State of Cybersecurity
Implications for 2016
An ISACA and RSA Conference Survey

RSA Conference | Where the world talks security

ISACA
Trust in, and value from, information systems

The State of Cybersecurity

In November and December 2015, ISACA and RSA Conference conducted a global survey of 461 cybersecurity managers and practitioners. Survey participants confirmed that the number of breaches targeting organizational and individual data continues to go unchecked and the sophistication of attack methodologies is evolving. The current state of global cybersecurity remains chaotic, the attacks are not expected to slow down, and almost 75 percent of respondents expect to fall prey to a cyberattack in 2016. Cybercriminals are the most prevalent attackers and continue to employ social engineering as their primary initial attack vector.

As the rate of incidents continues to escalate, the magnitude of related brand, reputation, and fiscal impact is driving organizations to address cybersecurity risk. Executive leadership teams are demonstrating cybersecurity resiliency support by taking a more active role in enforcing policy, mandating awareness training, supporting budgetary increases for cybersecurity-related technology and training, and modeling the way by practicing good cybersecurity practices themselves. Although enterprises continue to increase spending and effort on cybersecurity, respondents indicate that they struggle to fill positions with highly skilled workers—60 percent of all respondents do not believe their information security staff can handle anything more than simple cybersecurity incidents.

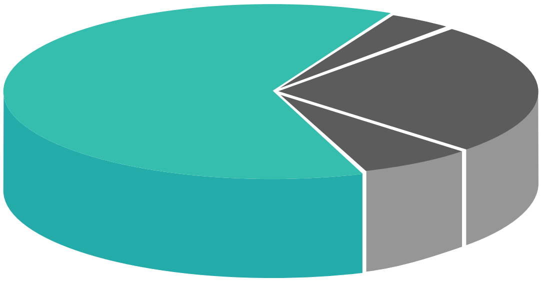
Survey Methodology

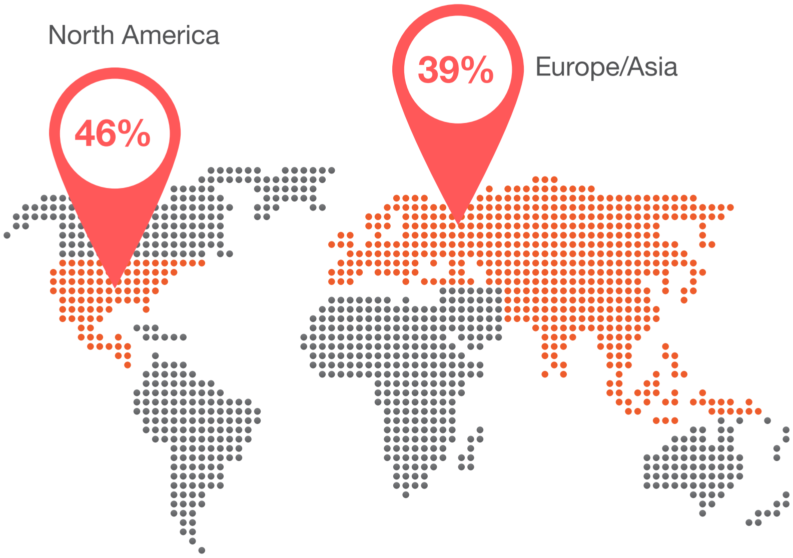
An invitation to participate in the survey was emailed to a global population of cybersecurity professionals composed of individuals holding ISACA's Certified Information Security Manager® (CISM®) and Cybersecurity Nexus Practitioner™ (CSX Practitioner™) designations, individuals in information security positions, RSA Conference's Loyalty Plus customers, and individuals preregistered for the 2016 RSA Conference. The survey data were collected anonymously through SurveyMonkey®. The results reveal many interesting findings that indicate positives and negatives for cybersecurity professionals. The survey, which used multiple-choice and Likert scale formats, was organized in four major sections:

- Demographics
- Organizational security
- Threats, attacks and crime
- Emerging trends

The populations invited to respond to the survey were selected ISACA certification holders and RSA Conference constituents. Due to the nature of the survey, the targeted population consisted of individuals who have cybersecurity job responsibilities. More than 842 individuals participated, of which 461 indicated that their primary job function is cybersecurity or information security. The data represented in this report reflect the information provided by those 461 individuals. A typical respondent can be described as:

81%
A member of ISACA



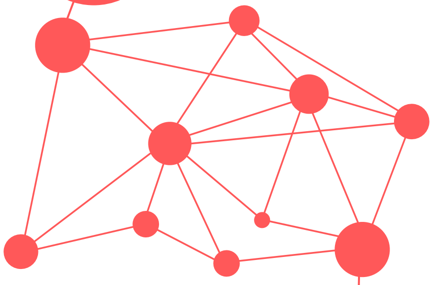


21%

Working in technology services/consulting

22%
financial services

79% Cybersecurity/ Information Security Management



Cybersecurity/ Information Security Practitioners 21%

69%

Employed in an enterprise with at least 1,000 employees

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 Representation
In which of the following industries are you employed?

