CSX™
CYBERSECURITY NEXUS

State of Cyber Security 2017

Part 2: Current Trends in the Threat Landscape

Abstract

State of Cyber Security 2017 reports the results of the annual ISACA global cyber security survey, conducted in October 2016. The survey results bolster the belief that the field of cyber security remains dynamic and turbulent. Weekly news headlines confirm that cyberattacks are not a seasonal threat or dependent on specific industry environmental attributes, but are constant and should remain forefront in every enterprise executive's thought process. To equip you with a comprehensive understanding of the cyber security industry through the lens of those who define it—the managers and practitioners—ISACA is presenting the survey results in a two-part report that focuses on individual topics. This report is the second part of the *ISACA State of Cyber Security 2017* white paper series and presents timely information about current cyber security trends—staffing, budget allocation, the threat environment, and controls and countermeasures.

ISACA®
Trust in, and value from, information systems

Table of Contents

State of Cyber Security 2017

Part 2: Current Trends in the Threat Landscape

The practice of cyber security in a real-world context can often feel to the practitioner like standing at ground zero between the proverbial irresistible force and an immovable object. As attacker sophistication and skill seem to increase exponentially, the resources available to defend against them (e.g., staff and supporting tools) seem harder and harder to come by. The cyber security function feels short-staffed, underfunded and always struggling to do more with less.

But perceptions do not always align perfectly with reality. Do these perceptions reflect the actual state of the profession? Are they real, observable phenomena or are they the stress-induced byproduct of a high-stakes and fast-moving profession?

To answer these questions, ISACA conducted its annual State of Cyber Security survey in October 2016. The purpose of the survey was to gather information about the state of the cyber security profession and the overall state of cyber security. The survey canvassed cyber security managers and practitioners about their enterprise staffing, budget allocation, threat environment, and controls and countermeasures. With a focus on the human-capital marketplace, the survey asked respondents about the skill level of applicants seeking employment in enterprise cyber security teams, the degree to which new hires into an existing team deliver against enterprise expectations, and the overall challenges new hires encounter.

State of Cyber Security 2017 compares the results of this year's survey with previous results to determine recognizable trends that impact how cyber security is practiced, particularly where such trends point to an overall shift in the profession. This report summarizes the key survey findings and apparent trends observed over time. *State of Cyber Security 2017* further provides, where possible, forward-looking analysis about the implications of these trends on the cyber security profession.

Survey Methodology

An invitation to participate in the survey was emailed to a global population of cyber security professionals who hold ISACA's Certified Information Security Manager® (CISM®) and/or Cybersecurity Nexus Practitioner™ (CSX Practitioner™) designations, and individuals in information security positions. The survey data was collected anonymously through SurveyMonkey®. The results reveal positive and negative findings about the current state of cyber security. The survey, which uses multiple-choice and Likert-scale formats, is organized into four major sections:

Budgets, Hiring and Skills

Threats

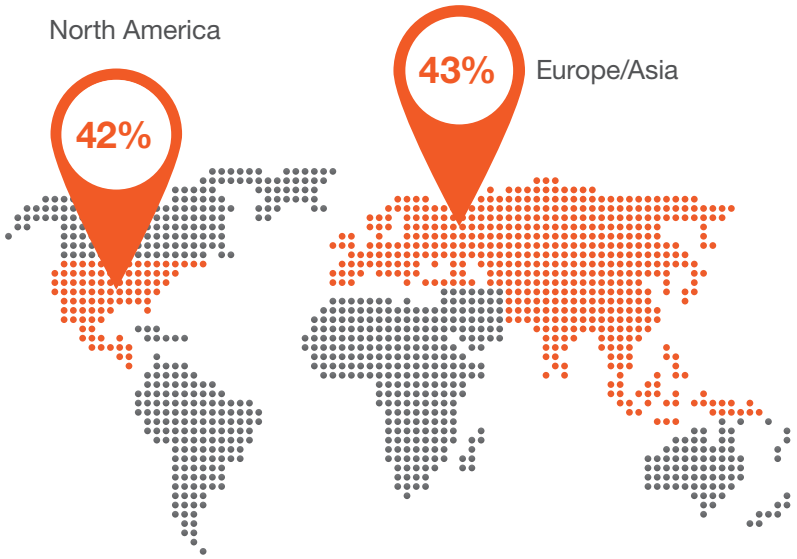
Internet Crime and Fraud

Organizational Security and Governance

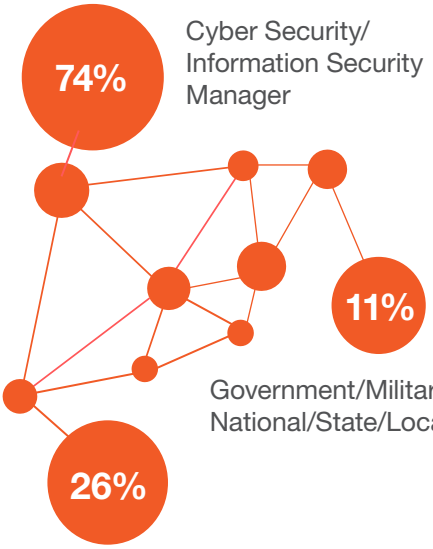
The ISACA survey targets managers and practitioners who have cyber security job responsibilities. Although 950 individuals participated in the survey, only those respondents whose primary job function is cyber security or information security (633 participants) are included in the survey results.

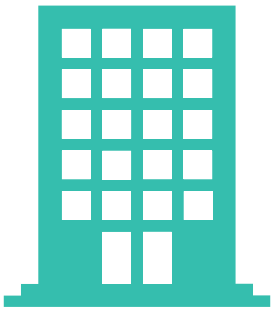
A typical respondent can be described as:

100%
A member of ISACA



28%
Working in technology services/consulting





49%
Employed in an enterprise with at least 1,500 employees

23%
Financial Services

While the norms of the sample population are interesting to consider, it is important to note some characteristics that reflect the population's diversity. Among those surveyed, respondents hailed from more than 20 industries (**Figure 1**) and all five major global regions (**Figure 2**).

FIGURE 1—INDUSTRY SECTORS

In which of the following industries are you employed?

