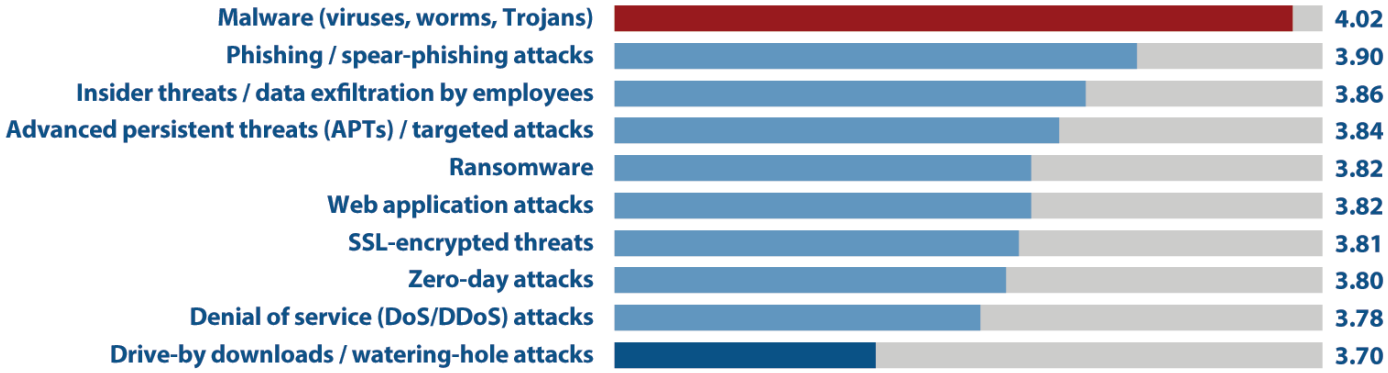


Figure 10: Relative concern by type of cyberthreat.

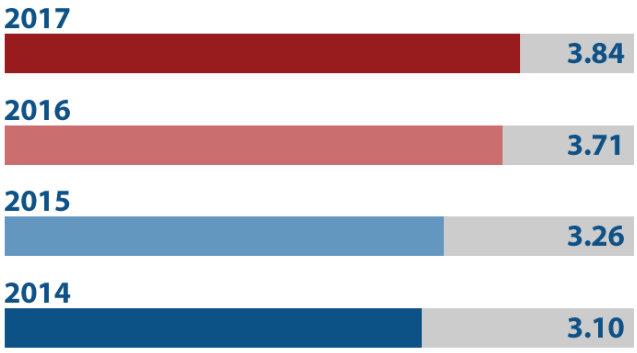


Figure 11: Average concern across all types of cyberthreats.

After a back-and-forth battle with phishing/spear phishing over the past few years, malware solidified its standing (and even pulled away a bit) as the type of cyberthreat that concerns our respondents the most (see Figure 10). Phishing/spear phishing retained its position as runner-up in this anti-beauty contest, while drive-by downloads and watering-hole attacks trailed the field once again.

Despite the overwhelming attention it has received in the press – not to mention security vendors' marketing collateral – over the past year, ransomware only ranked in the middle of the pack. This result put it behind even "insider threats / data exfiltration by employees," the other type of cyberthreat newly added to the list for this year's survey.

"...malware solidified its standing (and even pulled away a bit) as the type of cyberthreat that concerns our respondents the most..."

Two additional observations:

- The level of concern grew across the board, with the weighted scores for all types of cyberthreats increasing year over year. This result is reflected in our newly created Threat Concern Index, which shows a continuing rise in the average (weighted) concern expressed about all types of cyberthreats from our inaugural CDR in 2014 to the current one (see Figure 11).
- The total span of the weighted scores was its lowest yet (0.32), reinforcing last year's supposition that to many respondents, a "threat is a threat" – all types warrant concern and, presumably, attention.

Section 2: Perceptions and Concerns

Ransomware's Pain Points

Which of the following potential impacts of ransomware concerns your organization the most? (Select one.) (n=1,083)

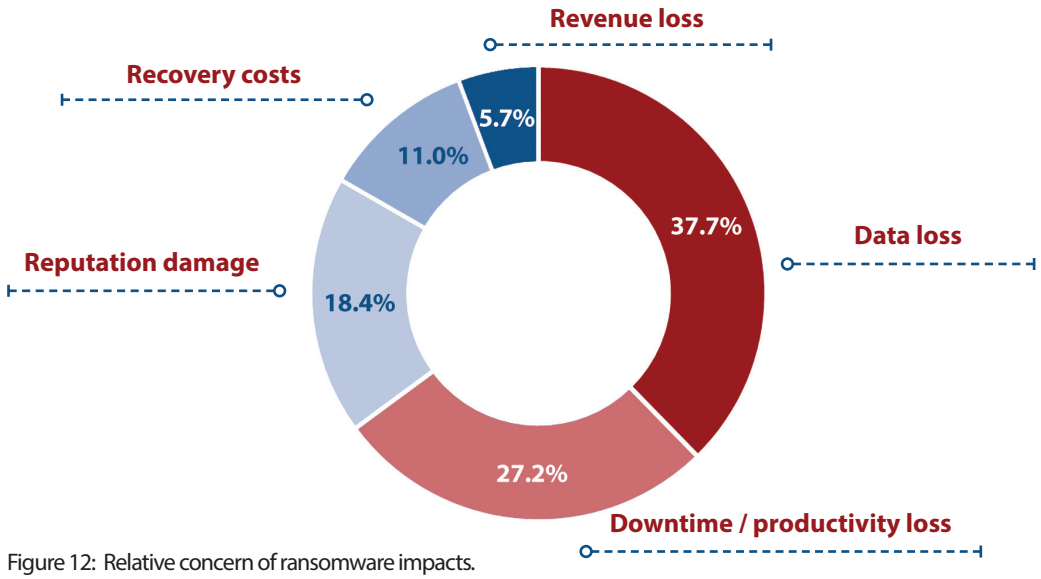


Figure 12: Relative concern of ransomware impacts.

To say that ransomware – especially the crypto variety – has morphed from a mildly annoying consumer-centric affliction to a top concern for businesses of all types and sizes would, perhaps, be an understatement. Just ask the management teams at Hollywood Presbyterian Medical Center (California), Methodist Hospital (Kentucky), MedStar Health (Maryland), or the University of Calgary (Canada), all of which had their operations tied in knots by ransomware at least once in 2016. Or ask the FBI, which after tallying $209 million in ransomware payments over the first quarter of 2016, projected total losses stemming from ransomware would exceed $1 billion for the year (source: http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/).

So, what is it about ransomware that concerns organizations the most? What are the potential impacts that worry respondents, and, therefore, are likely to have the greatest influence on the tactics and technologies they select to defend against this growing plague? We're glad you asked. Receiving more than a third of the vote, "data loss" (37.7%) outstripped its nearest competitor, "downtime / productivity loss" (27.2%), by a healthy margin (see Figure 12). This left "reputation damage" (18.4%), "recovery costs" (11.0%), and "lost revenue" (5.7%) trailing behind. Somewhat surprising to us, at least on the surface, these results demonstrate the extent to which businesses now acknowledge the modern reality that data is, in fact, money!

"...these results demonstrate the extent to which businesses now acknowledge the modern reality that data is, in fact, money!"

Other notable findings:

- For U.S. respondents, "data loss" (30.1%) and "downtime / productivity loss" (30.7%) are essentially tied as the greatest concern.
- For German (41.7%) and Australian (30.0%) respondents, "downtime / productivity loss" is, by a significant margin, the greatest concern.
- Somewhat predictably, "downtime / productivity loss" topped the charts for the manufacturing (35.9%) and retail sectors (35.0%), while "data loss" was the runaway leader for health care (54.8%).

Responding to Ransomware

If victimized by ransomware in the past 12 months, did your organization pay a ransom (using Bitcoins or other anonymous currency) to recover data? (n=1,085)

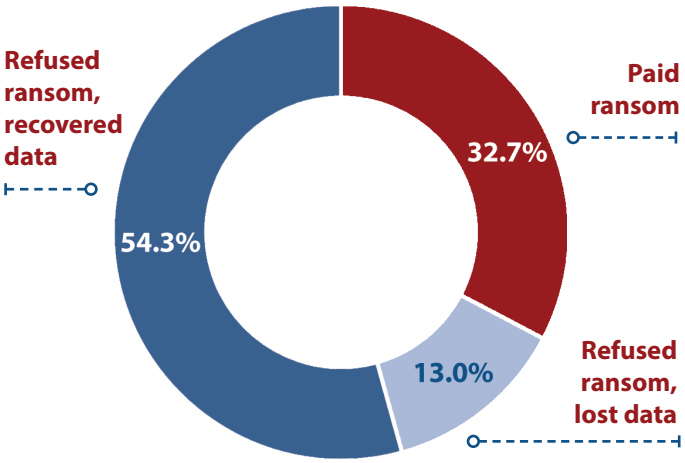


Figure 13: How victims responded to ransomware.

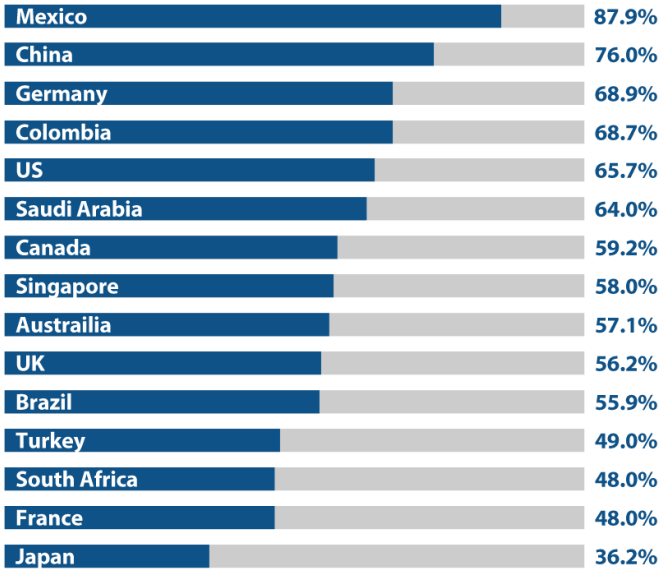


Figure 14: Percentage affected by ransomware in the past 12 months.