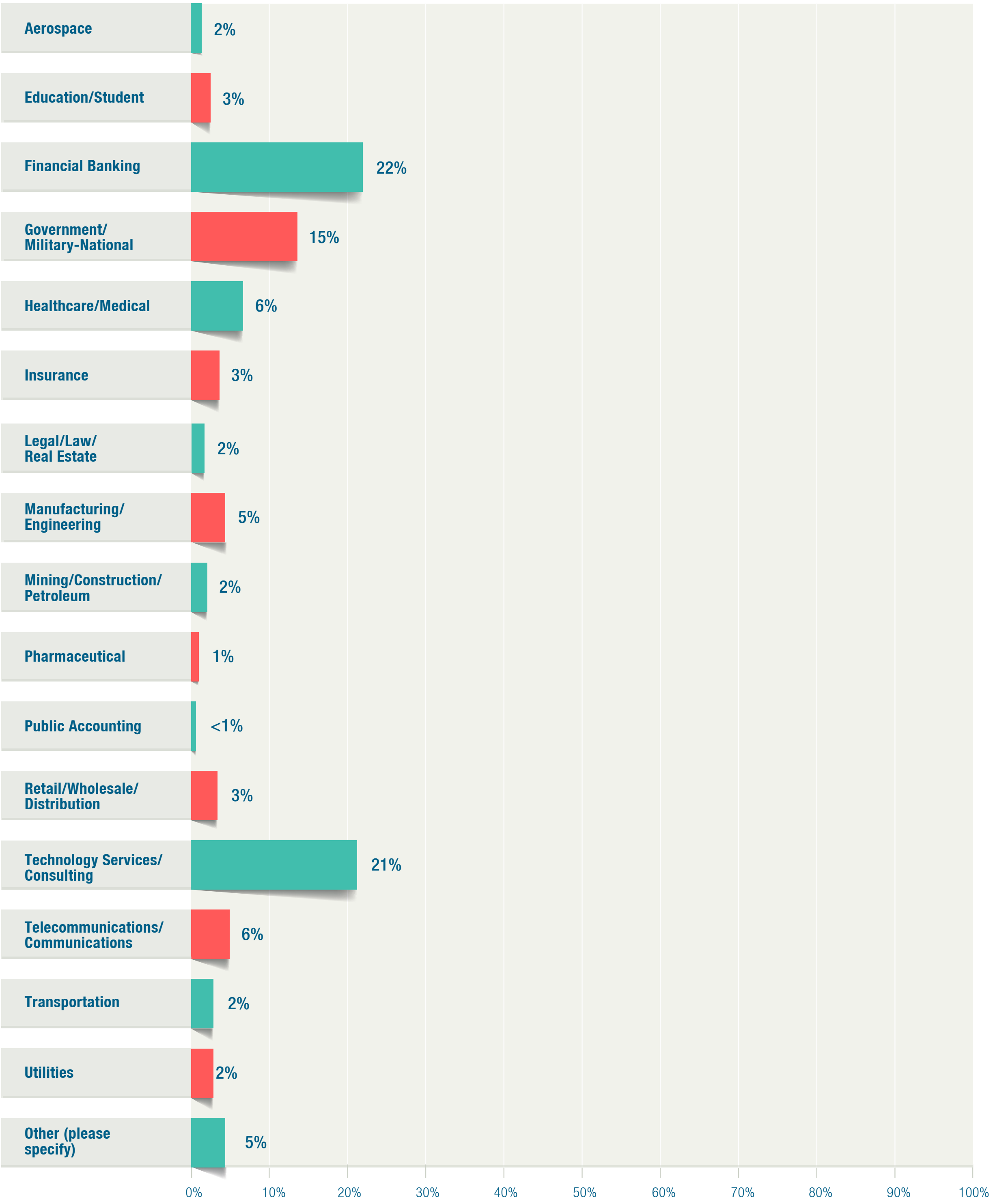
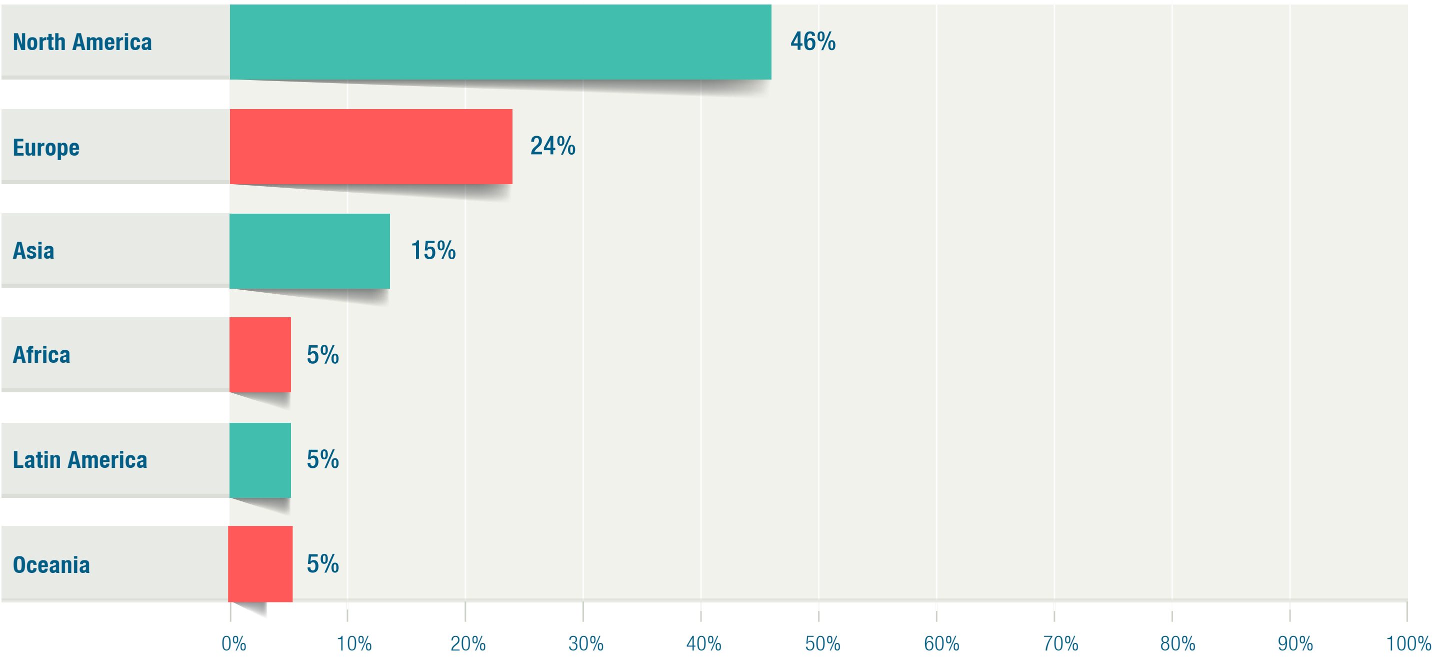


Figure 2—Geographic Representation
In which region do you reside?



Organizational Security

Cybersecurity incidents continue to escalate in frequency and impact to enterprises. Each year breaches headline the news with the resulting enterprise impact such as loss of customer confidence, financial loss and, in some situations, the inability of an enterprise to recover and eventual shut down. It is clear that security breaches are not a remote threat any longer but are now fact. Enterprises are dealing with attacks daily **(figure 3)** and they must be prepared to deal with adversaries that are evolving and motivated to achieve their goal. In order to address the threat landscape, enterprises must have continued focus on cybersecurity risk so they can achieve resilience when an incident does occur.

Fortunately, this year's data demonstrate a plan for better governance. Security has become a board and executive level issue. In fact, 82 percent of respondents report that their enterprise board of directors is "concerned" or "very concerned" about cybersecurity **(figure 4)**. As the interest of the board is a positive indicator for security, so is the fact that executives are actively demonstrating support for the security program. While enterprise leadership appears to be concerned with security and has taken an increased level of interest in the impact that security has on the organization, the reporting structure for security has not matured as just 21 percent of chief information security officers (CISOs) report to the chief executive officer (CEO) or the board, while most (63 percent) report through the chief information officer (CIO) **(figure 5)**. This reporting structure is unfortunate as it positions security as a technical issue rather than a business concern.

Figure 3—Type and Frequency of Malicious Activity Occurrences

Please select the type and frequency of malicious activity occurrences that may have affected your organization in 2015. (Check all that apply.)