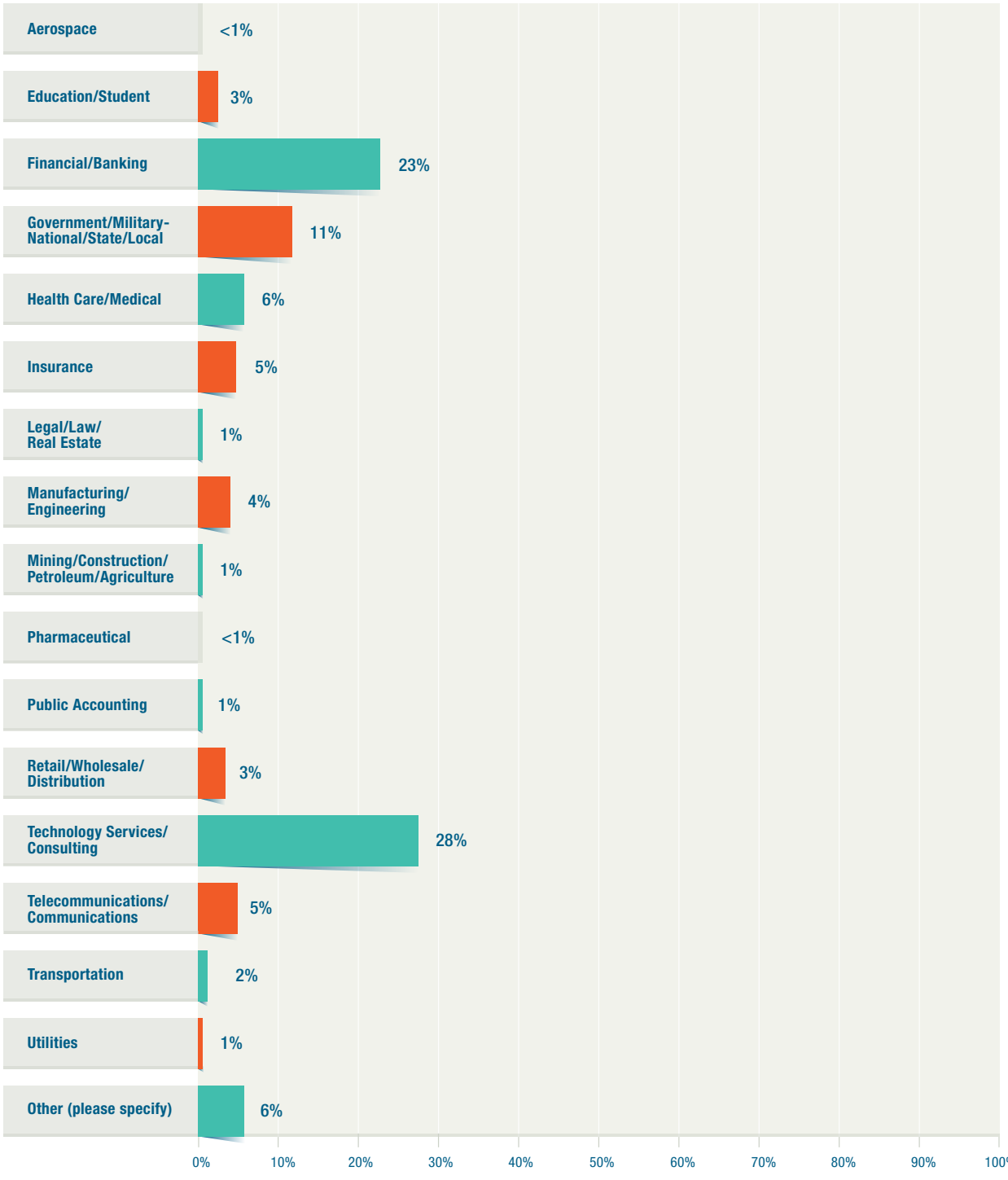
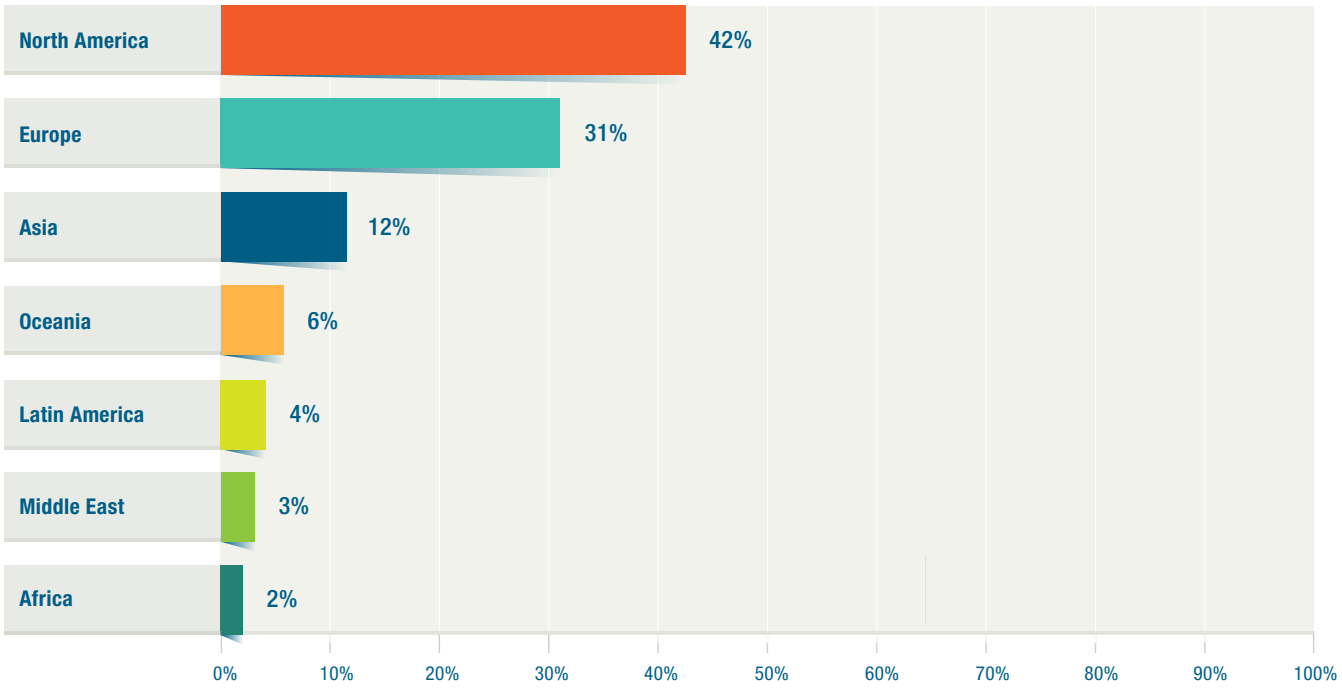


FIGURE 2—REGIONS

In which reigon do you reside?



Key Findings

As highlighted in part 1 of this report[1], enterprises have continued difficulty finding qualified personnel to fill cyber security positions. For example, one-third of the respondents note that their enterprises receive more than 10 applicants for an open position, but 64 percent of that one-third indicate that fewer than half of the applicants are qualified. Moreover, even skilled resources, once hired, require time and training before they are fully up to speed and performing their job at a competence level equivalent to others who are already in the enterprise.

These personnel and staffing challenges compound the challenges that enterprises are already experiencing in the threat landscape—those associated with a slowdown in the allocation of resources to combat threats and the growth in complexity and hostility of the threat environment itself. Specifically, attacks are increasing, but the resources allocated to combat those attacks, while still growing, are growing at a reduced rate compared with prior years. This year's survey reveals emerging areas of concern—Internet of Things and ransomware—that are concerning to practitioners over and above the traditional threats that are already on practitioners' radar.

1 ISACA, "State of Cyber Security 2017: Current Trends in Workforce Development," February 2017, *www.isaca.org/cyber/pages/state-of-cyber-security-2017.aspx*

The following key survey findings pertain to the threat landscape:

- **Budgets are still expanding, but more slowly.** Half of the enterprises represented by the survey respondents anticipate a growth in their cyber security budget over the next year. Although this is an encouraging sign and points to the fact that cyber security is increasingly being seen as an investment area, the rate of growth appears to have slowed. Specifically, for 2016, 61 percent of survey participants indicated expected budget growth; for 2017, only 50 percent report an expected increase.
- **The threat environment is increasingly hostile.** This slowdown in expansion is occurring at the same time that enterprises are seeing an increase in attacks. 53 percent of respondents reported an increase in attacks in 2016, and 80 percent believe it is either "likely" or "very likely" that they will be attacked in 2017.
- **Internet of Things (IoT) is replacing mobile as the emerging area of concern.** Threats resulting from mobile-device loss are down from last year, but a new challenge area appears to be emerging—IoT. Concern about the cyber security ramifications of IoT shows no sign of slackening, while the number of respondents for whom IoT is "on the organization's radar" increased significantly over last year.
- **Ransomware is expanding, but the processes to address it are not yet ubiquitous.** The number of malicious code attacks, including ransomware, remains high. More than three-quarters (78 percent) of the respondents report that their enterprises experienced attacks in 2016 that included malicious software, and 62 percent report a ransomware attack specifically. Only 53 percent of the participants indicate that their enterprises have a formal process in place to deal with ransomware attacks.

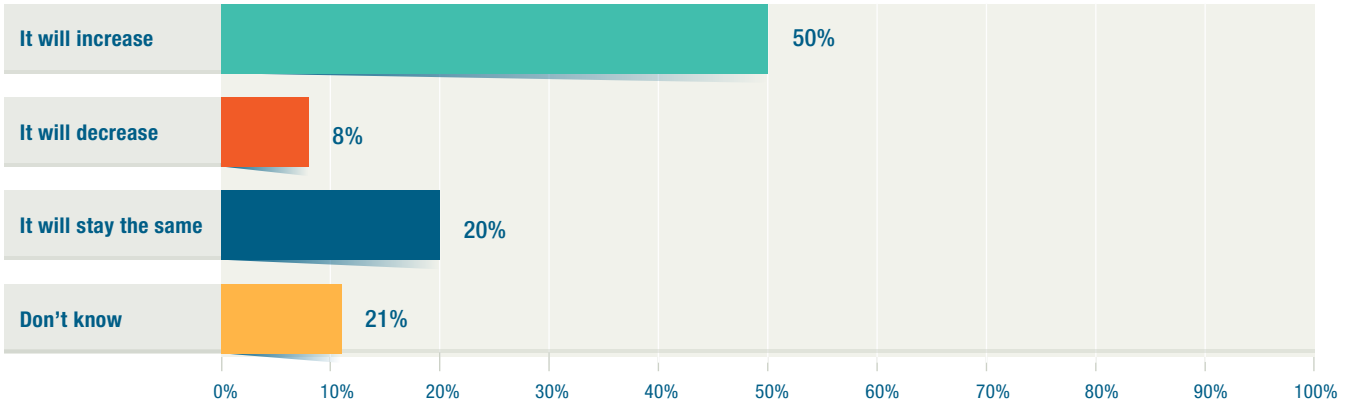
Resource Slowdown

Budgets for cyber security activities continue to expand in 2017, as reported by half of the respondents (**figure 3**). Note, however, that this is down from last year, when 61 percent reported an increase in overall cyber security budget. This means that cyber security budgets are still increasing, but they are doing so more slowly than in prior years.