Just like every class of threat that came before it, ransomware is evolving. At the same time that the emergence of ransomware-as-a-service is making it extremely easy to perpetrate attacks, we're also seeing an explosion of new "features" designed to increase damage and accelerate the need for response. Variants that randomly (and permanently) delete encrypted files and target executables are just two examples. It's only a matter of time, too, before self-propagation becomes a common characteristic and the scope of systems being targeted expands to include medical, industrial control, and Internet of Things devices.

The continuing evolution of ransomware will clearly have an impact on who's being hit, how often, and how organizations elect to respond. For now, though, our data indicates that a whopping 61% of organizations were affected by ransomware in 2016. Of those affected, the majority (54.3%) recovered their data without paying a ransom (see Figure 13), presumably through data backups. Nearly a third (32.7%) paid the ransom to recover their data while 13% refused the ransom and lost their data.

Geographically, Mexican (87.9%) and Chinese (76.0%) organizations had the highest hit rates, while their French (48.0%) and Japanese (36.2%) counterparts experienced the lowest frequency of ransomware attacks (see Figure 14).

"...our data indicates that a whopping 61% of organizations were affected by ransomware in 2016..."

Other notable findings:

- The countries whose organizations most often paid the ransom were Colombia (59.1%), Mexico (51.8%), and the United States (44.8%), while those paying least often were from Turkey (0%) and Singapore (13.8%).
- The vertical industries hit the hardest by ransomware were telecom/technology (71.2%) and finance (68.2%), while those impacted the least were government (25.7%) and – somewhat surprisingly given the frequency of news stories that suggest otherwise – health care (45.0%).

Section 2: Perceptions and Concerns

Microsoft Office 365 Security Perceptions

Describe your agreement with the following statement: "I am satisfied with the security measures offered by Microsoft to secure our Office 365 deployment." (n=1,091)

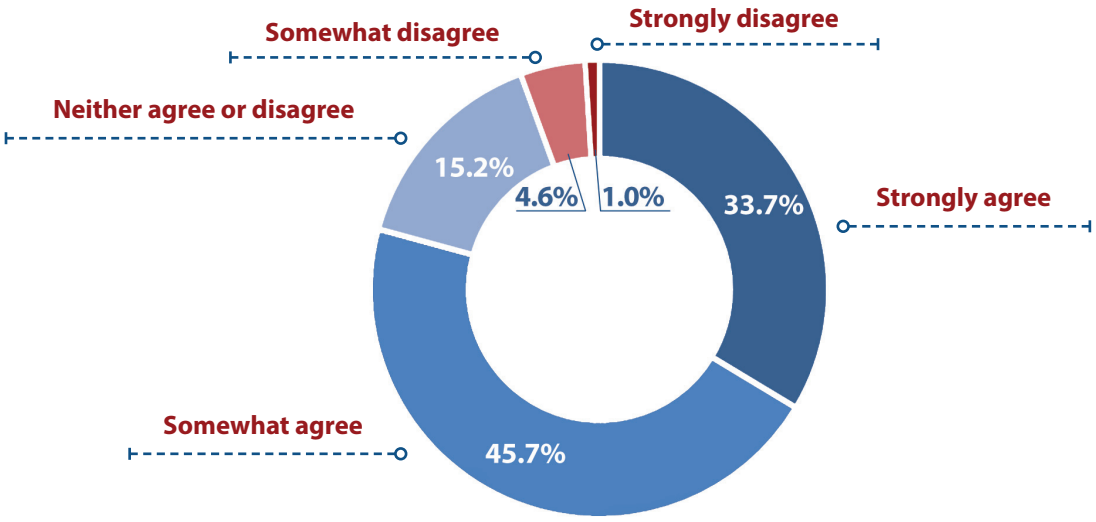


Figure 15: Satisfaction with Microsoft Office 365 security.

Let's face it, Microsoft gets a lot of things right, but security hasn't always been one of them. Microsoft Windows is a good case in point. Although the situation has improved significantly over the past decade or so, for a long while Windows was both the most popular desktop OS (based on adoption rates), but also the one most maligned from a security perspective (due to the frequency and severity of associated vulnerabilities).

That track record led us to explore how Microsoft is faring security-wise with its latest home run, Office 365. The answer: so-so. Although one third of respondents indicated they "strongly agree" with the statement "I am satisfied with the security measures offered by Microsoft to secure our Office 365 deployment," that leaves a clear majority that feel otherwise (see Figure 15).

To us, this signals that there's still plenty of room for improvement, and, therefore, for third-party providers of alternate/add-on security solutions. In fact, third-party security solutions may even be a wiser choice in some scenarios – such as when an organization requires coverage across a broader portfolio of cloud applications/assets (as opposed to just those available from Microsoft), or when the nature of the capabilities in question is more appropriately delivered by an external party (think audit and compliance assessments).

"To us, this signals that there's still plenty of room for improvement..."

A few other wrinkles from the demographic breakdowns:

- Satisfaction with Microsoft's security measures for Office 365 – as measured by the combination of "strongly agree" and "somewhat agree" responses – is lowest in Japan (44.9%). Germany (64.9%) was the only other country where less than two-thirds of respondents were generally satisfied in this regard.
- Government respondents (61.0%) had the lowest satisfaction level, while telecom/technology respondents (80.5%) had the highest.
- Only 68.6% of smaller organizations (500-999 employees) were generally satisfied with Microsoft's security measures for Office 365, compared to an average of 77.9% for all larger organizations (1,000 or more employees).

Section 2: Perceptions and Concerns

Barriers to Establishing Effective Defenses

On a scale of 1 to 5, with 5 being highest, rate how each of the following inhibit your organization from adequately defending itself against cyberthreats. (n=1,087)

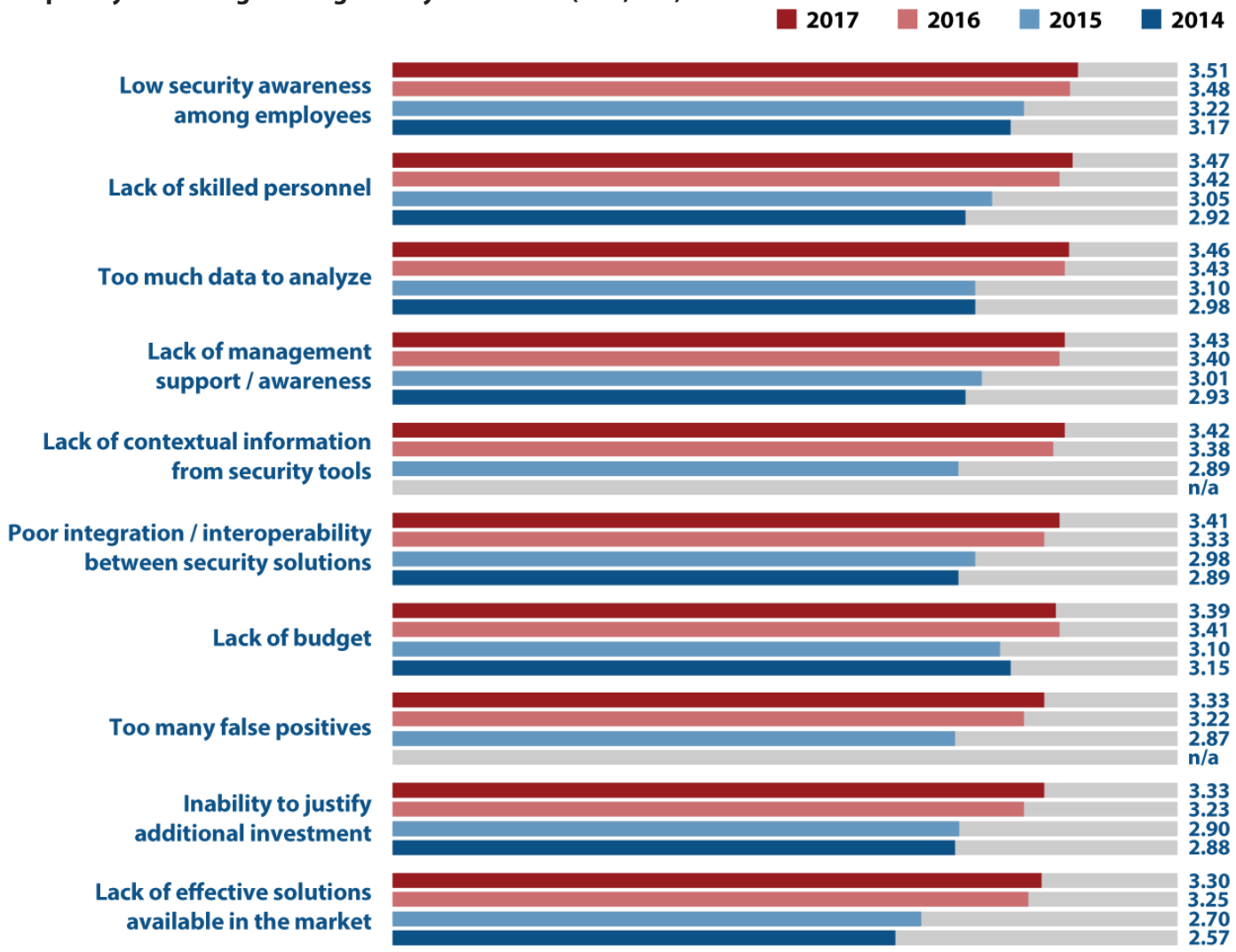


Figure 16: Inhibitors to establishing effective cyberthreat defenses.

Establishing effective cyberthreat defenses is not easy. If it were, there would be far fewer successful cyberattacks and greater confidence on the part of IT security practitioners (see Figures 1 and 3, respectively). Part of the issue is the ever-evolving threat landscape, along with the nature of "playing defense."