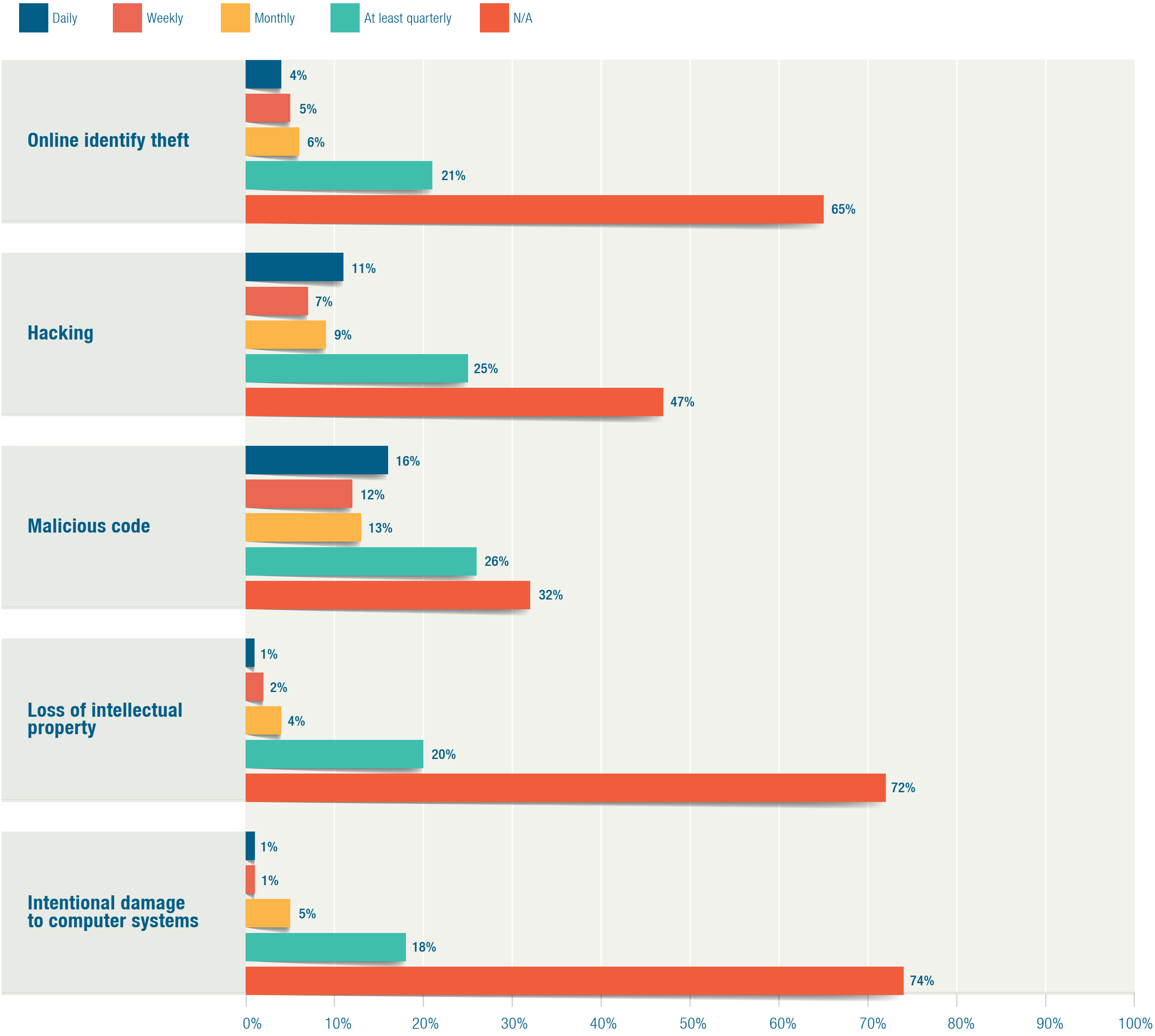


Figure 3—Type and Frequency of Malicious Activity Occurrences (Continued)

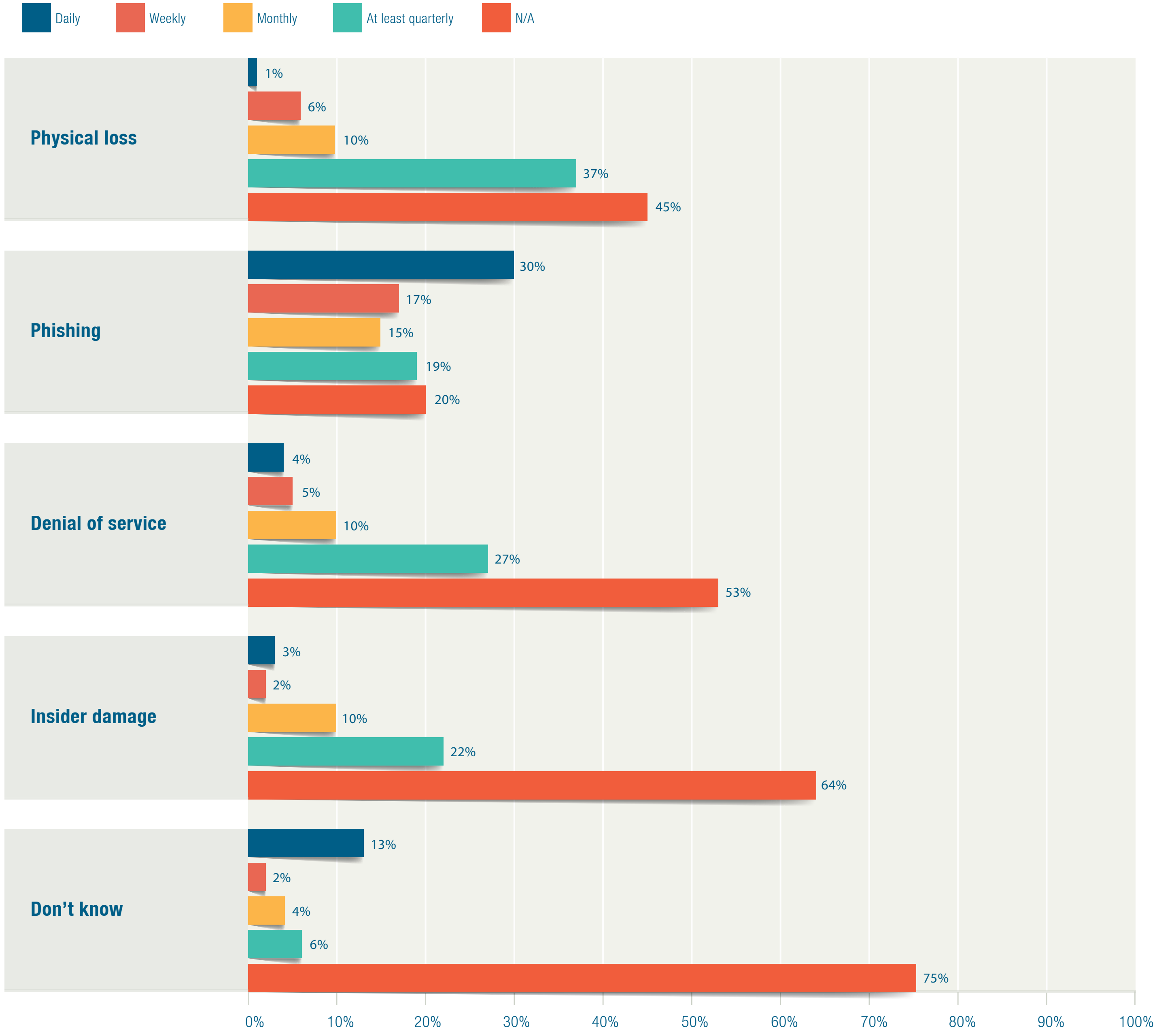


Figure 4—Board of Directors Concern
How concerned is your organization's board of directors about cybersecurity/information security?