This implies potential challenges further down the road, particularly in light of the staffing challenges observed in part 1 of this report. Specifically, many enterprises are leveraging both automation and external resources (e.g., consultants and MSSPs) as a strategy to offset missing

FIGURE 3—CHANGES IN THE CYBER SECURITY BUDGET

How, if any, will your enterprise's security budget change in 2017?



skills or skills that are in short supply within the enterprise, i.e., making investments in tools or external service providers to accomplish tasks that would otherwise fall on the shoulders of cyber security personnel. This strategy relies on there being budget available to offset a shortage of skills. If the skills gap continues unabated, which appears likely given the findings from part 1 of this report, and the funding for automation and external third-party support is reduced, it will become more difficult for enterprises to fill their cyber security needs.

Increased Threats

The budgetary slowdown noted in the previous section may forecast additional challenges considering the volume of overall attacks. This decrease in the pace of budget expansion is occurring despite an increase in attacks overall and an increase in the sophistication of these attacks. Half of the respondents indicate that their enterprises executed their incident response plan in 2016 (**figure 4**), and 53 percent report an increase in the overall number of attacks compared to 2015 (**figure 5**). This means that, on the whole, attacks are increasing at a faster rate than in prior years. Considering the budgetary considerations outlined in the previous section, it follows that less funding will likely be available on a per-attack basis to respond to (or prevent) these attacks.

In terms of the specific kinds of attacks experienced and their associated impacts, 10 percent of respondents report experiencing a hijacking of corporate assets for botnet use, 18 percent report experiencing an advanced persistent threat (APT) attack, and 14 percent report stolen credentials (**figure 6**). Last year's results for the three types of attacks were 15 percent for botnet use, 25 percent for APT attacks and 15 percent involving stolen credentials.

Phishing (40 percent), malware (37 percent) and social engineering (29 percent) continue to top the charts in terms of specific attack vector utilized (**figure 7**). These are the same top three vectors as in prior years, although the relative order shifted somewhat and the overall frequency of occurrence decreased (**figure 8**). This implies that, although attacks are up overall, the number of successful attacks (at least in these three categories) is down.

The trend of increasing attacks is likely to continue in 2017, according to the survey respondents, of whom 39 percent believe it is very likely that their enterprise will experience a cyberattack and 41 percent consider it likely (**Figure 9**).

Key Implication of the Budget Trend

Slowdown in budget expansion can be a potential risk if it is sufficient to cause economic-related hiring freezes or reductions in open headcount requisitions. As noted in part 1 of this report, enterprises are already challenged with acquiring the right skills; hiring freezes or other "belt tightening" from the enterprise overall can exacerbate this issue. Enterprises may want to begin planning strategies now to ensure that they are prepared, e.g., by investing in talent retention, personnel development, cross training or other activities that maximize current staff and minimize the impact of attrition.

FIGURE 4 — EXECUTION OF INCIDENT RESPONSE PLAN

If your enterprise had an incident response plan, was it executed in 2017?

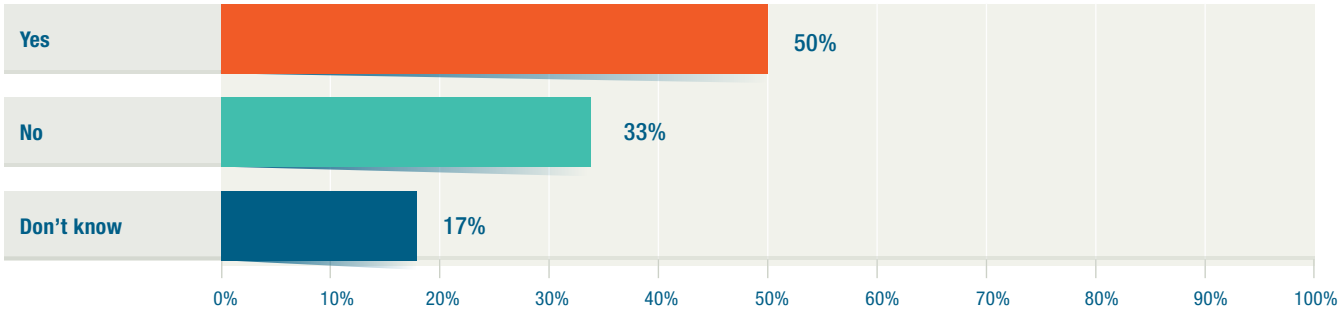


FIGURE 5 — CHANGE IN NUMBER OF CYBER SECURITY ATTACKS

Is your enterprise experiencing an increase or decrease in security attacks as compared to 2015?

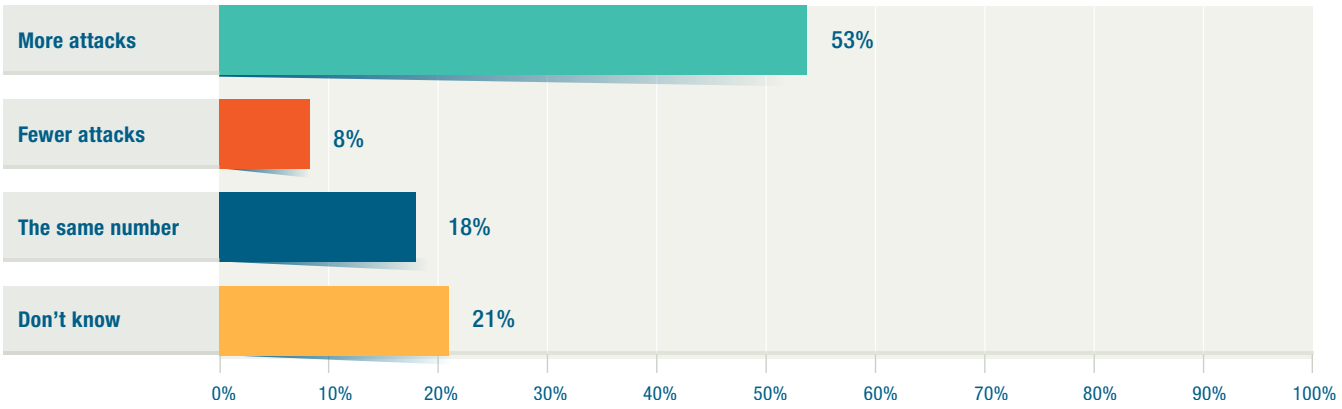
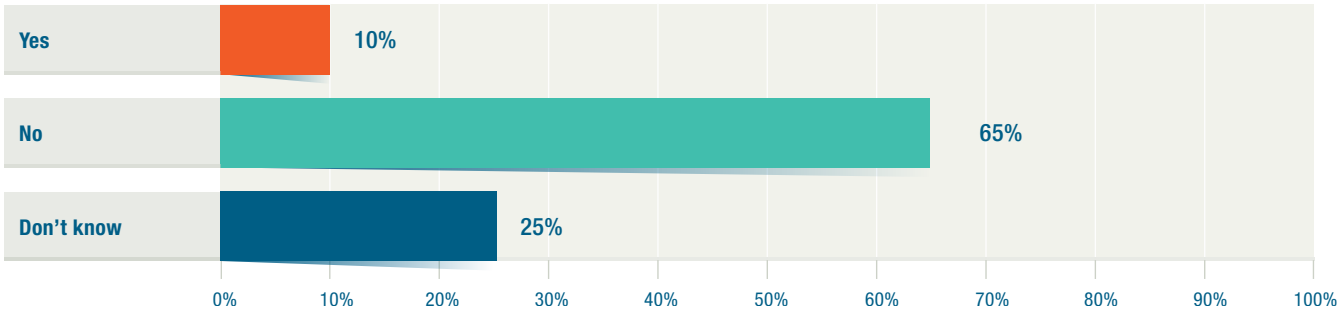
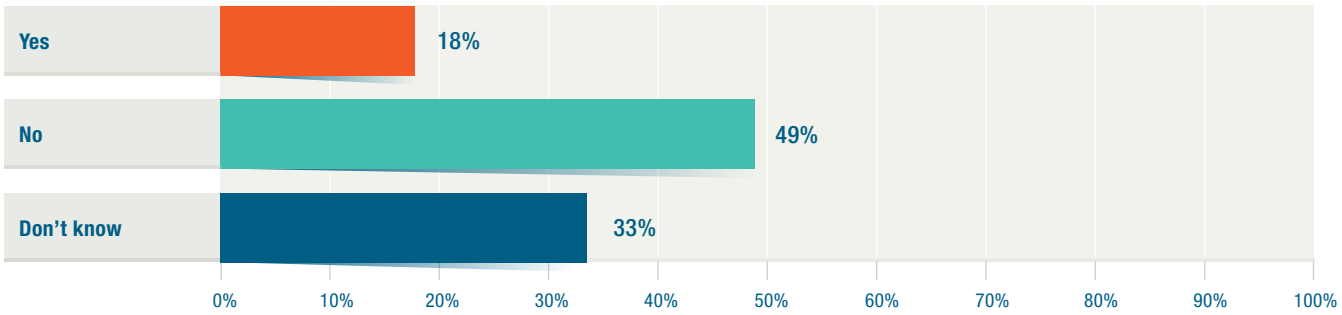