Today's threat actors have a seemingly endless capacity to advance their wares and only need to find a single weak spot. As defenders, however, IT security teams can only guess at hackers' next moves and must provide coverage for every single user, endpoint, server, and application within and beyond the physical walls of the datacenter. Then there are all the other obstacles that must also be overcome to achieve success (see Figure 16).

"Given the consistency of this finding, don't you think it makes sense to try investing a bit more in all of those human firewalls at your disposal?"

Section 2: Perceptions and Concerns

Once again, respondents cited users as the greatest obstacle to their organization's establishing effective defenses, as "low security awareness among employees" topped the chart for a remarkable fourth consecutive year. "Ahem … enterprise security teams, can you hear us?" Given the consistency of this finding, don't you think it makes sense to try investing a bit more in all of those human firewalls at your disposal? Call us crazy, but armed with the proper knowledge, we think they could easily flip the script, and go from being your biggest security burden to your biggest security asset.

Other notable findings:

- "Lack of skilled personnel" edged its way into second place on the list. No surprises there. This finding echoes what we've all been hearing about for years, and only serves to further validate how crucial the human component is in the "people, process, technology" triumvirate of security defenses.
- Consistent with other findings confirming that information security budgets are healthy (see Figures 17 to 20), "lack of budget" continued its slide from second place two years ago to seventh on the list this time around.
- Having "too much data to analyze" remained among the top obstacles to effective defenses (in third place), while "lack of effective solutions available in the market" was designated by our respondents as the least significant issue (of those listed) faced by today's security teams.

As for the biggest upward mover year over year, "too many false positives" holds that dubious honor, jumping two spots (and more than a tenth of rating point) into eighth position on the list.

Section 3: Current and Future Investments

IT Security Budget Allocation

What percentage of your employer's IT budget is allocated to information security (e.g., products, services, personnel)? (n=1,046)

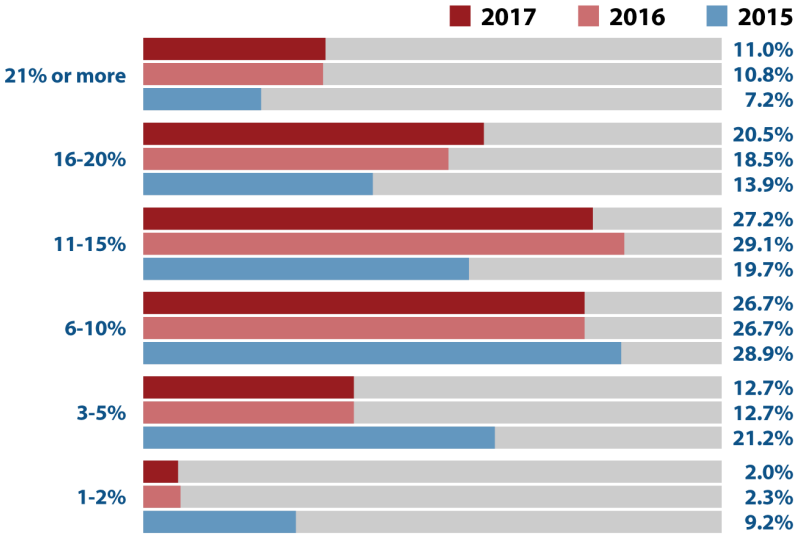


Figure 17: Percentage of IT budget allocated to security.

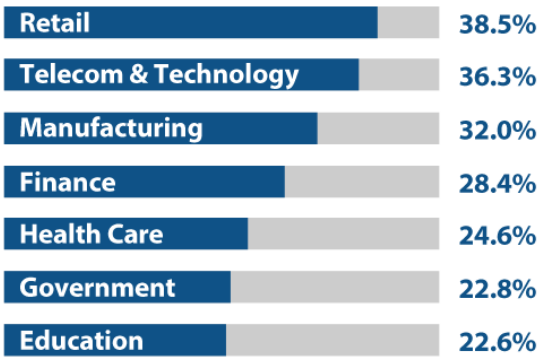


Figure 18: Percentage spending 16% or more on security.

For last year's CDR we were pleased to observe strong year-over-year growth of organizations' budgets for information security products, services, and personnel. Sorry, not this time. But before your inner Chicken Little takes over, please take a moment to consider a few points.

To begin with, IT security budgets remain quite healthy overall. A decade ago, most security teams were scraping by on something in the neighborhood of 3%-5% of the IT budget. Now, more than 85% of respondents' organizations exceed that level (see Figure 17). And nearly six out of 10 are allocating more than 10% of their IT budgets to security.

Next, we didn't say security budgets were retreating. The gains may not have been great this time around, but they were still positive. For instance, 85.3% indicated an allocation of more than 5% to security, up from 85.0% the year prior. Similarly, those spending north of 16% on security rose by 2.2 percentage points, while those spending less than 2% of their IT budgets on security declined incrementally (from 2.3% to 2.0%).

Finally, we need to keep in mind that observing constant growth in this area would be a bad thing. After all, wouldn't that be indicative of the failure of the security industry as a whole – vendors and practitioners alike – to deliver and maintain anything remotely resembling effective cyberthreat defenses?

"85.3% indicated an allocation of more than 5% to security, up from 85.0% the year prior."

Other notable findings:

- Geographically, Brazil (57.6%), South Africa (47.0%), and Colombia (40.6%) have the greatest percentage of organizations spending in excess of 16% of their IT budgets on security. This result probably reflects their attempts to catch up after historically under-investing in security relative to organizations in other countries.
- Of the "big 7 industries" (see Figure 18), it is not surprising to see education (22.6%), government (22.8%), and health care (24.6%) at the low end of the spectrum for organizations that are spending more than 16% of IT budget on security.
- The percentage of smaller organizations (< 5,000 employees) investing more than 16% of their IT budget on security increased considerably from last year (up from 19.7% to 31.3%), while the percentage of very large organizations (> 25,000 employees) investing at the same level rose only slightly, from 47.1% to 49.2%.

Section 3: Current and Future Investments

Network Security Technology Deployment Status

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=1,075)

	Currently in use	Planned for acquisition	No plans
Network-based anti-virus (AV)	67.7%	24.9%	7.4%
Advanced malware analysis / sandboxing	66.9%	24.4%	8.7%
Secure email gateway (SEG)	63.0%	26.4%	10.6%
Secure web gateway (SWG)	62.2%	26.2%	11.6%
Web application firewall (WAF)	62.0%	28.7%	9.3%
Intrusion detection / prevention system (IDS/IPS)	58.7%	29.7%	11.6%
Data loss / leak prevention (DLP)	57.2%	34.7%	8.1%
Denial of service (DoS/DDoS) prevention	56.3%	30.0%	13.7%
Security information and event management (SIEM)	54.9%	32.5%	12.6%
Security analytics / full-packet capture and analysis	52.3%	35.0%	12.7%
Privileged account / access management (PAM)	51.9%	33.2%	14.9%
Network behavior analysis (NBA) / NetFlow analysis	51.4%	34.0%	14.6%
Next-generation firewall (NGFW)	48.3%	39.2%	12.5%
Threat intelligence service	45.5%	37.1%	17.4%
User and entity behavior analytics (UEBA)	44.9%	38.3%	16.8%
Honeypots / network deception	35.6%	40.5%	23.9%

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

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, mobile, and application security technologies are addressed in subsequent sections.)

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

Our first observation is that this year's results are nearly a mirror image of those from 2016. For instance, the greatest positive change in adoption rate was +3.2% for advanced malware analysis, while the greatest negative changes were only -4.4% and -3.9%, for denial of service prevention and data loss prevention, respectively.

" ... honeypots / network deception is ... the top-rated network security technology planned for acquisition in 2017."

By the way, one potential explanation for the retreating adoption rates for these latter technologies – as well as for intrusion detection/prevention systems (-1.1%) and user behavior analytics / activity monitoring (-3.5%) – could be the

Section 3: Current and Future Investments

expansion of our survey into less "security mature" countries, or at least ones with greater diversity in this regard (such as China, Colombia, South Africa, and Turkey). Whatever the explanation, the main point is that the differences from this year to last for both current adoption and planned acquisition rates are, for all intents and purposes, negligible.

Other notable findings:

- Despite its declining rate of use, network anti-virus (AV) remains atop the heap as the most frequently deployed network security technology in our list.
- With an adoption rate nearly identical to that of network AV (67.7%), advanced malware analysis / sandboxing (66.9%) appears to have reached commodity status.
- A relatively low adoption rate for honeypots / network deception (35.6%) is offset by the fact that it's the top-rated network security technology planned for acquisition in 2017. (For more insights on this up-and-coming technology, be sure to catch "The Road Ahead" section near the end of this report.)
- Both next-generation firewalls and threat intelligence services continue to exhibit promising trajectories, with 39.2% and 37.1% of respondents signaling their intent to acquire these respective solutions in 2017.
- With multiple flavors of analysis/analytics technologies (i.e., security, network, and user behavior) and SIEM among the leaders for adoption in the coming year, it's clear that bolstering capabilities for monitoring and analyzing network traffic for the presence of cyberthreats remains a high priority for many organizations.

Our closing observation for this table is favorable for most security solution providers: with an average adoption rate hovering somewhere around 50%, there still appears to be plenty of opportunity for additional sales of many of these important – if not essential – network security technologies.

Section 3: Current and Future Investments

Endpoint Security Deployment Status

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=1,036)

	Currently in use	Planned for acquisition	No plans
Basic anti-virus / anti-malware (threat signatures)	79.8%	14.3%	5.9%
Advanced anti-virus / anti-malware (machine learning, behavior monitoring, sandboxing)	65.0%	28.9%	6.1%
Disk encryption	63.7%	24.8%	11.5%
Data loss / leak prevention (DLP)	61.8%	26.3%	11.9%
Application control (whitelist / blacklist)	59.9%	28.3%	11.8%
Digital forensics / incident resolution	50.9%	35.5%	13.6%
Self-remediation for infected endpoints	48.2%	36.6%	15.2%
Endpoint deception	47.4%	36.2%	16.4%
Containerization / micro-virtualization	40.5%	43.7%	15.8%

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

The same approach used to assess network security technologies was repeated to gain insight into deployment status and acquisition plans for endpoint security technologies (see Table 2). Once again, percentages in dark blue correspond to a higher frequency of adoption and/or acquisition plans, while percentages in light blue correspond to a lower frequency of adoption and/or acquisition plans.