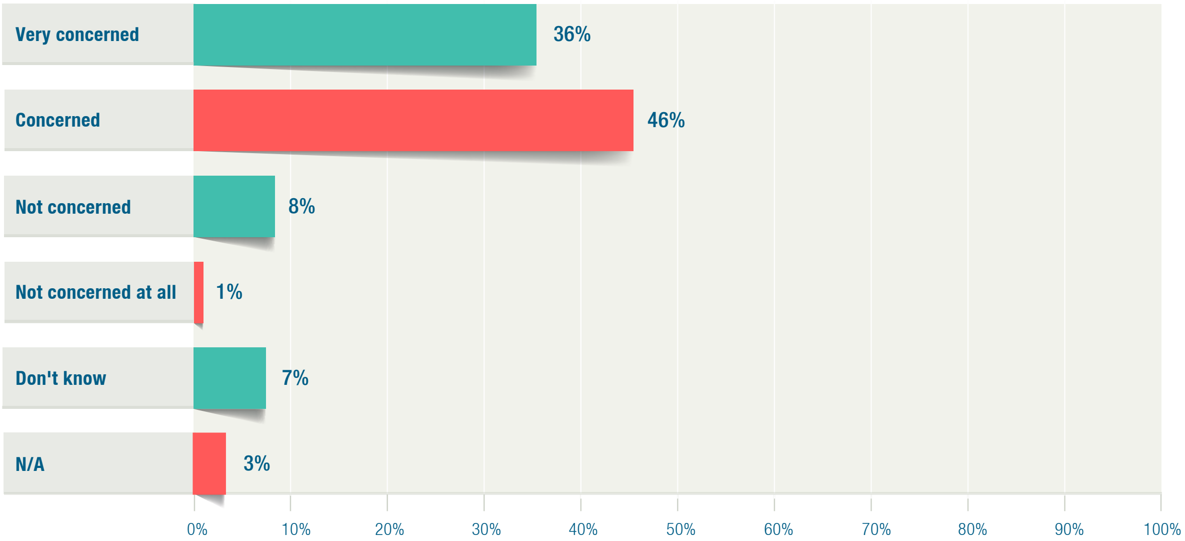
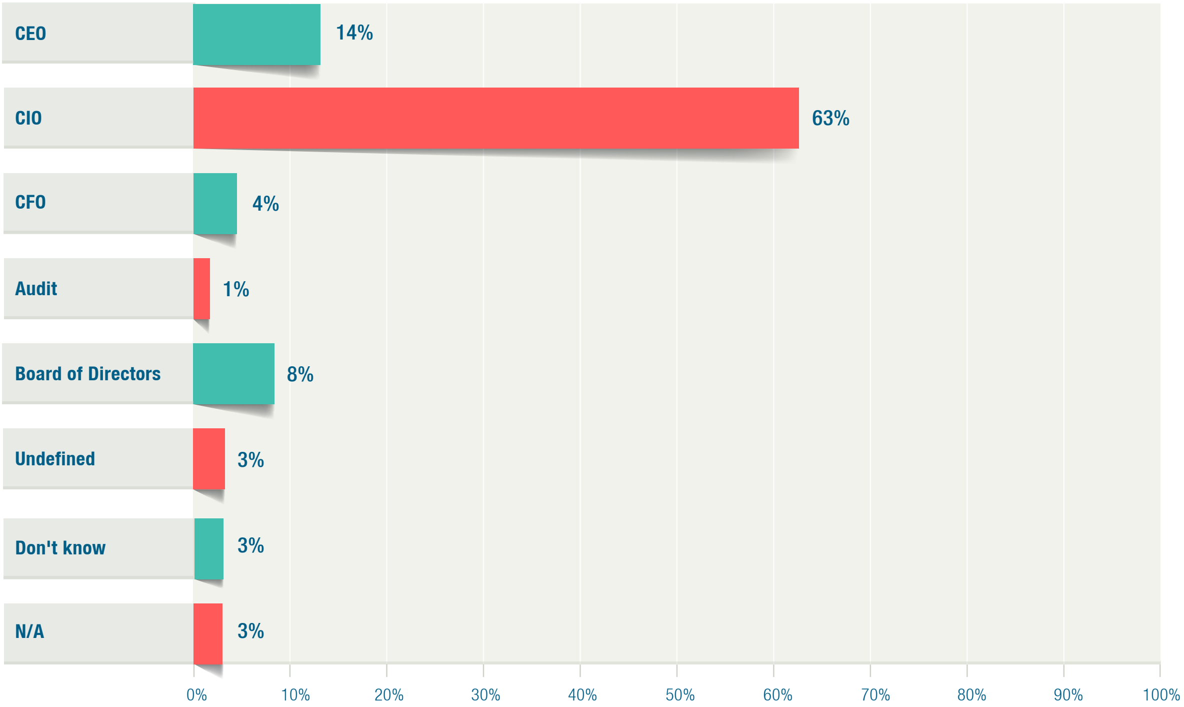


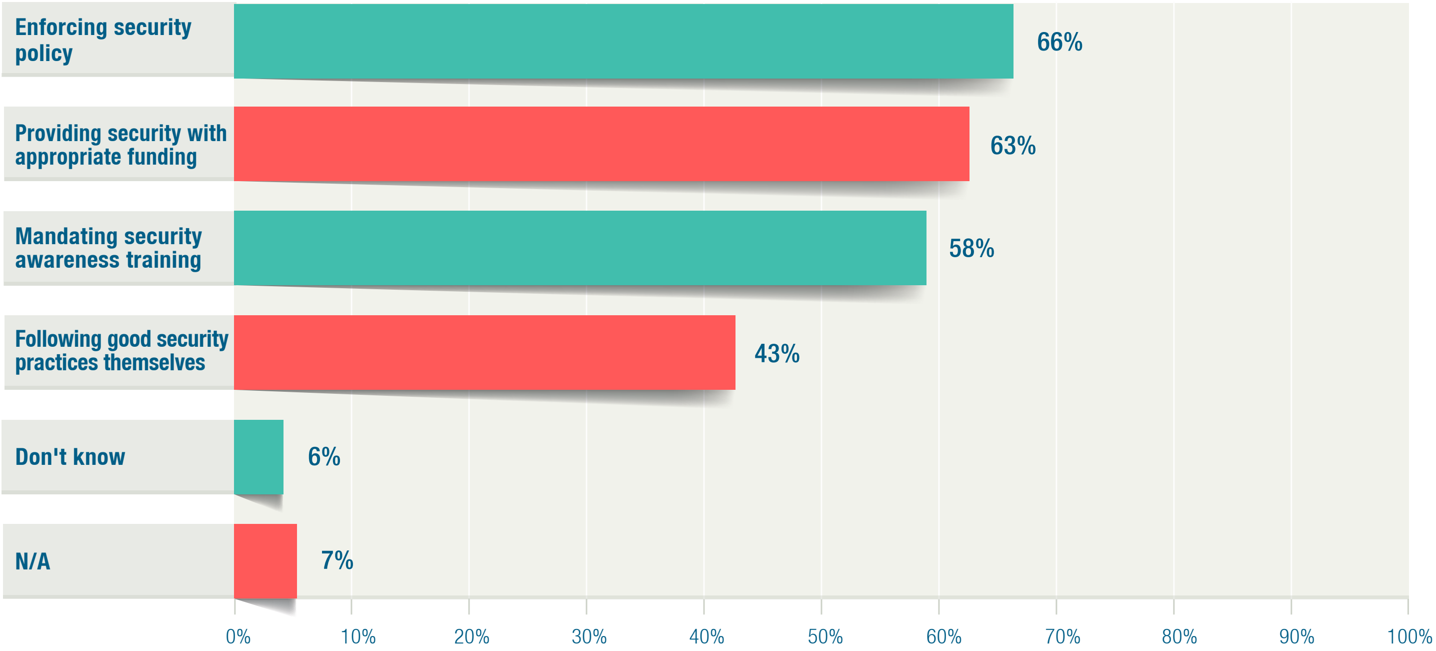
Figure 5—Reporting Structure for Cybersecurity
Where does the cybersecurity/information security function report within your organization?