FIGURE 6 — ATTACK TYPES IN 2016

Where any of your enterprise's corporate assests hijacked for botnet use in 2016?



Did your enterprise experience an APT attack during 2016?



Were any user credentials stolen from your enterprise during 2016?

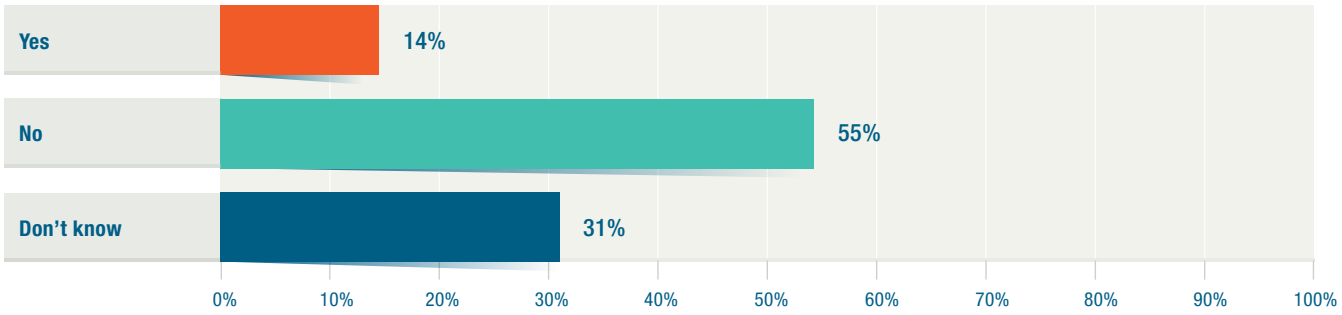


FIGURE 7 — ATTACK VECTORS

If your enterprise was exploited in 2016, which of the following attack types were used?

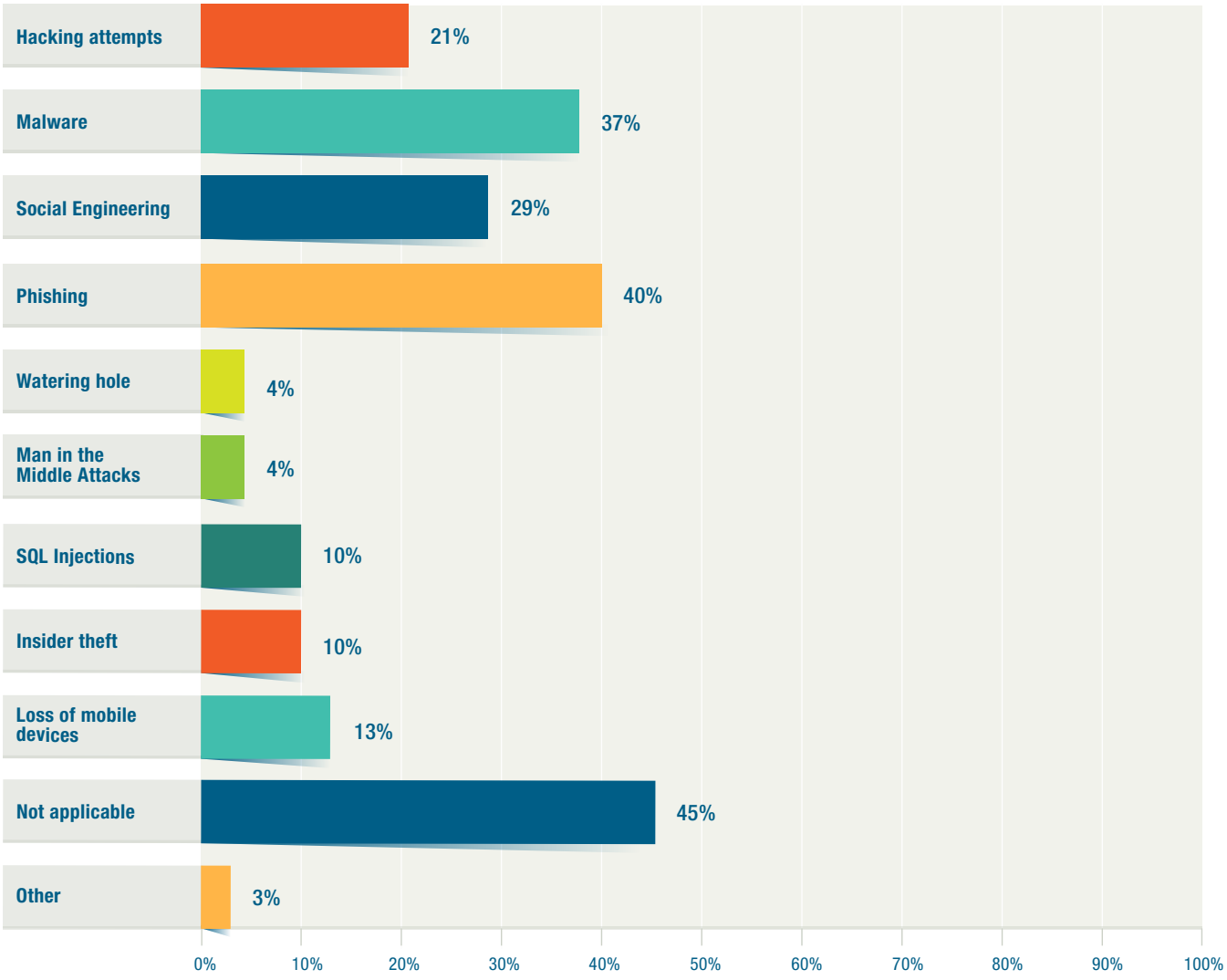


FIGURE 8 — COMPARISON OF CURRENT ATTACK TYPES TO LAST YEAR'S RESULTS

What is the percentage of enterprises exploited with phishing, malware and social engineering attacks in 2015 and 2016?