Is everyone ready for a Clint Eastwood spaghetti western reference?

The good: with the exception of a minor blip for containerization / micro-virtualization solutions (-0.1%), the adoption rates for all listed endpoint security technologies increased from last year to this one.

The bad: we remain somewhat baffled by the relatively modest adoption rates for proven technologies such as application control and disk encryption. Delivering the ability to significantly reduce an organization's exposure to malware and keeping sensitive data out of harm's way, respectively, these two technologies seem like no brainers to us.

"... with the exception of a minor blip for containerization / micro-virtualization solutions (-0.1%), the adoption rates for all listed endpoint security technologies increased from last year..."

The ugly (or at least strange): With a year-over-year bump of +9.3%, basic signature-based anti-malware technology appears to have reversed its former decline in adoption (-11.5% from 2015 to 2016). Once again, we point to the expanding geographic reach of our survey as a likely explanation.

As for which endpoint security technologies organizations plan to acquire in the coming year, the data shows containerization / micro-virtualization (43.7%) leading the way, followed by endpoint self-remediation solutions (36.6%), and the new kid on the block, endpoint deception (36.2%).

Mobile Security Deployment Status

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=1,075)

	Currently in use	Planned for acquisition	No plans
Mobile device anti-virus / anti-malware	62.1%	28.7%	9.2%
Mobile device / application management (MDM/MAM)	60.7%	29.7%	9.7%
VPN to on-premises security gateway	58.2%	30.2%	11.6%
Network access control (NAC)	57.6%	31.0%	11.4%
VPN to cloud-based security gateway	55.9%	30.7%	13.4%
Mobile device file / data encryption	55.1%	30.2%	14.7%
Virtual desktop infrastructure (VDI)	52.7%	35.1%	12.2%
Containerization / micro-virtualization	44.0%	38.2%	17.8%

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

Next in our crosshairs is the mobile security landscape. Even though the deployment rate for each technology listed has either held pretty much steady or increased by a few percentage points, none is currently in use by a heavy majority of organizations. To us, this result points to: (a) a market segment that is still shaking itself out and, therefore, is fertile ground for further investment and innovation; (b) a domain where many organizations still have some work to do; and/or (c) an area where organizations are potentially leveraging multiple, overlapping solutions to get the job done.

Other notable findings from Table 3:

- As with the previous two domains (network and traditional endpoints), anti-virus/anti-malware remains atop the leader board as the most frequently deployed technology in our list (62.5%).
- With 38.2% of responding organizations signaling their intent to acquire it in the coming year, containerization / micro-virtualization consolidates the title of most sought-after endpoint and mobile security technology for 2017 (see Table 2).
- Not to be outdone, each of the other technologies listed can also boast a relatively healthy "planned for acquisition" rate. This finding – along with our respondents' identification of mobile devices as their organization's Achilles' heel (see Figure 5) – reinforces our earlier suggestion that mobile security is an area still in need of considerable attention.

"With 38.2% of responding organizations signaling their intent to acquire it in the coming year, containerization / micro-virtualization consolidates the title of most sought-after endpoint and mobile security technology for 2017..."

Of course, another potential reason for the somewhat lackluster adoption of mobile security technologies could be the perceived lack of related threats. Although we expect the situation is soon likely to change, at least for now, cyberthreats targeting mobile devices continue to be predominantly consumer oriented/focused. Further evidence supporting this point comes from the 2016 Verizon Data Breach Investigations Report, which noted an absence of significant real-world data on mobile technologies as the vector of attack on organizations.

Application and Data Security Technology Deployment Status

Which of the following application and data-centric security technologies are currently in use or planned for acquisition (within 12 months) by your organization to guard enterprise applications and associated data repositories against cyberthreats? (n=1,045)

	Currently in use	Planned for acquisition	No plans
Database firewall	65.4%	24.6%	10.0%
Web application firewall (WAF)	64.9%	25.3%	9.8%
Database encryption / tokenization	59.5%	27.8%	12.7%
Application delivery controller (ADC)	58.7%	27.9%	13.4%
Database activity monitoring (DAM)	54.2%	31.6%	14.2%
File integrity / activity monitoring (FIM/FAM)	52.2%	33.6%	14.2%
Runtime application self-protection (RASP)	52.1%	31.5%	16.4%
Application vulnerability scanner	51.4%	36.1%	12.5%
Cloud access security broker (CASB)	51.1%	32.9%	16.0%
Static/dynamic/interactive application security testing (SAST/DAST/IAST)	50.7%	36.8%	12.5%
Deception technology / distributed decoy systems	45.7%	35.2%	19.1%

Table 4: Application and data security technologies in use and planned for acquisition.

Anecdotal evidence suggests enterprises are continuing to place greater emphasis on protecting that which arguably matters most at the end of the day: sensitive data and the applications on which their businesses depend. To better understand what this suspected trend actually means for current priorities and future plans, we once again took the same approach used for network, endpoint, and mobile security technologies to delve into the all-important areas of application- and data-centric defenses (see Table 4).

Key findings:

- Database firewalls (65.4%) and web application firewalls (64.9%) continue to claim the top spots as the most widely deployed app/data security technologies.
- With the greatest year-over-year increase in adoption rate (6.3%), application delivery controllers (ADCs) are clearly recognized as having evolved beyond their load balancing and performance optimization roots to be strong app/data security platforms.
- Along with having the second-greatest increase in adoption rate (4.6%), application security testing once again emerged as the top-rated security technology planned for acquisition in the coming year, arguably making it the hottest technology in this market segment.

Our closing thought on this topic: with increased adoption rates across the board, we can safely say that enterprises are indeed focusing heavily on the areas of application and data security.

"Database firewalls (65.4%) and web application firewalls (64.9%) continue to claim the top spots as the most widely deployed app/data security technologies..."

Section 3: Current and Future Investments

IT Security Budget Change

Do you expect your employer's overall IT security budget to increase or decrease in 2017? (n=1,074)

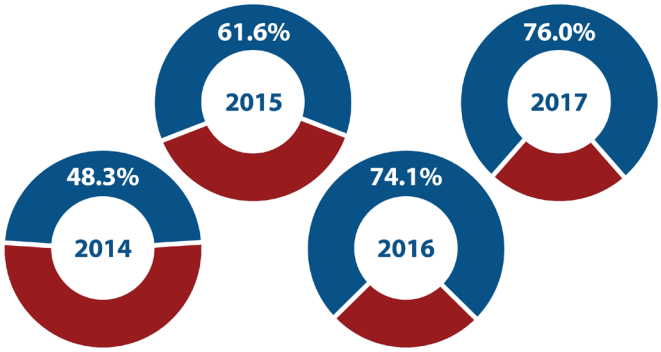


Figure 19: Percentage indicating security budget is growing.

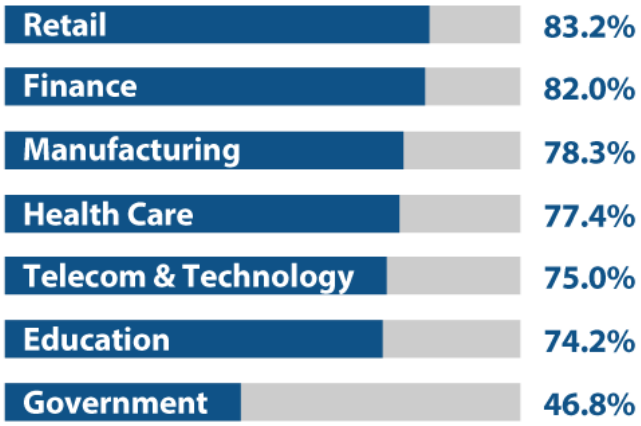


Figure 20: Percentage indicating security budget is growing by industry.

Without adequate funding, no IT security team stands a chance of keeping pace with the cyberthreats it is likely to face. Thankfully, for the fourth consecutive year, our data shows that IT security budgets are in excellent shape. Up from just over 61% two years ago, now more than three-quarters of respondents indicated that their organization's security budget is expected to grow in the coming year (see Figure 19). At the top end, one in five projected a budget increase of "10% or more," while only 4.2% expected their budget to shrink in 2017.

Other notable findings:

- The countries with the fewest respondents expecting a security budget decrease in 2017: Canada (2.0%), China (2.0%), and United Kingdom (2.2%). The countries with the most: Brazil (12.1%), Australia (8.2%), and Turkey (8.1%).
- The vertical industry with the biggest gain in respondents expecting a security budget increase for 2017: education (up 16 points to 74.2%), followed by retail (up nearly 12 points to 83.2%, and top place on the chart – see Figure 20).
- The vertical industry that's not keeping pace: government, with both the lowest rate of respondents expecting a budget increase (46.8%) and the highest rate expecting a budget decrease (10.9%).

Thankfully, for the fourth consecutive year, our data shows that IT security budgets are in excellent shape.