While the security team is frequently still positioned within IT, there is clear evidence that enterprise executives are supporting the program. Support from the executive team comes in a variety of activities such as enforcing policy, providing appropriate funding, and mandating awareness training **(figure 6)**. Sixty-one percent surveyed state that they expected an increase in their cybersecurity budgets in 2016. Budgeted items include increased pay for skilled workers, skills development training, awareness programs and response planning. In addition to increased spending on cybersecurity, 75 percent of respondents report that their organizations' cybersecurity strategy now aligns to enterprise objectives.

Figure 6—Executive Team Support to Cybersecurity Risk Mitigation

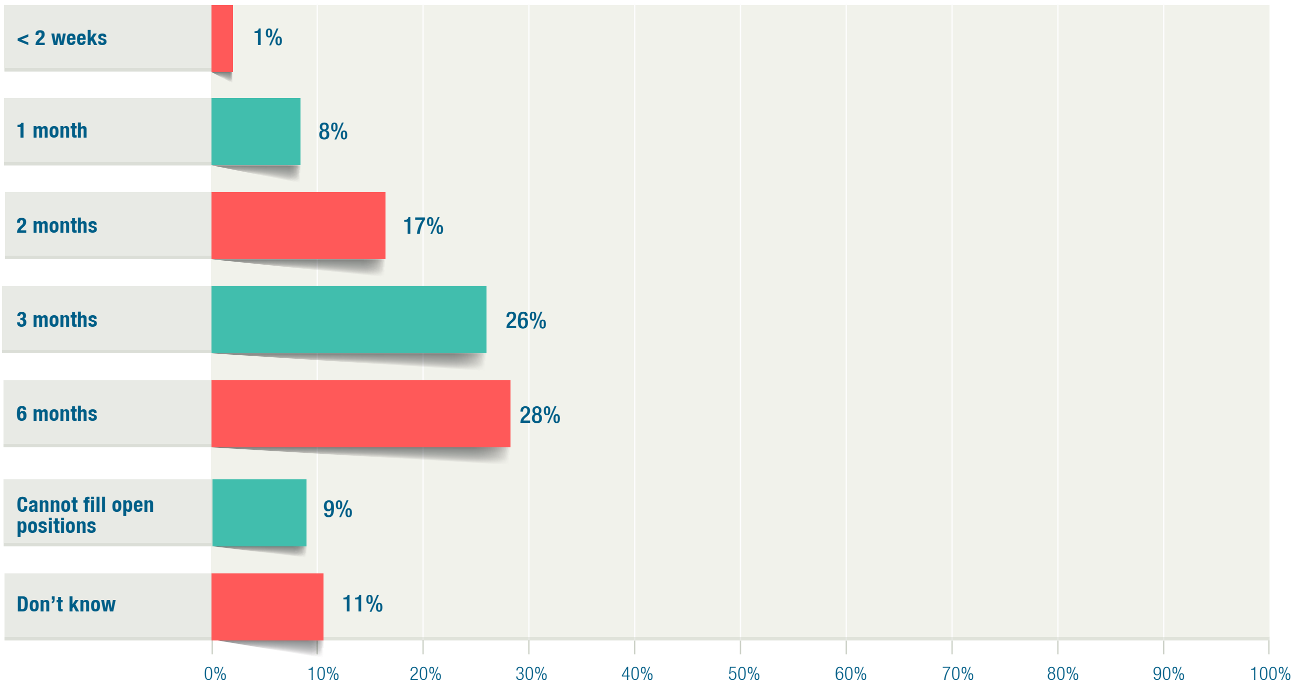
How does your organization's executive team demonstrate support to cybersecurity risk mitigation?



As mentioned previously, reports indicate that the cybersecurity profession is struggling to find well-trained and highly skilled workers to fill open positions. Many factors, including increased attention to cybersecurity by governments and enterprises as well as an evolving threat landscape, are combining to create an expected exponential increase in cybersecurity jobs that will require skilled professionals. "The 2015 (ISC)^2 Global Information Security Workforce Study" reported that the information security workforce shortfall is widening.[1] In 2015, 62 percent of the study's respondents stated that their organizations have too few information security professionals. This compares to 56 percent in the 2013 study. The report concludes that this decline is not about shortfalls in organizational budgets, but rather an insufficient pool of suitable/skilled candidates as the cause. The shortfall is negatively impacting organizations and their customers, leading to more frequent and costly data breaches. The ISACA/RSA Conference survey data from both 2014 and 2015 confirm that organizations are having a difficult time hiring skilled people. The 2015 survey indicated that just over half (53 percent) of organizations require at least three months to fill open cybersecurity positions and nine percent could not fill the positions at all **(figure 7).**

Figure 7—Filling Open Cybersecurity Positions

On average, how long does it take to fill a cybersecurity/information security position within your organization?

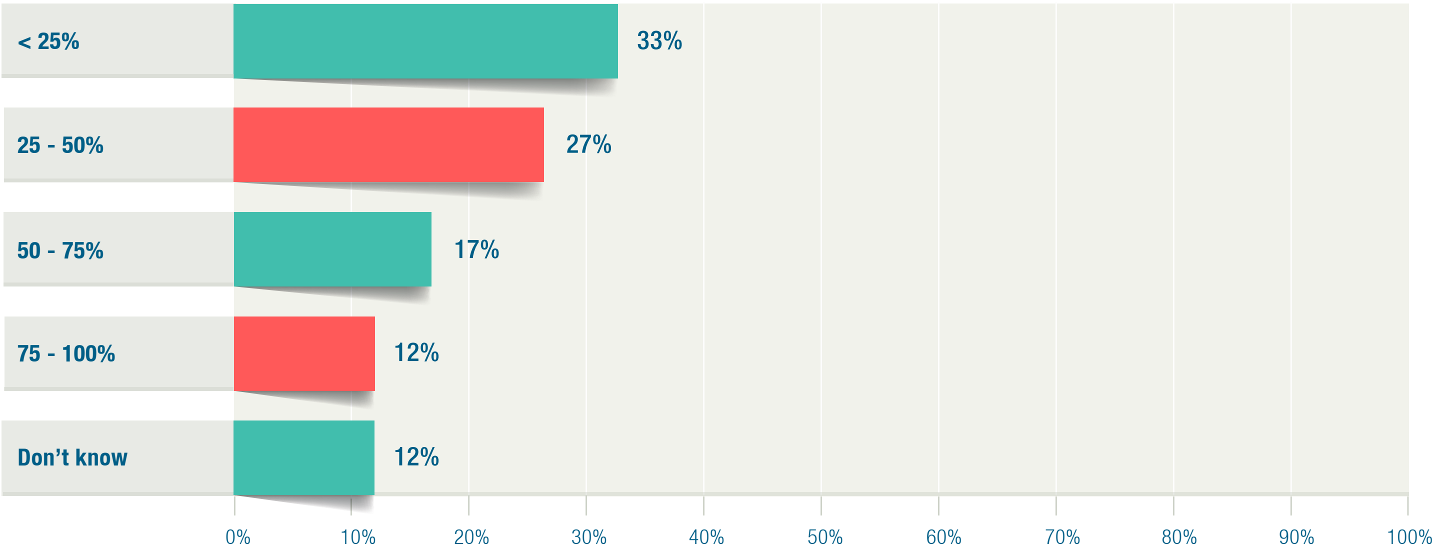


While most organizations are eventually able to hire professionals into cybersecurity and information security positions, most applicants submitting resumes do not have adequate skills to meet the needs of the business. In 2014, 50 percent of respondents reported that less than half of the job candidates their organizations reviewed were considered "qualified upon hire." In 2015, that percentage increased, with 59 percent noting the lack of qualification of half of the job candidates **(figure 8).**

[1] Suby, Michael; Frank Dickson; "The 2015 (ISC)^2 Global Information Security Workforce Study," Frost & Sullivan, in partnership with (ISC)2, Booz Allen Hamilton, NRI Secure Technologies and Cyber360, 2015, https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

Figure 8—Qualified Applicants

On average, how many cybersecurity/information security applicants are qualified upon hire?