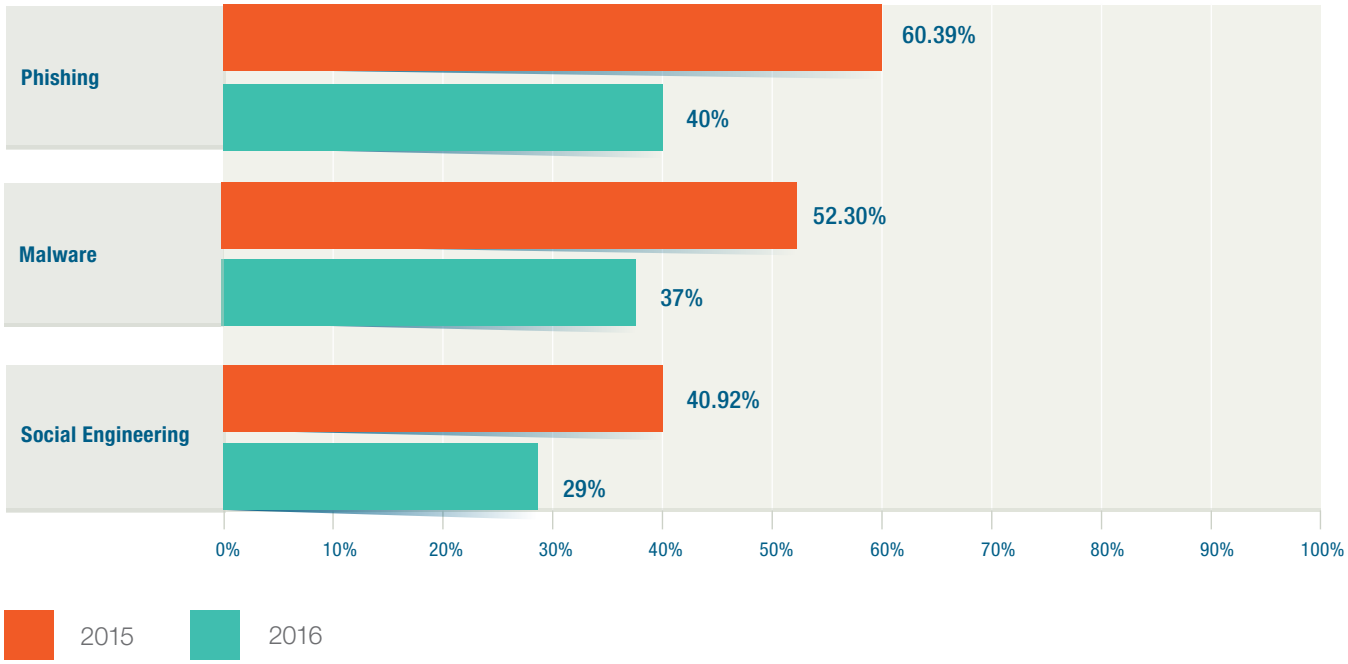
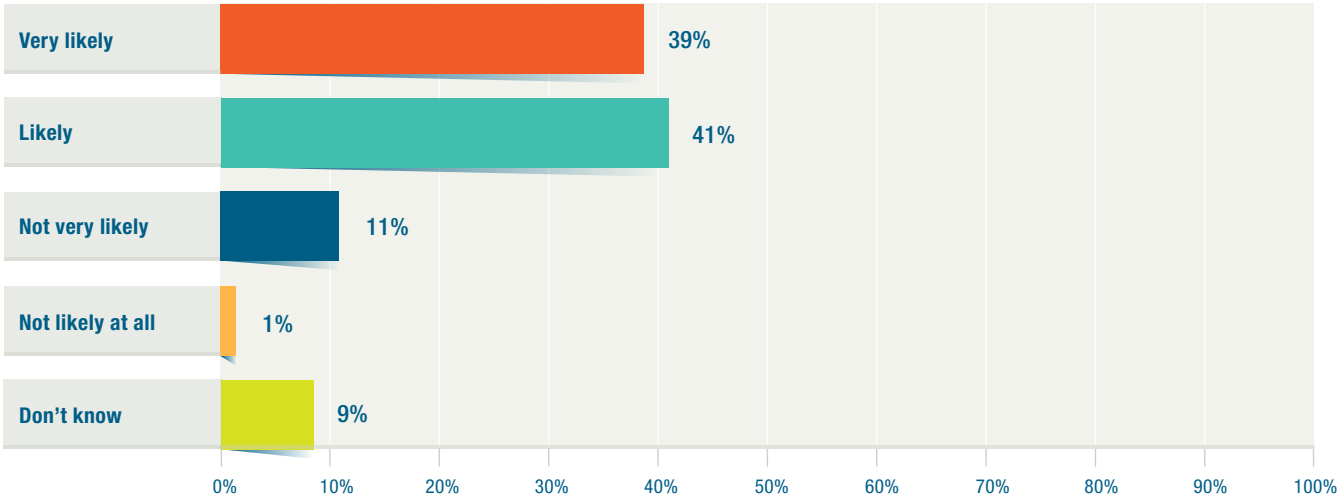


FIGURE 9 — LIKELIHOOD OF CYBERATTACK IN 2017

How likely do you think it is that your enterprise will experience a cyber-attack in 2017?



What This Mean to Enterprises

- Attacks are likely to increase; likewise, sophistication of attacks may continue to increase. Challenges associated with prevention and response are likely to increase due to both volume and complexity.
- An increase in attacks may increase the relative value of intelligence-driven cyber security methods relative to traditional perimeter defense methods. Specifically, as threats increase and are more often successful, the value of detection of active threats in the environment increases.
- As threat information increases in value, information sharing becomes paramount. Enterprises may want to consider expanding participation in information-sharing and collaborative-analysis venues.

What This Means to Enterprises

- IoT is an increasingly-important element in governance, risk and cyber security activities. This is a challenge area for many, because traditional security efforts may not already cover these devices.
- Enterprises may want to assign accountability for cyber security hygiene tasks for devices. This might include consumer devices like smart TVs or it can include other operational technology, such as industrial control systems. Specific policies and procedures may need to be developed to support these activities.

IoT and Mobile Threats

Exploits resulting from mobile devices are down significantly from 2015. Only 13 percent of respondents cite lost mobile devices as an exploitation vector in 2016, compared to 34 percent in 2015. A contributory factor to this decrease may be the prevalence of encryption as a mobile device protection strategy; only 9 percent indicate that lost or stolen mobile devices were unencrypted (**figure 10**). Again, this is a positive trend, illustrating an overall improvement in how enterprises are addressing the mobile workforce as part of their cyber security strategy and planning.

As enterprises have become more sophisticated in the mobile arena, however, a new potential challenge area has arisen that continues to be of concern—IoT. IoT was noted as a potential emerging area of concern in the 2015 survey by a majority of respondents (53 percent) and that figure increases slightly in 2016; specifically, 59 percent of the 2016 respondents cite some level of concern relative to IoT while an additional 30 percent are either “extremely concerned” or “very concerned” (**figure 11**).

Note that while the overall number of respondents who are concerned is not up tremendously, the story is a bit more nuanced than it appears on the surface. Specifically, the number for whom IoT is “not applicable” is down over 20 percentage points (from 25 percent to 3 percent). This suggests an observable rise in the prevalence of IoT in industry generally and an increased rate of cyber security practitioners encountering it in the field. Therefore, the implication is that IoT is becoming more common, i.e., cyber security planning needs to account for it; likewise, it represents an attack surface that should also be considered.

FIGURE 10 — ENCRYPTION OF LOST MOBILE DEVICES

If mobile devices were lost in 2016, were they encrypted?