Technologies for Attack Surface Reduction

Which of the following technologies does your organization regularly use to reduce your network's attack surface? (Select all that apply.) (n=1,070)

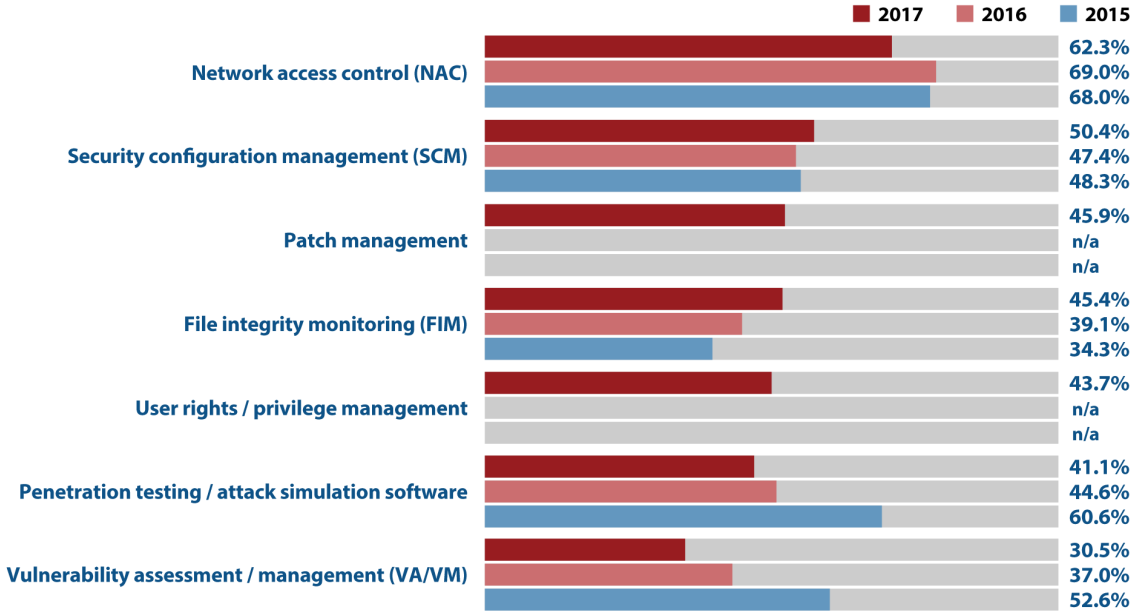


Figure 21: Technology choices for attack surface reduction.

Identified earlier as playing a respectable role in organizations' mobile security strategies (see Table 3), NAC was also selected by respondents as the top technology for reducing their network's attack surface (see Figure 21). Holding steady in second place, and even gaining a few percentage points (50.4%) compared to its result from last year, was security configuration management.

Clustered in the middle ground were file integrity monitoring (45.4%) and two new entrants, patch management (45.9%) and user rights / privilege management (43.7%). Once again, vulnerability assessment / management technology (30.5%) was designated the least popular option for attack surface reduction technology. And, once again, we find these results…baffling.

"Identified earlier as playing a respectable role in organizations' mobile security strategies, NAC was also selected by respondents as the top technology for reducing their network's attack surface..."

One possible explanation is that some respondents may have interpreted the survey question to be narrowly focused on the reduction of "network" or "networking" issues (such as overly permissive access control policies); whereas the intended scope encompassed all "networked" components and systems. If that isn't it, then we're at a loss as to what's going on. Because, with the 2015 Verizon Data Breach Investigation Report having taught us that 99.9% of exploited vulnerabilities were compromised more than a year after the corresponding CVE, we'd certainly expect to see greater use of many, if not all, of the technologies in Figure 21.

Other notable findings:

- Only Chinese organizations had an average usage rate greater than 50% across all the technologies listed.
- Education had the lowest average usage rate for the listed technologies at 38.7%, compared to an average of 46.1% across all other vertical industries.
- On average, very large organizations (> 25,000 employees) use each of the listed technologies 6% more than small organizations (500 to 999 employees).

Section 4: Practices and Strategies

Data Retention Practices for Network Forensics

On average, how long does your organization retain full-packet traffic data to assist with network forensics investigations? (n=1,038)

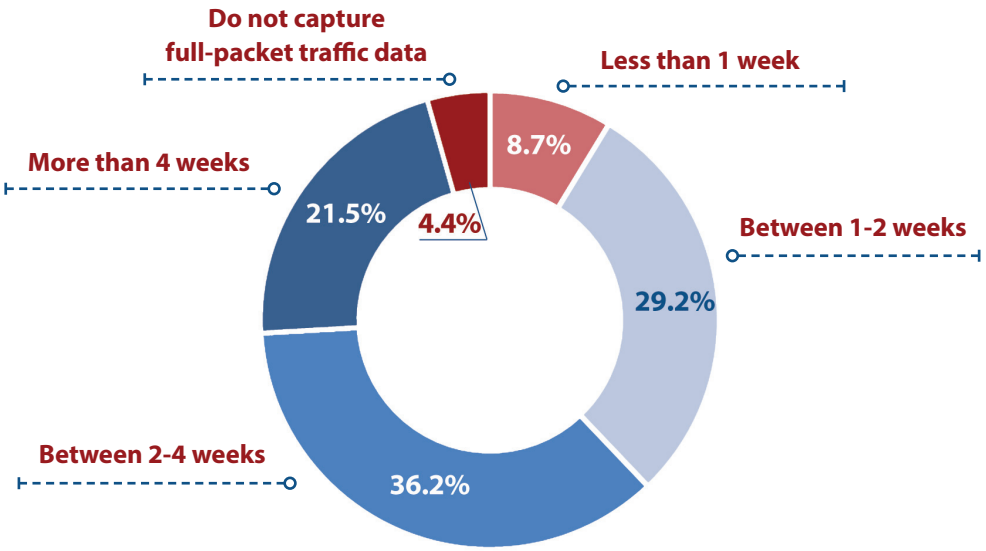


Figure 22: Retention practices for full-packet traffic data.

Full-packet capture of network communications is generally regarded as desirable, if not best practice, at least for network locations associated with business-critical assets/applications. The resulting cache of data is an unmatched resource IT teams can use in support of a wide variety of important processes – not the least of which is detailed investigation of security incidents, including suspicious events, ongoing attacks, and breaches that occurred in the past.

So, how long do organizations retain such data?

The most frequent answer, given by 36.2% of our respondents, was "between 2-4 weeks" (see Figure 22). Less-popular options were "between 1-2 weeks" (29.2%), "more than 4 weeks" (21.5%), and "less than 1 week" (8.7%).

The most frequent answer, given by 36.2% of our respondents, was "between 2-4 weeks".

Digging into the demographic breakdowns, we found the data also shows:

- Japanese (11.8%) and Canadian (10.2%) organizations are the least likely to be collecting full-packet traffic data.
- Government organizations are both the most likely to retain full-packet traffic data for more than 4 weeks (42.1%) and the most likely not to capture such data in the first place (12.3%).
- Very large organizations (>25,000 employees) are also a bit polarized in their practices, with both the greatest frequency for dumping their data in under a week (13.4%), as well as for retaining it more than four weeks (31.9%). These numbers compare to averages of 8% and 20%, respectively, for organizations of all other sizes.

Section 4: Practices and Strategies

Threat Intelligence Practices

Select the following reasons your organization has integrated commercial and/or open source threat intelligence into your existing security infrastructure. (Select all that apply.) (n=1,075)

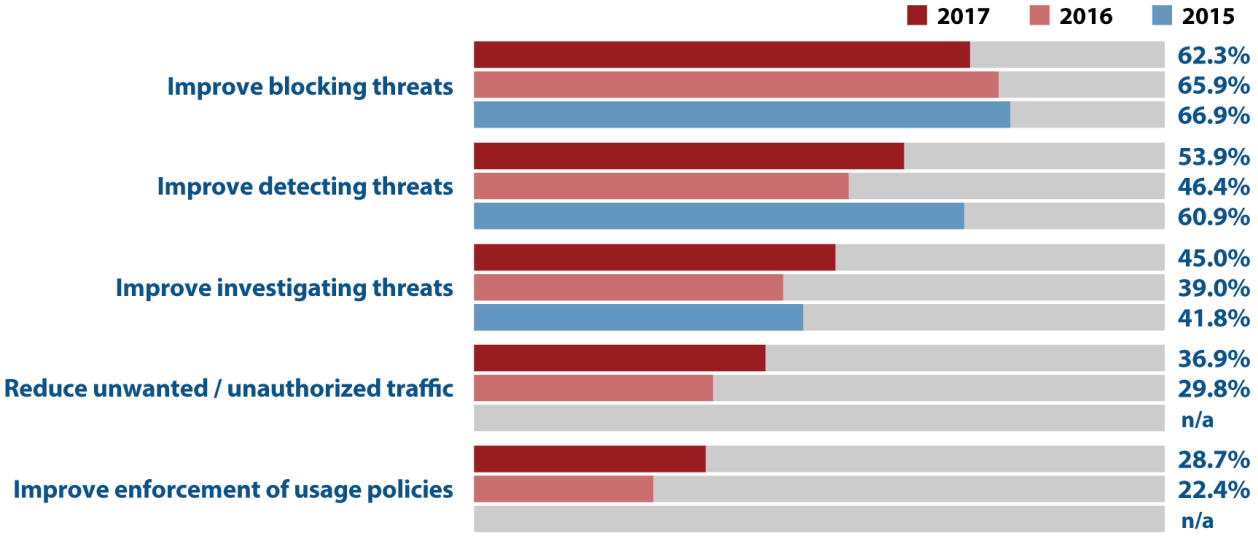


Figure 23: How threat intelligence is being leveraged.

Supplemental (i.e., third-party) threat intelligence services continue to be among the hottest areas of investment by organizations seeking to bolster their cyberthreat defenses (see Table 1). But how are IT security teams actually using this valuable resource – which can include everything from ordinary threat indicators (e.g., file hashes and reputation data) and threat data feeds (e.g., malware analysis and trend data) to strategic intelligence (e.g., detailed information on adversaries and their motivations, intentions, tactics, techniques, and procedures)?

The answer, again this year, is that the predominant use case for threat intelligence services is to enhance an organization's ability to block threats (62.4%). The next highest-ranking options – improving threat detection capabilities (53.9%) and improving threat investigation capabilities (45.0%) – both trail blocking by a considerable margin. Even further behind are the less-defense-oriented uses of keeping unwanted traffic off the network (36.9%) and better enforcing corporate policies (28.7%) (see Figure 23).

"The answer, again this year, is that the predominant use case for threat intelligence services is to enhance an organization's ability to block threats."

One particularly interesting finding from this year's data is the incremental gains observed for each of the four use cases other than blocking. These increases suggest to us that IT security teams are steadily evolving and maturing their intelligence-related practices, as they begin to leverage available intelligence data more thoroughly, including – presumably – for more strategic purposes, such as informing their organization's longer-term security strategy and investment decisions.

One final observation from the data for this question is that there were no notable differences in the findings based on geography, vertical industry, or size of company.