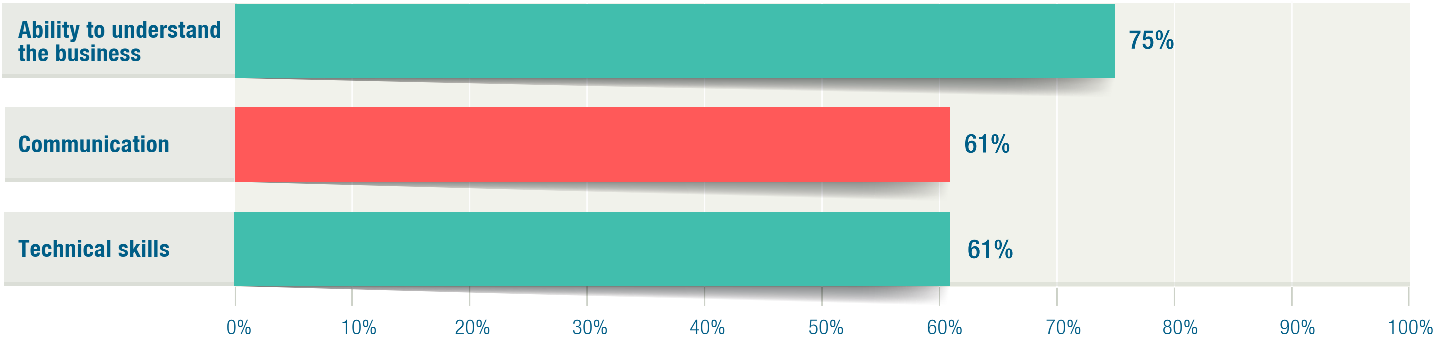


As in 2014, the 2015 respondents reported that lack of hands-on skills is the most important factor in judging a candidate not qualified for a position. The second most frequent reason for not considering a candidate qualified is lack of a certification. When asked why qualified candidates were not hired (excluding those who turned down the position), respondents reported that the flexibility of the job requirements and starting salaries were the two biggest roadblocks to obtaining skilled employees.

Security managers continue to see a skills gap among existing employees as well. Survey participants overwhelmingly reported that the largest gap exists in cybersecurity and information security practitioners' ability to understand the business; this is followed by technical skills and communication **(figure 9).** Not having skilled employees certainly impacts an enterprise's ability to identify, contain and mitigate complex security incidents, which results in increased cost to the enterprise.

Figure 9—Cybersecurity Skills Shortage

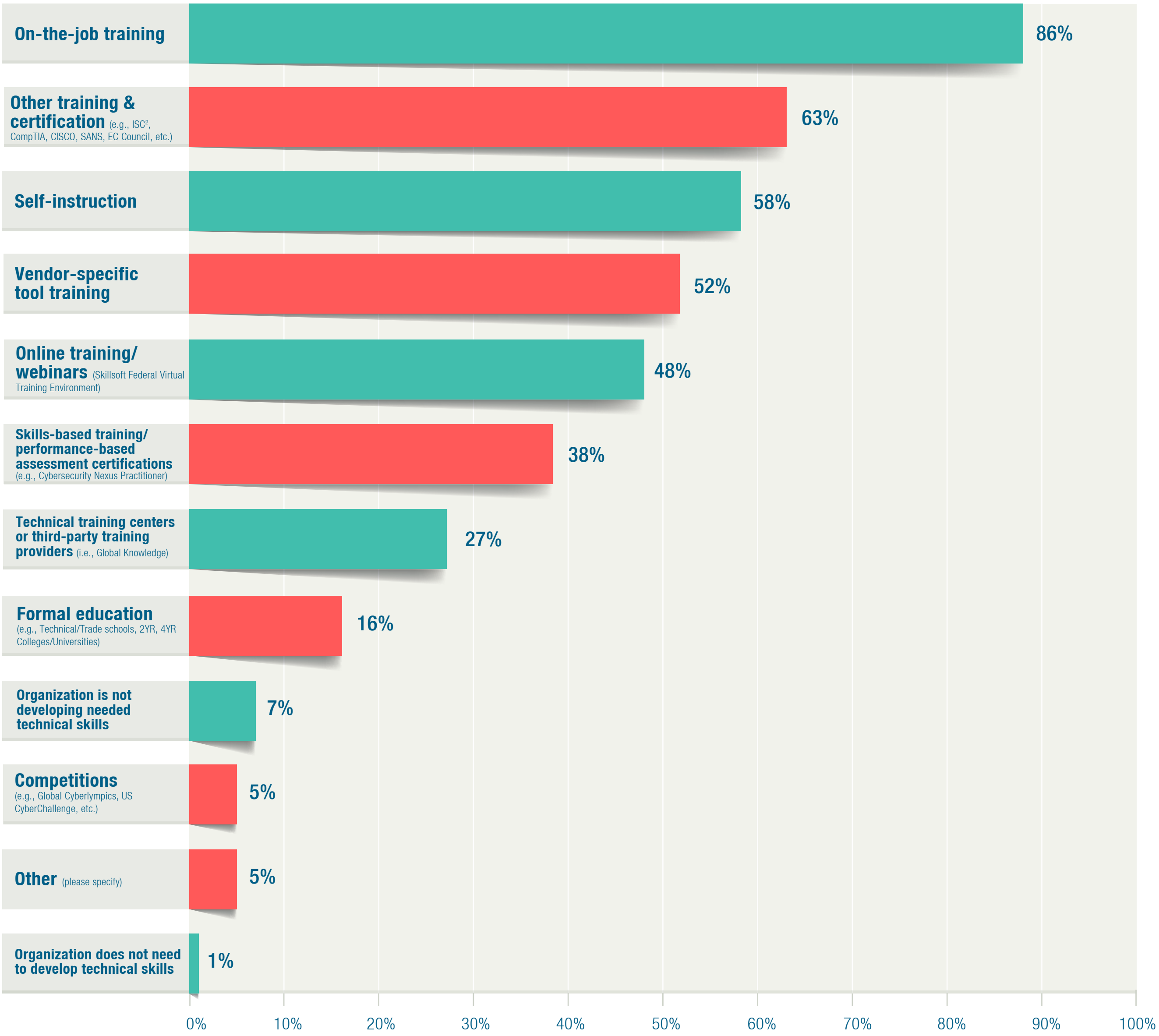
What are the most significant skills gaps you or your organization sees among today's cybersecurity/information security professionals?