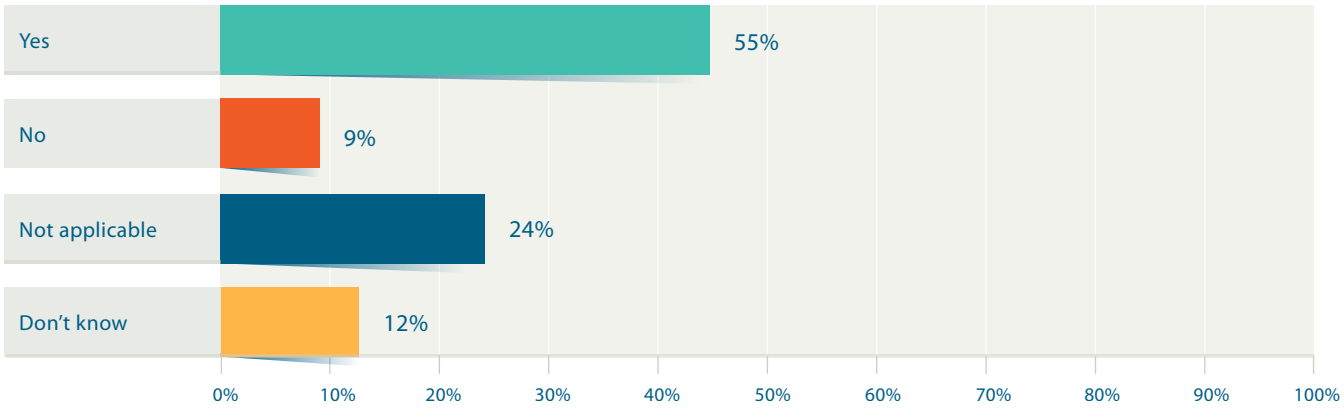
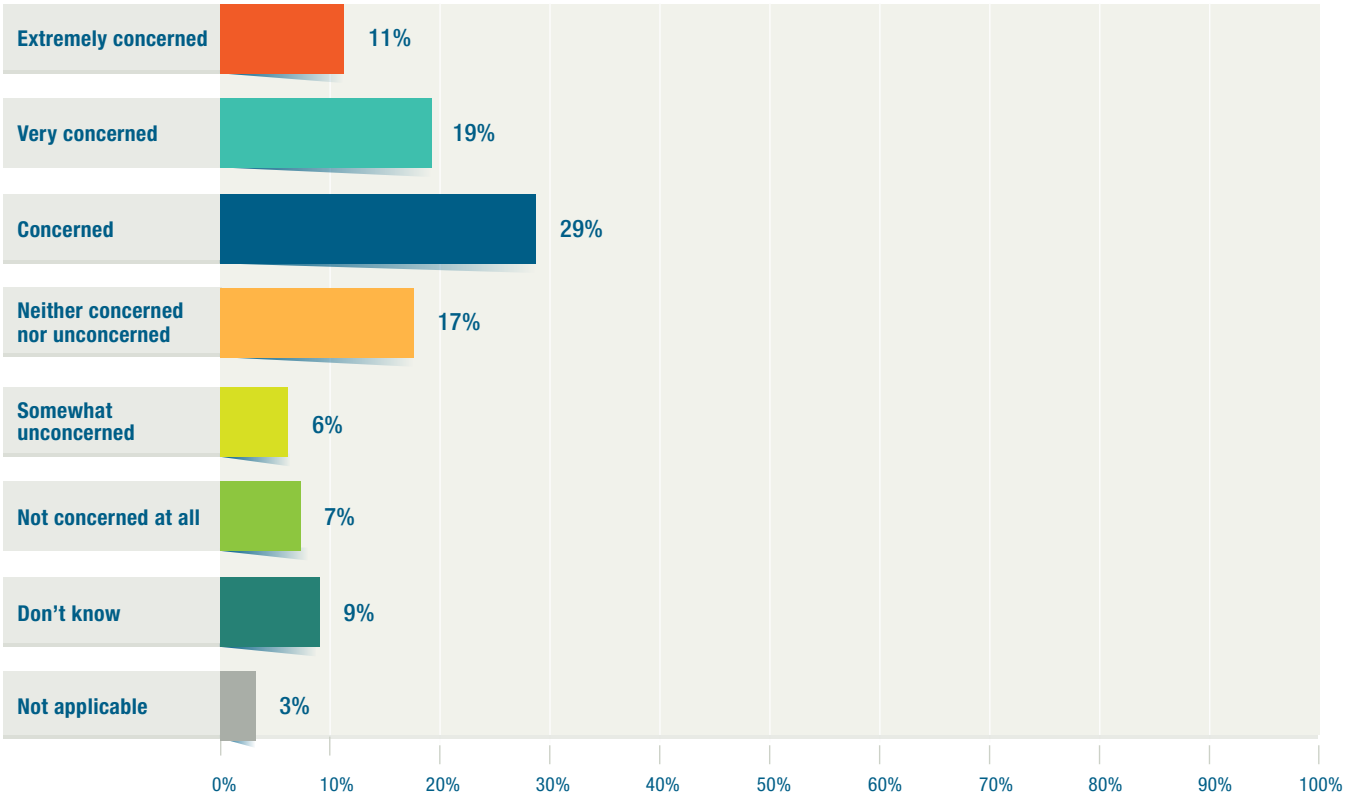


FIGURE 11 — CONCERN ABOUT IoT

How concerned is your enterprise with Internet of Thinks (IoT) in the workplace?



Ransomware

The number of malicious code attacks, including ransomware, remains high. More than three-quarters (78 percent) of the respondents indicate that their enterprises experienced attacks in 2016 that included malicious software, while 62 percent report their enterprises experiencing a ransomware attack specifically (**figure 12**). Only 53 percent of respondents' enterprises have a formal process in place to deal with ransomware attacks (**figure 13**).

It is possible that the prevalence of ransomware is due in part to the motivations of threat actors. Half of the respondents indicate that the motivation of future attackers is most likely to be financial gain (**figure 14**). Ransomware provides a fruitful avenue for financially motivated criminals, because it creates a direct path between their actions and remuneration through the payment of the ransom by the victim.

This suggests that active planning for ransomware can be a fruitful endeavor for enterprises that have not already done so, e.g., by conducting "tabletop" exercises that stage a ransomware event or by discussing in advance decisions about payment vs. non-payment. Payment of the ransom can seem appealing during an actual ransomware situation. For example, a study from IBM[2] found that 70 percent of business ransomware targets paid the ransom. However, it is not a decision to be undertaken lightly. Law enforcement typically advocates nonpayment of the ransom to discourage the utility of ransomware for financially-motivated criminals; they further warn that paying the ransom can have an encouraging effect on those criminals—even in some cases leading to subsequent targeting of that same enterprise for further attacks. Additionally, it bears noting that a substantial number of those who pay the ransom do so without the hackers upholding their side of the exchange.

Regardless, nonpayment can be a difficult position to argue in the face of heightened emotions during an actual ransomware situation. Planning it out in advance—potentially even implementing a governing corporate policy or other operating parameters—can help to ensure that the best decisions are made when the time comes.

2 IBM, "Ransomware: How Consumers and Businesses Value Their Data," 2016, www-03.ibm.com/press/us/en/pressrelease/51230.wss

FIGURE 12 — FREQUENCY OF DIFFERENT TYPES OF CYBER-ATTACKS

How often, if at all, did your enterprise experience the following cyber-attacks in 2016?

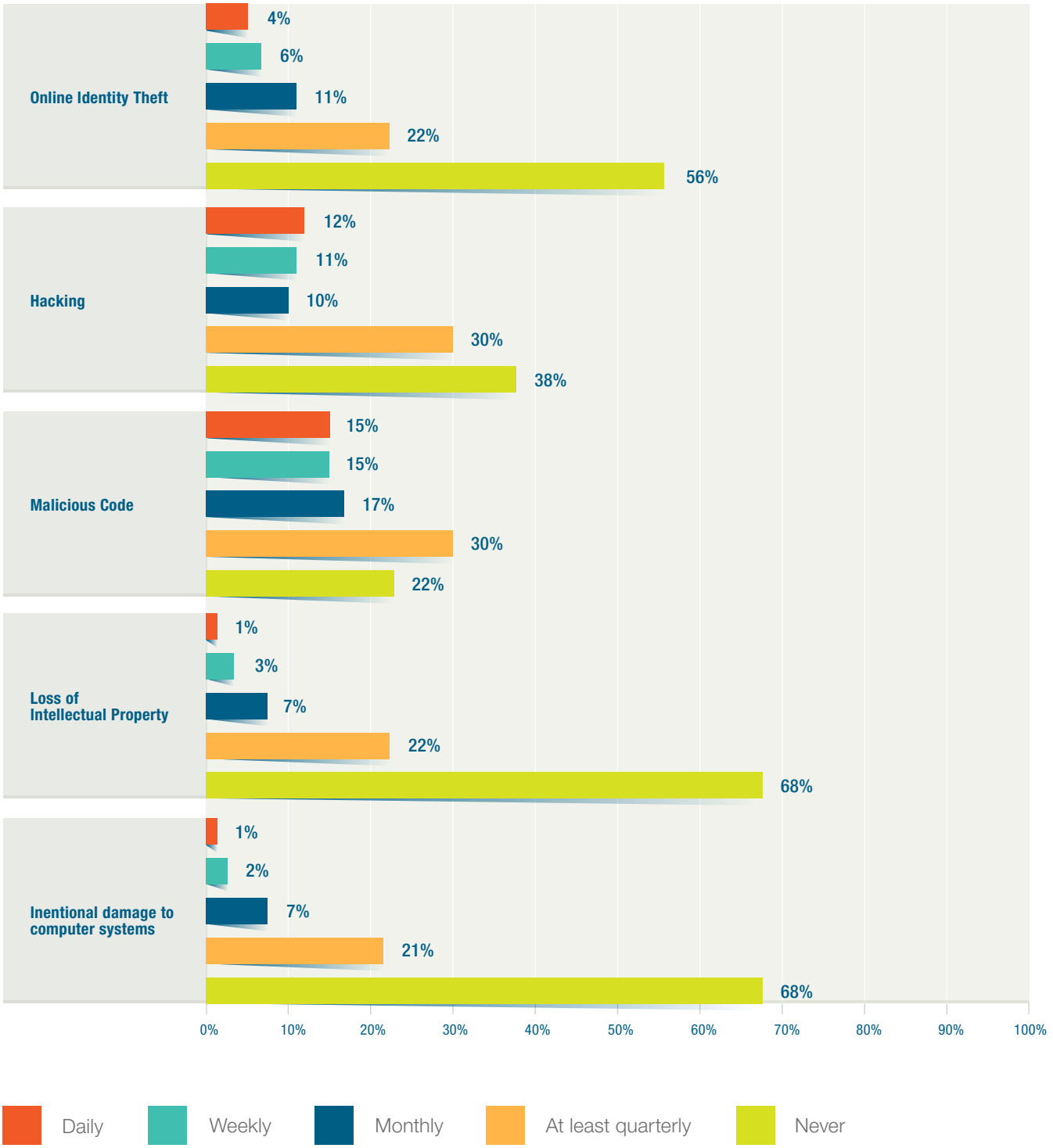


FIGURE 12 — FREQUENCY OF DIFFERENT TYPES OF CYBER-ATTACKS

How often, if at all, did your enterprise experience the following cyber-attacks in 2016?