Section 4: Practices and Strategies

User and Entity Behavior Analytics Practices

Select the following reasons your organization operates user and entity behavior analytics (UEBA) technology. (Select all that apply.) (n=1,065)

Figure 24: How UEBA is being leveraged.

In The Road Ahead section of last year's CDR, we used the observation that "more data breaches result from credential theft and threat actors' masquerading as authorized users than from any other cause" as the basis for suggesting that organizations consider placing greater emphasis on what we dubbed "user-centric security." To be clear, our intent wasn't to distract security teams from their relatively newfound focus on application- and data-centric security investments; rather, it was to rejuvenate interest in user awareness training and core identity and access management practices, while calling attention to the emerging technology of user and entity behavior analytics (UEBA).

Now, one year down the road, we thought it would be interesting to take a closer look at the details of how/why IT security teams are using UEBA – which currently ranks among the hottest security technologies on the market (see Table 1). Our results show a tight cluster (see Figure 24), with the use of UEBA to detect account hijacking (52.5%) slightly edging out the triumvirate of detecting data exfiltration (48.9%), detecting privilege access abuse (48.0%), and defending against insider threats (47.8%).

"Our results show a tight cluster, with the use of UEBA to detect account hijacking (52.5%) slightly edging out the triumvirate of detecting data exfiltration (48.9%), detecting privilege accessabuse (48.0%), and defending against insider threats (47.8%)."

To be fair, these use cases represent some of the biggest challenges facing today's security teams. So, it's not surprising to see relatively high uptake for them across the board. Nor is it particularly surprising to see the one challenge that is clearly attributable to external threat actors (i.e., account hijacking) topping the list. What did catch us off guard a bit, however, is the rather substantial gap to the remaining two use cases listed.

Based on anecdotal evidence, we anticipated a dichotomy: some organizations effectively treating their SIEM solution as a data source for their UEBA implementation, and others doing the opposite. And while the data does indicate some of that is going on, what it more clearly reveals is that most organizations, at least for now, are operating their SIEM and UEBA solutions independently. For more on how this young "relationship" is evolving, be sure to catch the 2018 edition of this fine report.

In the meanwhile, it's also important to acknowledge that the potential use cases for UEBA are not limited to those highlighted in Figure 24. Indeed, early feedback from the field indicates security teams are finding numerous ways to take advantage of the underlying behavioral modeling, machine learning, and advanced analysis capabilities ... not only to help address many of the top challenges they're facing (see Figure 16), but also to enhance the effectiveness of their other defenses.

Cloud Access Security Broker Practices

Select the reasons your organization operates cloud access security broker (CASB) technology. (Select all that apply.) (n=1,062)

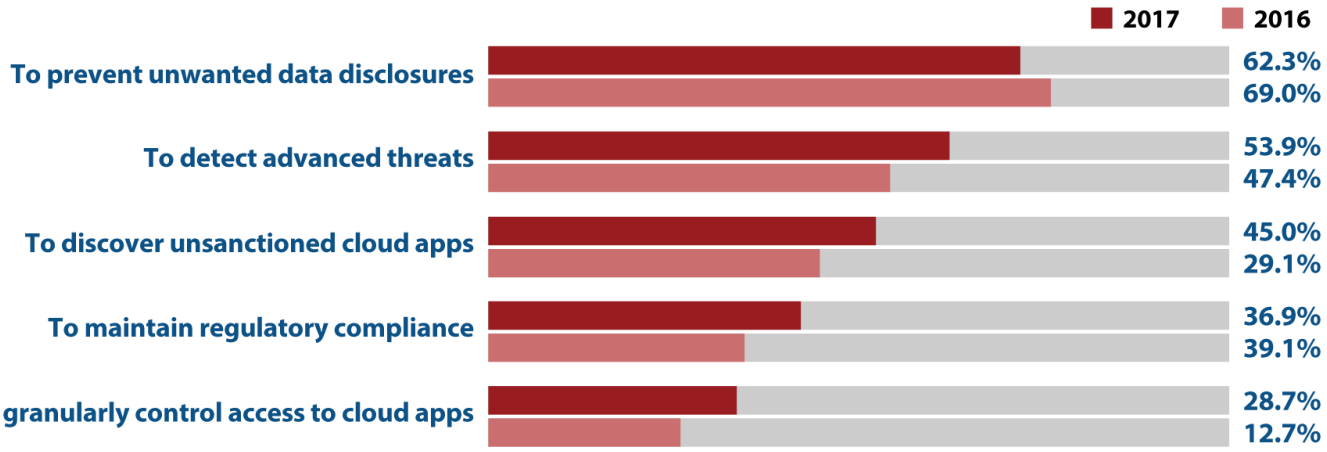


Figure 25: How cloud access security brokers are being leveraged.

"For the second year, preventing unwanted data disclosures was the most common reason selected by respondents (56.1%) for their organization's investment in CASB technology."

By no means are CASBs as pervasive as network firewalls or endpoint anti-malware software… yet. With everything they've got going for them, though, there's good reason to expect they will get there within a few years. The accelerating adoption of cloud applications and infrastructure services, continued inconsistency in the breadth and depth of native security capabilities offered by cloud service providers, and the rich feature sets and flexibility of leading CASBs are all points in their favor and, undoubtedly, major contributors to the excellent traction they continue to exhibit in the market (see Table 4).

As the Swiss Army knives of cloud application and data protection, leading CASB solutions are capable of providing everything from visibility into shadow IT and cloud application usage patterns to comprehensive access control, data protection, threat prevention, and even compliance support. Of course, the presence of a bunch of capabilities doesn't mean they're all going to be used, or valued, to the same degree.

For the second year in a row, preventing unwanted data disclosures was the most common reason selected by respondents (56.1%) for their organization's investment in CASB technology (see Figure 25). Cited progressively less often and, therefore, presumably less important, were the need to detect advanced threats plaguing cloud services (48.3%), discover use of unsanctioned applications (48.0%), and help maintain regulatory compliance (41.6%).

Related observations:

- Detecting advanced threats nudged ahead of discovering unsanctioned applications this year, as the concern for concrete threats was finally deemed to outweigh those of the shadow variety.
- Maintaining regulatory compliance gained the most ground over the past year, as it went from being a key CASB justification for 26.5% of respondents in 2016 to 41.6% in 2017.
- Using CASBs to granularly control user access to cloud services slipped, unceremoniously, into last place. To us, this finding signals a liberalization of security policies as enterprises continue to embrace the cloud – or, if you prefer, increased recognition that restricting users and being known for always saying "no" are sub-optimal, potentially career-limiting approaches to establishing effective cyberthreat defenses.

Section 4: Practices and Strategies

Overcoming the IT Security Skills Shortage

Which of the following strategies does your organization practice to overcome the worldwide shortage of qualified IT security talent? (Select all that apply.) (n=1,063)

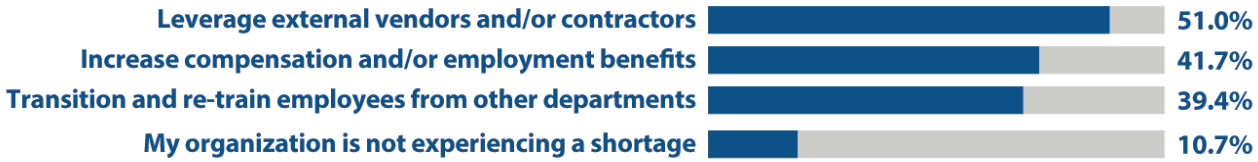


Figure 26: Overcoming the cybersecurity skills shortage.

We routinely encounter headlines and articles claiming there's a global shortage of one to two million skilled cybersecurity personnel. But are these figures legitimate estimates, or just puffed up claims to garner attention and pull in readers?

Given that a whopping nine out of 10 respondents indicated their organization is experiencing a shortage of IT security talent (see Figure 26), we're inclined to believe the estimates. As for how organizations are addressing the shortfall, the most frequently cited approach was to leverage external sources of talent, such as contractors or security service providers (51.0%). Trailing by a small margin and almost evenly matched were the tactics of increasing compensation and/or benefits as means to attract/retain talent (41.7%) and re-training employees from other areas of IT, or even the business at large (39.4%).

"...a whopping nine out of 10 respondents indicated their organization is experiencing a shortage of IT security talent..."

Although we didn't ask about it, further leveraging technology is another important approach to pursue. Investing in security solutions capable of automating manpower-intensive tasks (such as scanning, event aggregation, and reporting) or accelerating incident response activities to shrink an organization's window of exposure will certainly pay dividends. Our only caution is that IT security managers keep their expectations realistic in this regard. After all, technology still can't replace all of the skilled humans needed for more cerebral tasks, such as security planning, solution architecture and design, and incident investigation – just to name a few.

Returning to the data:

- Australia (83.7%), South Africa (84.0%), and the United States (86.4%) are the countries "least" impacted by the cybersecurity skills shortage, while China (100%) and Mexico (100%) are being impacted the most.
- Oddly, at least to us, health care (82.3%) and government (85%) organizations are struggling the least among listed industries when it comes to this challenge (see Figure 27). Call us crazy, but we would have expected just the opposite, especially given all of the data we've seen so far where the respondents from this pair of verticals indicated their organizations were behind the curve compared to the rest of the "big 7 industries."
- Overall, the skills shortage is slightly more acute (with +6% of respondents indicating there's an issue) for smaller organizations (500 to 4,999 employees) than it is for larger ones (5,000+ employees).

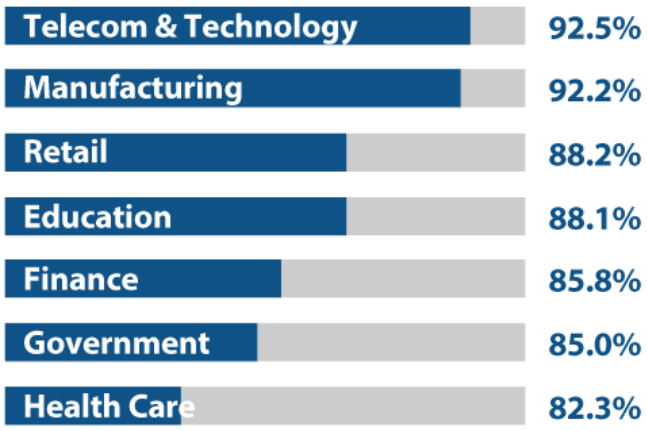


Figure 27: Percentage affected by the cybersecurity skills shortage.