While respondents recognize that they need to provide technical training for current employees, only 13 percent of participants reported that their organizations spent more than US $50,000 on training and skills development. In order to close the skills and knowledge gaps, enterprises still rely upon on-the-job training, training vendors and self-instruction to educate their existing workforce. While on-the-job training remains primary, a sharp increase in skills-based training and performance-based assessments is noted among techniques being employed by organizations to address the skills gap **(figure 10).**

Figure 10—Developing Technical Skills

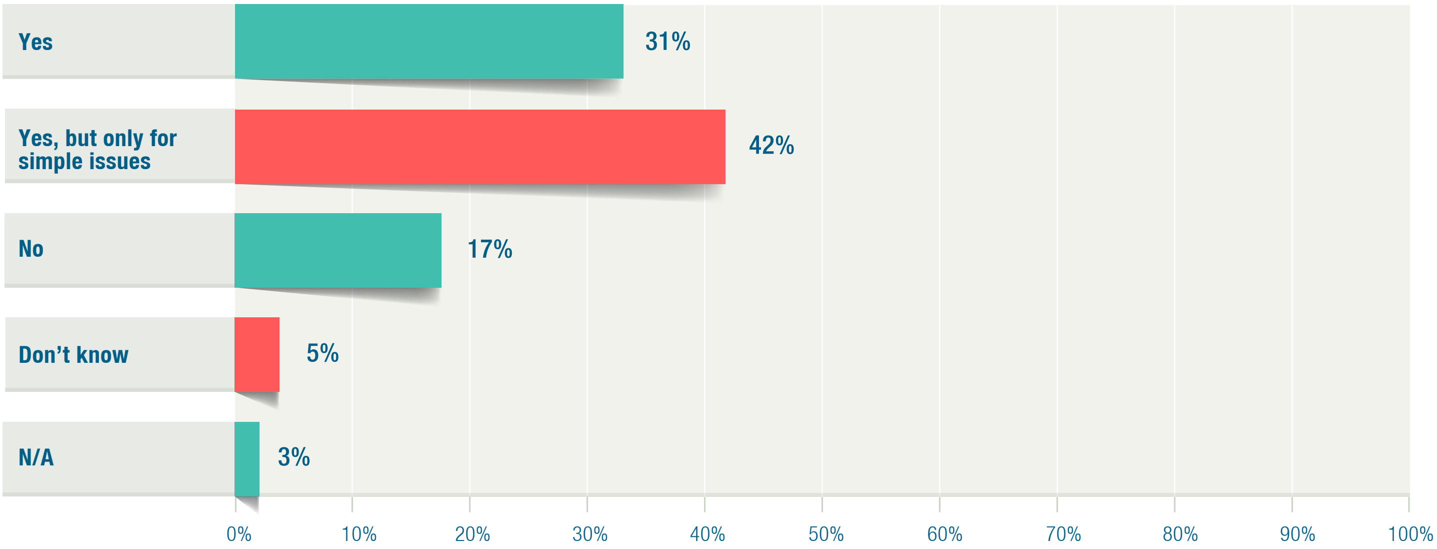
The 2015 State of Cybersecurity Survey indicated that nearly 65 percent of all entry-level cybersecurity applicants lacked the requisite skills to perform the tasks related to the jobs they were seeking. How is your organization developing those needed technical skills? (Check all that apply.)



While many respondents report having an experienced staff that they rely on, they also recognize that experience is not a determinant of requisite skills to deal with complex security incidents. The survey data indicate that 92 percent of respondents' organizations' information security/cybersecurity staff average at least three years of experience and 73 percent average more than five years of experience, yet respondents are not feeling comfortable with their teams' ability to detect and react. In 2014, 87 percent of respondents reported that they are comfortable with their security teams' ability to detect and respond to incidents; however, that sense of comfort slipped to 75 percent in 2015. Of that 75 percent, 42 percent indicated that their comfort with the team's ability is limited to simple incidents only **(figure 11).**

Figure 11—Detection and Response Confidence

Are you comfortable with your cybersecurity/information security team's ability to detect and respond to incidents?



The survey results indicate that organizations continue to focus on increasing cyber resilience through sharing information, aligning cybersecurity policy with organizational objectives, and increasing investment in cybersecurity personnel, technologies and related services. Although efforts to recruit talent have expanded from 2014, organizations still struggle with the skills gap that exists among applicants and seasoned professionals. Even though significant increases in training spending occurred in 2015, the methods that are most commonly used (e.g., on-the-job training, knowledge-based vendor training or self-training) have not closed the gap. This is evidenced by the decrease in ratings indicating the respondents' degree of comfort that their organizations' cybersecurity professionals can handle evolving threats.