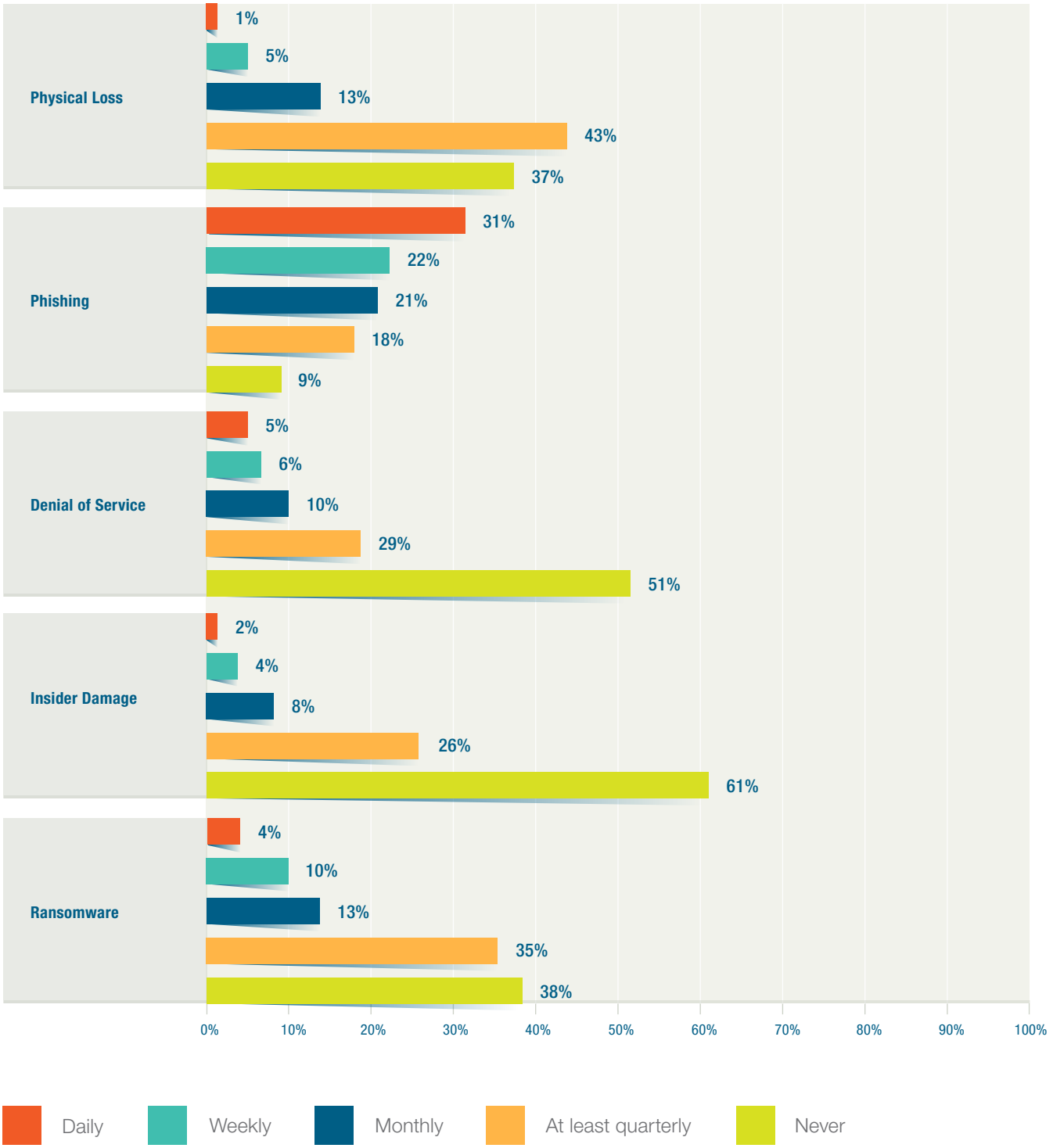


FIGURE 13 — PLAN FOR ADDRESSING RANSOMWARE ATTACKS

Do you feel that your board of directors has adequately prioritized enterprise security?

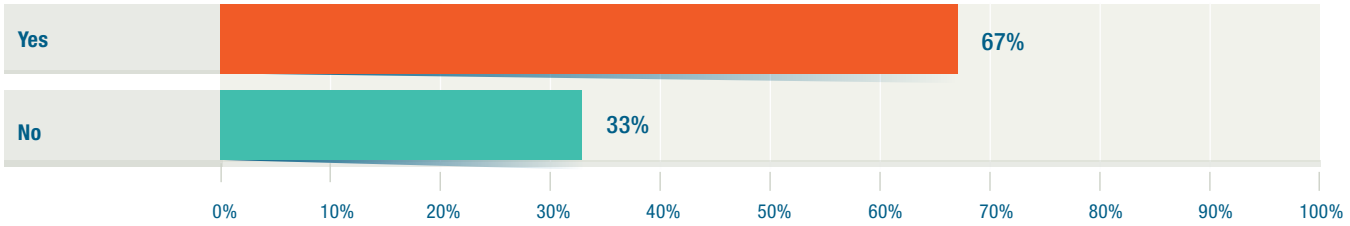
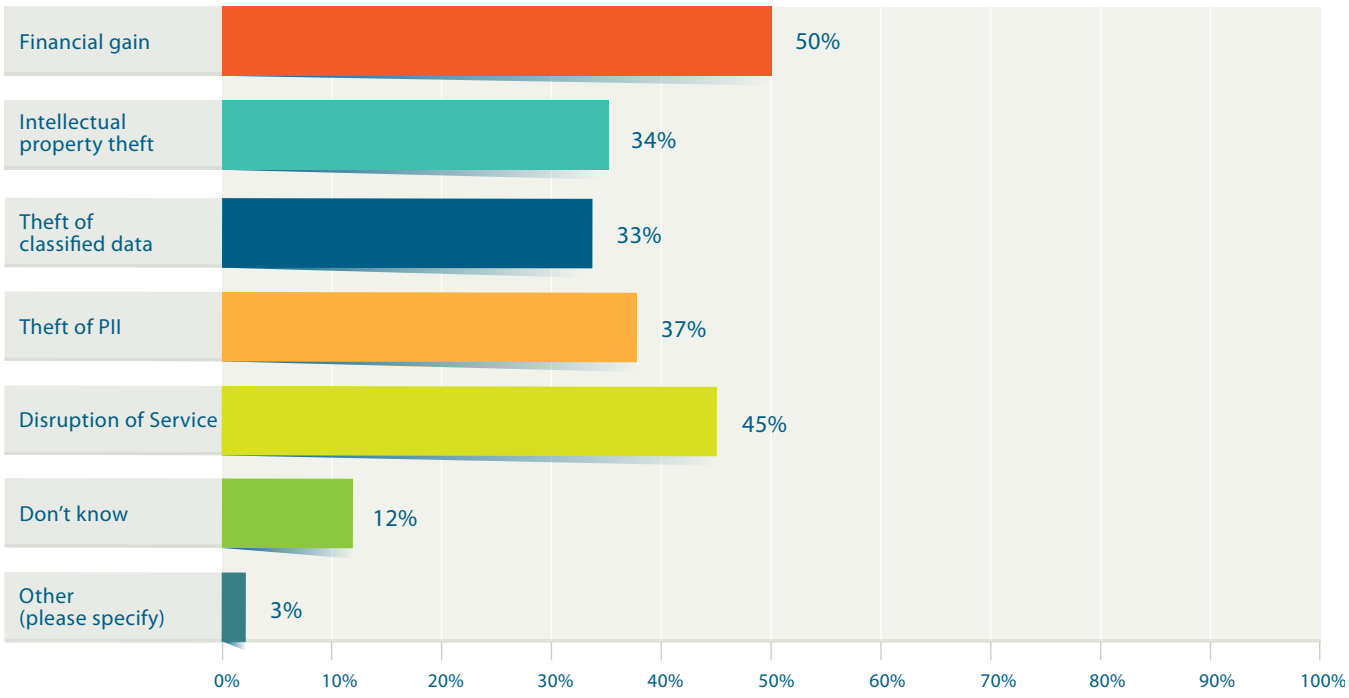


FIGURE 14 – ATTACK MOTIVATIONS

If your enterprise is attacked in 2017, what do you think the attacker's motivation(s) will be?