The Road Ahead

IT security is clearly a harsh mistress. In what other IT discipline is success measured by the absence of something bad happening (i.e., a cyberattack)? Then there's the cruel reality that while the industrialization of hacking is making it ever easier for attackers to succeed, a steadily expanding attack surface makes it ever harder for IT security teams to successfully thwart them.

The bottom line is that it really shouldn't come as a surprise that so many IT security teams are already behind the eight ball. Or that so many organizations still have plenty of room to improve, even in areas typically considered core defenses. For example:

- Endpoint devices of all types – but especially mobile ones such as smartphones and tablets – are relative weak spots in most organizations' defenses (see Figure 5).
- Building security into applications in the first place is not a strong suit for today's organizations (see Figure 6).
- Although they're among the leading solutions planned for acquisition in the coming year, many emerging technologies most likely to be effective against advanced malware and targeted attacks – such as user and entity behavior analytics and cyberthreat intelligence services – show fairly modest adoption rates (see Table 1).
- Only a third of IT security professionals are confident that their organization is doing enough to monitor privileged user accounts for signs of misuse and/or compromise (see Figure 7).
- Adoption rates for key technologies aimed at reducing a network's attack surface – such as patch management, penetration testing, and vulnerability scanning – remain shockingly low (see Figure 21).

All is not lost, though. On the positive side of the ledger, anecdotal evidence indicates that cybersecurity is now a board-level topic for more organizations than at any time in the past. The fact that security budgets are both healthy and growing is also an encouraging sign (see Figures 17 to 20). Having additional funding at their disposal should enable enterprise security teams not only to fill known gaps in their organization's defenses, but also to start getting ahead in the game.

Looking beyond the scope of this year's survey, here are some key areas where we believe additional/proactive attention and investments have the potential to enhance an organization's defenses against current and future generations of cyberthreats.

Deception technology. There is little doubt that sophisticated attackers are increasingly penetrating enterprise defenses and subsequently operating – often unimpeded and for months – on internal networks. Compounding matters is the high volume of events and false positives generated by incumbent detection/behavior analysis/analytics technologies. Newly emerging deception technology promises relief on both fronts. Related solutions are extending well beyond the basic approach of traditional honeypots/honeynets – which focus on gathering threat intelligence – to deliver a broader set of capabilities. Resulting value propositions include:

- High probability alerts that are almost always indicative of an ongoing attack
- Increased costs, and, therefore, greater deterrence for attackers
- The ability to trick attackers into making off with useless files/data
- Enhanced event prioritization and threat actor intelligence

Of course, fully realizing these benefits is by no means a given. Forward-leaning IT security teams evaluating deception technology as a way to evolve their cyberthreat defenses will be well served by focusing on solutions that thoroughly address essential requirements. In particular, leading solutions should provide:

- Coverage for all layers of the computing stack (e.g., endpoint, network, app, data) and a wide range of decoy types (e.g., desktops, servers, switches, ATM/POS/medical/IoT devices)
- Extensive automation for decoy generation, deployment, and maintenance
- Innovative techniques for "hiding" decoys from normal users and for keeping attackers "on the hook" so the security team has sufficient time to respond
- Integration with "consumers" of threat intelligence (e.g., security infrastructure with prevent/response capabilities)

The Road Ahead

Container security. Because they offer developers numerous compelling benefits – including simple packaging, rapid deployment, reduced environmental dependencies, and horizontal scalability – container technologies/solutions such as Docker are here to stay. This situation, however, presents a major challenge from a security perspective. Not only are containers a new/unfamiliar technology (at least to security professionals), but also, practically by definition, they reduce transparency and auditability.

IT security teams looking to get in front of (or at least keep up with) this latest wrinkle in the application security landscape should recognize that container security is still immature. As a result, it will typically be necessary to look beyond the organization's container technology provider(s) to establish comprehensive defenses. As to what these defenses should include, we recommend enterprises take a multi-layer approach to container security by identifying and applying a combination of best practices (e.g., least privileges), existing countermeasures, and emerging technologies across each of the following areas:

- The build environment (e.g., controlling access/usage of build tools and security testing for the code included in a container)
- The container environment (e.g., controlling containers' permissions and vetting their contents)
- Runtime protection (e.g., protecting the container engine and host OS from any malicious containers and providing network-layer isolation)
- Monitoring and auditing (e.g., to verify that both your containers and security controls are operating as intended)

Remote/virtual browsing. Tired of drive-by downloads and watering-hole attacks leading to malware infections on your network? With the web being the second-greatest source of malware (behind only email), it's probably safe to say you're not alone. One intriguing solution that warrants consideration in this regard is remote browsing.

Also known as virtual browsing, this emerging technology works by isolating each browser session within a single-use virtual machine running on either an on-premises or cloud-based server. An employee uses his normal client-side browser to seamlessly control a corresponding server-side browser, which is responsible for parsing/rendering website code and then relaying a real-time, interactive display of the website being accessed. No website content is executed on the user's machine (or even gets to it, for that matter), and at the end of the session the virtual machine and any potential infections it has been exposed to are wiped from existence.

Unlike traditional anti-malware solutions, protection is provided for all forms of web-borne malware, including zero-day attacks, without the need for a steady stream of signature/content updates. In addition, centralization of browsing services streamlines related software maintenance while making it easier to consistently enforce desired web access policies and practices.

Attack/breach simulation. Enterprises' ongoing susceptibility to cyberattacks is not a result of a failure to deploy appropriate prevention and detection technologies. In many cases, the real issue is that our defenses have become so complex that it's practically impossible to know whether they were implemented correctly and continue, over time, to work as planned.

Penetration testing, vulnerability/configuration scanning, and other validation technologies certainly help in this regard, but they have notable limitations – such as being dependent on testers' skillsets, having a narrow focus, and only providing point-in-time assessments. Emerging attack/breach simulation platforms address these and other shortcomings of traditional solutions, for instance, by incorporating a comprehensive "hacker's playbook," running continuous, non-disruptive simulations against an organization's production environment, and integrating with existing security infrastructure to enable automated response and remediation.

The net result is a new class of security solution that not only provides a clear picture of whether an organization's security systems are truly working as expected and what its actual risks are at all times, but also can be used to:

- Shorten the duration of exposure, such as to newly discovered vulnerabilities and threats
- Proactively understand the impact of a new attack
- Train your security operations team
- Ensure compliance with regulatory mandates

For further insights on these and other emerging areas pertinent to IT security, be sure to tune in for the fifth annual CDR, currently scheduled for release in the first quarter of 2018.

Appendix 1: Survey Demographics

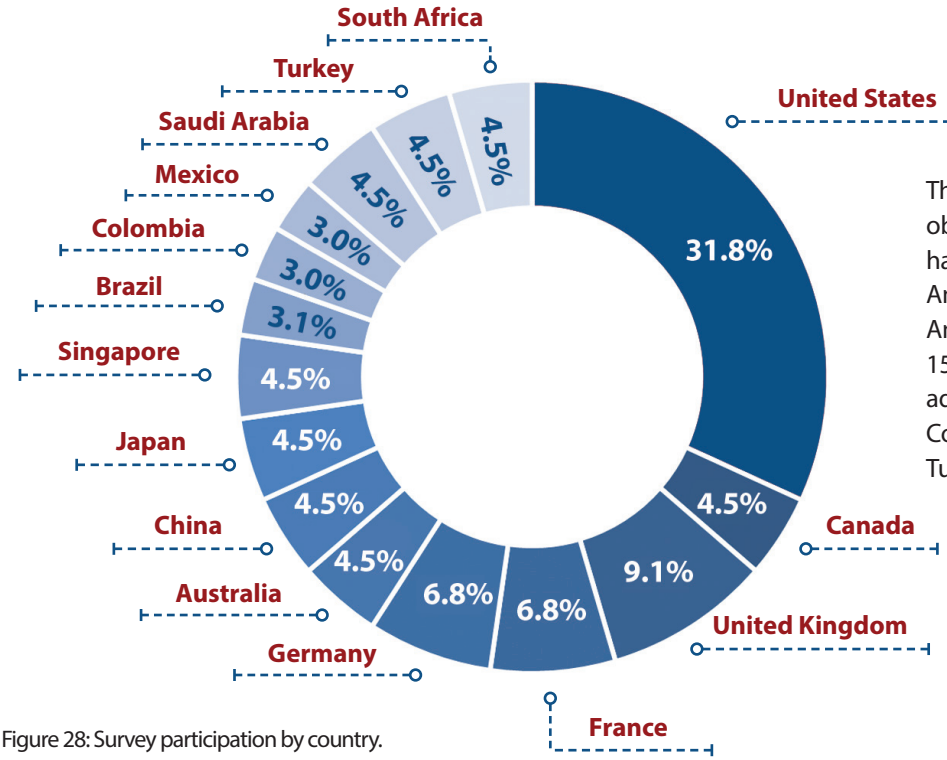


Figure 28: Survey participation by country.

This year's CDR is based on survey results obtained from 1,100 qualified participants hailing from six major regions (North America, Europe, Asia Pacific, Latin America, the Middle East, and Africa) and 15 countries spanning the globe. First-time additions included respondents from China, Colombia, Saudi Arabia, South Africa, and Turkey.

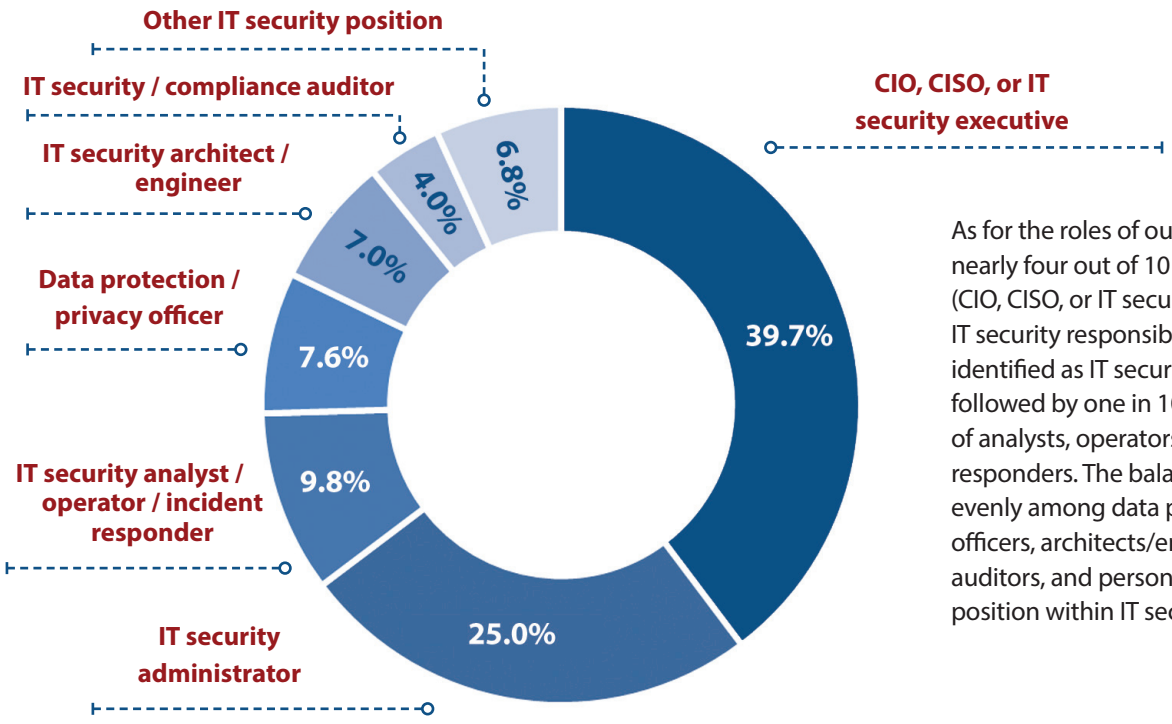
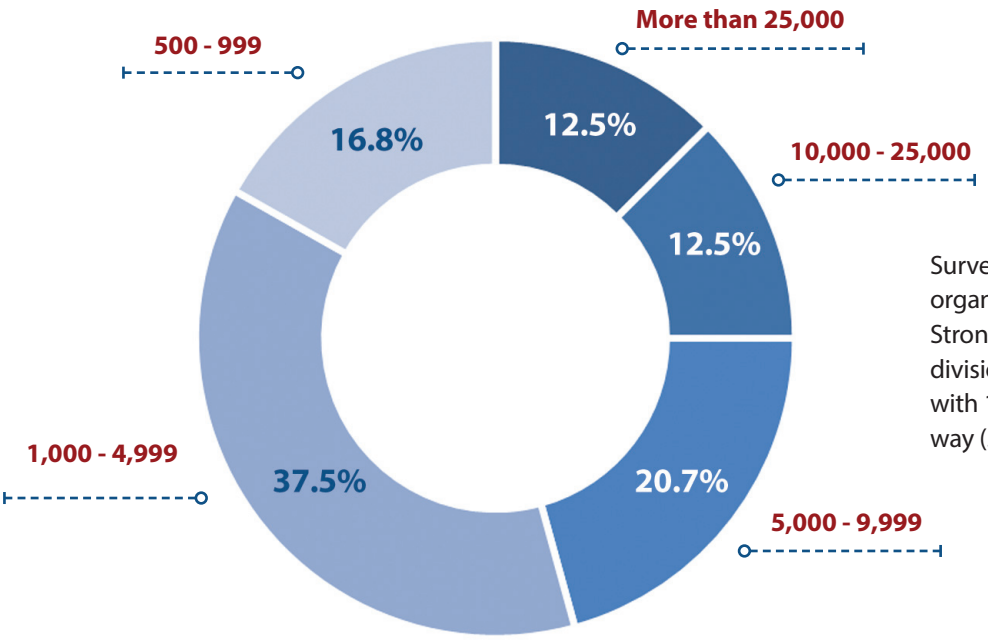


Figure 29: Survey participation by IT security role.

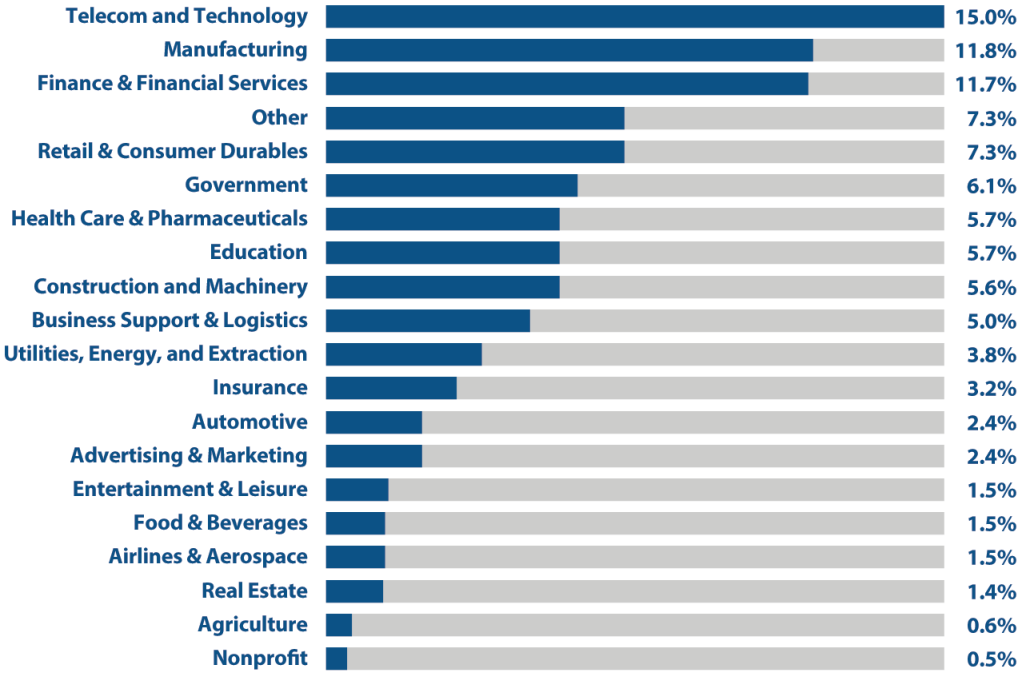
As for the roles of our survey participants, nearly four out of 10 held senior positions (CIO, CISO, or IT security executive) with IT security responsibilities. One quarter identified as IT security administrators, followed by one in 10 from the ranks of analysts, operators, and incident responders. The balance was split fairly evenly among data protection/privacy officers, architects/engineers, compliance auditors, and personnel identifying their position within IT security as "other."

Appendix 1: Survey Demographics



Survey respondents were from organizations with at least 500 employees. Strong representation was obtained from all divisions, with participants from enterprises with 1,000 to 4,999 employees leading the way (37.5%).

Figure 30: Survey participation by organization employee count.



Distribution of survey participants by vertical industry was fairly broad, with representation across 19 industry segments, and a twentieth category designated as "other." The "big 7 industries" – education, finance, government, health care, manufacturing, retail, and telecom/technology – accounted for just shy of two-thirds of all respondents. No single industry accounted for more than 15% of participants.

Figure 31: Survey participation by industry

Appendix 2: Research Methodology

CyberEdge Group developed a 27-question (10- to 15-minute) web-based survey instrument in partnership with its sponsoring vendors. (No vendor names were referenced in the survey.) The survey was promoted to information security professionals across North America, Europe, Asia Pacific, the Middle East, Latin America, and Africa in November 2016.

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, which altered the sample size ("n") for each set of survey question responses.

All qualified survey responses were inspected for potential survey "cheaters," meaning survey takers who 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 incentive. Suspected cheater survey responses were deleted from the pool of responses.

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
- Cloud Security
- Data Security
- Deception Technology
- DoS/DDoS Protection
- Endpoint Security
- Intrusion Prevention Systems (IPS)
- Managed Security Services Providers (MSSPs)
- Mobile Device Management (MDM)
- Network Behavior Analysis (NBA)
- Network Forensics
- Next-generation Firewall (NGFW)
- Patch Management
- Penetration Testing
- Privileged Account Management (PAM)
- Secure Email Gateway (SEG)
- Secure Web Gateway (SWG)
- Security Analytics
- Security Configuration Management (SCM)
- Security Information & Event Management (SIEM)
- Threat Intelligence Services
- User and Entity Behavior Analytics (UEBA)
- Virtualization 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 https://cyber-edge.com/.

CyberEdge Acceptable Use Policy

CyberEdge Group, LLC ("CyberEdge") encourages third-party organizations to incorporate textual and graphical elements of this report into presentations, reports, website content, product collateral, and other marketing communications without seeking explicit written permission from CyberEdge, provided such organizations adhere to this acceptable use policy.

The following rules apply to referencing textual and/or graphical elements of this report:

1. **Report distribution.** Only CyberEdge and its authorized research sponsors are permitted to distribute this report for commercial purposes. This restriction does preclude reproduction of the report for internal uses, such as a training.
2. **Source citations.** When citing a textual and/or graphical element from this report, you must incorporate the following statement into a corresponding footnote or other citation: "Source: 2017 Cyberthreat Defense Report, CyberEdge Group, LLC."
3. **Quotes and excerpts.** Quotes and excerpts extracted from this report must not be modified in any way. Rephrasing is not permitted.
4. **Figures and tables.** Figures and tables extracted from this report must not be modified in any way. Artwork for figures and tables for the most recent Cyberthreat Defense Report may be available for download at no charge on the CyberEdge website at **https://www.cyber-edge.com/cdr**.
5. **No implied endorsements.** CyberEdge does not endorse technology vendors. Cited CyberEdge content should never be used to imply favor from CyberEdge.

If you have questions about this policy or would like to incorporate content from this report in a manner not addressed by this policy, submit an email to **research@cyber-edge.com**.