Conclusion

It is apparent that cyber security is evolving as a discipline. Although there is no shortage of the same threats, threat actors, tradecraft and attack techniques as in prior years, there have been some very evident shifts.

First and foremost, the skills gap continues unabated as noted in part 1 of this report and in prior years. However, unlike prior years, there are now other factors that can serve to exacerbate the issue. Specifically, potential slowdowns in the expansion of the cyber security budget can cause skill-related challenges to compound, particularly given that attacks are increasing year over year. For example, building a "bench strength" of future cyber security leaders for the enterprise implies that the right skills are there to begin with, and there is time to hone and expand those skills over time. When there is not—for example, when acquiring staff is challenging or when the enterprise is understaffed—the ability to invest in bench strength is eroded.

Likewise, new threats are emerging. New mechanisms for conducting cybercrime (e.g., ransomware) are prevalent, with many enterprises being slow to respond. New devices in the enterprise, such as IoT systems, are gaining prevalence and reflect an area of concern for practitioners. Although this does not presuppose a need to adopt different mechanisms or techniques in the practice of how cyber security is effected for these areas, it does imply that there are areas where cyber security staff members need to polish their skills over time.

As noted in prior year surveys, the large number of individuals who do not know if their enterprise had been breached reflects a broader systemic problem. Despite advances made in intelligence-driven cyber security approaches, many cyber security professionals still are not able to say with certainty whether or not an enterprise breach had occurred. This may be reflective of the fact that not all cyber security organizations are employing intelligence-driven or adversary campaign-aware methods, or it could indicate that not all cyber security personnel (particularly in a large enterprise) are charged with incident response or are normally aware of incident activity.

What This Means to Enterprises

- **Enterprises may want to work through ransomware attacks and plan response procedures in advance. Paying the ransom may seem appealing in the heat of the moment, but may not lead to the attacker following through; it can also lead to further attacks at a later time.**
- **Financial motivations of adversaries are likely to spur the development of increasingly sophisticated ransomware in the future. This may mean an uptick in the amount of malware and its sophistication.**

Afterword

In this report, we've examined a number of factors impacting the state of cyber security—from the persistent skills shortage, to the critical need for a stronger understanding of the business among security staff, to the concerning lack of readiness for threats such as ransomware.

ISACA's 2016 State of Cyber Security report showed that 50 percent of the responding organizations had CISOs. This year, 65 percent have them. This news is encouraging. This is a strong indicator that executive leadership and boards have made this an organizational priority and are putting resources in place to address the challenge.

Less encouraging, however, is that attacks like ransomware are on the rise, and only slightly more than half of organizations have a process in place to handle and recover from such incidents.

We must be proactive in developing our cyber readiness and cyber resilience. Preparedness and vigilance make us successful – but they also require action. As US President John F. Kennedy said, "There are risks and costs to action. But they are far less than the long-range risks of comfortable inaction."

What actions are needed? One is building and maintaining a strong cyber security workforce. Security professionals must not only be trained, but have their skills maintained using hands-on technical training and hands-on performance based assessment. And this must be done while also assuring that these professionals understand the nature of the businesses for which they work. We continue to see demand increase for this type of hybrid professional as organizations worldwide seek to find this elusive combination of skills.

We must also facilitate better information sharing—both better dissemination of what we know and better intelligence gathering so we know more—to ensure that organizations are as well connected to information on the latest threats as their adversaries are.

And we must give cyber security the resources required. This year's data indicate that budgets aren't expanding as rapidly as they have in the past. The problem? Companies still do not have the skills they need or the plans in place to prepare them for advanced cyber threats. These things take resources.

Consider that this year's survey found that only fewer than half of security leaders are confident in their team's ability to handle anything beyond simple cyber incidents. To say that is concerning is an understatement. Resources must be allocated to sharpening those skills and improving organizations' abilities to rapidly detect and respond to advanced cyber threats.

Not all is doom and gloom. More colleges and universities are developing cyber security programs. Associations like ISACA are equipping cyber security professionals with critical skills and working on ways in which organizations can better assess their cyber readiness. As mentioned previously, executive leaders and boards are recognizing the critical importance of cyber security. And more governments are now taking steps to protect infrastructure and increase cyber workforce capabilities.

Cyber security is everybody's business. We must continue to be vigilant about meeting the challenges created by cyber security, especially in a landscape where rapid technology changes and increasing complexity in the regulatory and compliance environment have become the norm. I look forward to seeing what next year's State of Cyber Security reveals.

Matt Loeb
CGEIT, CAE
ISACA CEO

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Phone: +1.847.253.1545

Fax: +1.847.253.1443

Email: info@isaca.org

Web site: www.isaca.org

Provide feedback:
www.isaca.org

Participate in the ISACA Knowledge Center:
www.isaca.org/knowledge-center

Follow ISACA on Twitter:
https://twitter.com/ISACANews

Join ISACA on LinkedIn:
http://linkd.in/ISACAOfficial

Like ISACA on Facebook:
www.facebook.com/ISACAHQ

ISACA®

ISACA® (***isaca.org***) helps professionals around the globe realize the positive potential of technology in an evolving digital world. By offering industry-leading knowledge, standards, credentialing and education, ISACA enables professionals to apply technology in ways that instill confidence, address threats, drive innovation and create positive momentum for their organizations. Established in 1969, ISACA is a global association serving more than 500,000 engaged professionals in 188 countries. ISACA is the creator of the COBIT® framework, which helps organizations effectively govern and manage their information and technology. Through its Cybersecurity Nexus™ (CSX), ISACA helps organizations develop skilled cyber workforces and enables individuals to grow and advance their cyber careers.

Disclaimer

ISACA has designed and created "State of Cyber Security 2017 Part 2: Current Trends in the Threat Landscape" (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

Reservation of Rights

ACKNOWLEDGMENTS

ISACA would like to recognize:

Lead Developer

Ed Moyle
Director, Emerging Business and Technology, ISACA

ISACA Board of Directors

Christos K. Dimitriadis
Ph.D., CISA, CISM, CRISC,
INTRALOT S.A., Greece, International Chair

Theresa Grafenstine
CISA, CGEIT, CRISC, CIA, CGAP, CGMA,
CPA, US House of Representatives, USA, Vice-chair

Robert Clyde
CISM, Clyde Consulting LLC, USA, Director

Leonard Ong
CISA, CISM, CGEIT, CRISC, CPP, CFE, PMP, CIPM,
CIPT, CISSP ISSMP-ISSAP, CSSLP, CITBCM, GCIA,
GCIH, GSNA, GCFA, Merck, Singapore, Director

Andre Pitkowski
CGEIT, CRISC, OCTAVE, CRMA, ISO27kLA, ISO31kLA,
APIT Consultoria de Informatica Ltd., Brazil, Director

Eddie Schwartz
CISA, CISM, CISSP-ISSEP, PMP,
Dark Matter, LLC, USA, Director

Jo Stewart-Rattray
CISA, CISM, CGEIT, CRISC, FACS CP,
BRM Holdich, Australia, Director

Tichaona Zororo
CISA, CISM, CGEIT, CRISC, CIA, CRMA,
EGIT | Enterprise Governance (Pty) Ltd.,
South Africa, Director

Zubin Chagpar
CISA, CISM, PMP, Amazon Web Services,
UK, Director

Rajaramiyer Venketaramani Raghu
CISA, CRISC, Versatilist Consulting India Pvt. Ltd.,
India, Director

Jeff Spivey
CRISC, CPP, Security Risk Management Inc.,
USA, Director

Robert E Stroud
CGEIT, CRISC, Forrester Research,
USA, Past Chair

Tony Hayes
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA,
Queensland Government, Australia, Past Chair

Greg Grocholski
CISA, SABIC, Saudi Arabia, Past Chair

Matt Loeb
CGEIT, FASAE, CAE, ISACA, USA, Director