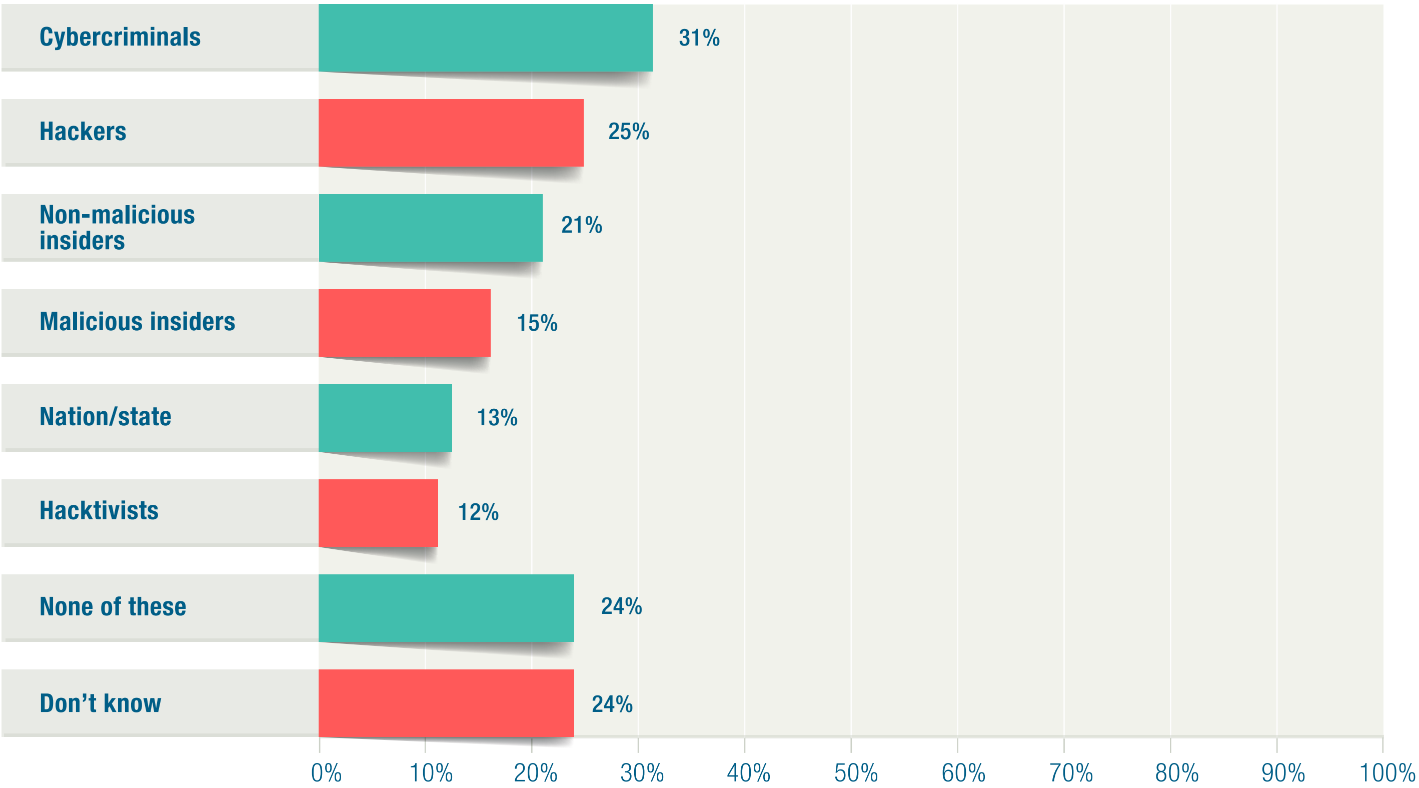
Threats, Attacks and Crime

While attacks have become more sophisticated and the motivations behind them seem to evolve on a daily basis, the perpetrators can be fairly clearly categorized. Primary categories focus on breaches that lead to financial gain, intellectual property theft, theft of classified data, theft of personally identifiable information (PII) and disruption of service.

Like the 2014 ISACA/RSA Conference survey, the 2015 data demonstrate that the threat actors that most frequently penetrate enterprise security include cybercriminals, hackers and non-malicious insiders **(figure 12).**

Figure 12—Threat Actors

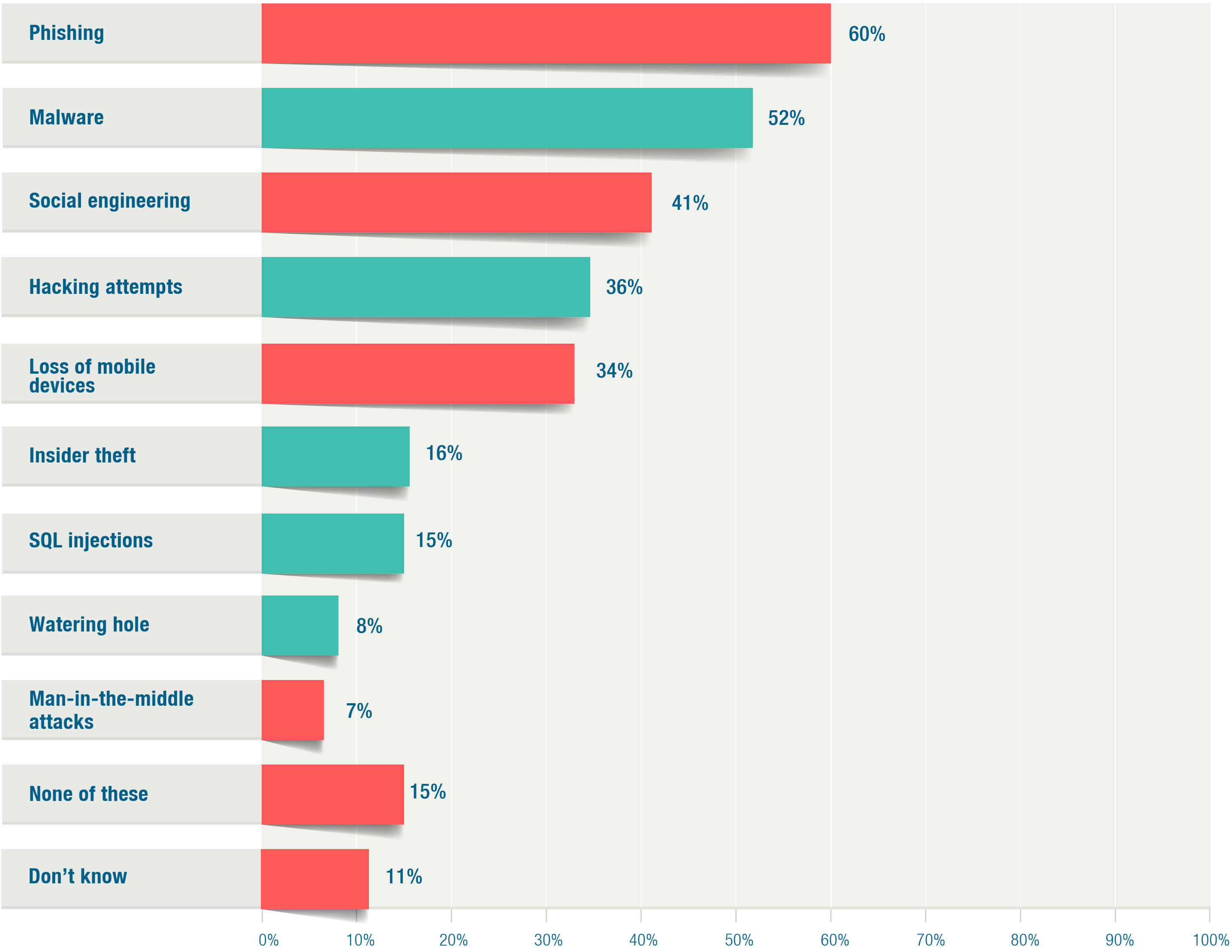
Which of the following threat actors exploited your organization in 2015?



The survey also asked respondents to indicate which attack types most commonly penetrated their enterprises' networks. The responses show that the most prevalent successful attack types hinge on the human factor. According to respondents, the attack types that most frequently exploited their organizations in 2015 were (in order) phishing, malware and social engineering **(figure 13)**. In 2015, social engineering moved ahead of hacking attempts, the attack type that was third in the 2014 survey. The biggest change from the 2014 to the 2015 data is the 13 percent decrease in loss of mobile devices.

Figure 13—Successful Attack Types

Which of the following attack types have exploited your organization in 2015?



While technical and administrative controls can aid in mitigating or at least delaying many of these attack types, often the human factor is the biggest weakness. Training people on how to detect and react to potential security attacks is widely believed to decrease the effectiveness of a particular attack vector. Correspondingly, a significant majority (87 percent) of the survey respondents reported having an awareness program in place and, of these, 53 percent believe it to be effective. It is troubling, however, that this percentage represents a significant drop from 2014, when 71 percent believed the awareness program to be effective.

Curiously, almost 24 percent of respondents indicated that they did not know which threat actors exploited their organizations. The survey highlighted a global lack of cyber situational awareness, which is surprising given that respondents are those who self-reported that cybersecurity or information security is their primary role. When asked whether their organization had fallen victim to an advanced persistent threat (APT) attack in 2015, 23 percent did not know, down slightly from 30 percent in the 2014 survey. Further situational awareness concern is generated by the data showing that 20 percent of respondents did not know whether they had any corporate assets hijacked for botnet use and 24 percent did not know if any user credentials were stolen in 2015 (up from 22 percent in 2014).

Organizations are expecting to see an increase in both the frequency and the devastating impact of cyberattacks. More than 71 percent of the ISACA/RSA Conference survey respondents stated that their organizations are “very likely” or “likely” to experience a cyberattack in 2016 **(figure 14)**. When asked what attack method is most likely in 2016, survey participants point toward social engineering vectors (e.g., phishing, water holing). Nearly one-third of participants voiced the opinion that financial gain is likely to be the motive for upcoming cyberattacks **(figure 15)**.

Figure 14—Likelihood of Cyberattacks in Respondents’ Organizations in 2016
How likely is it that your organization will experience a cyberattack in 2016?

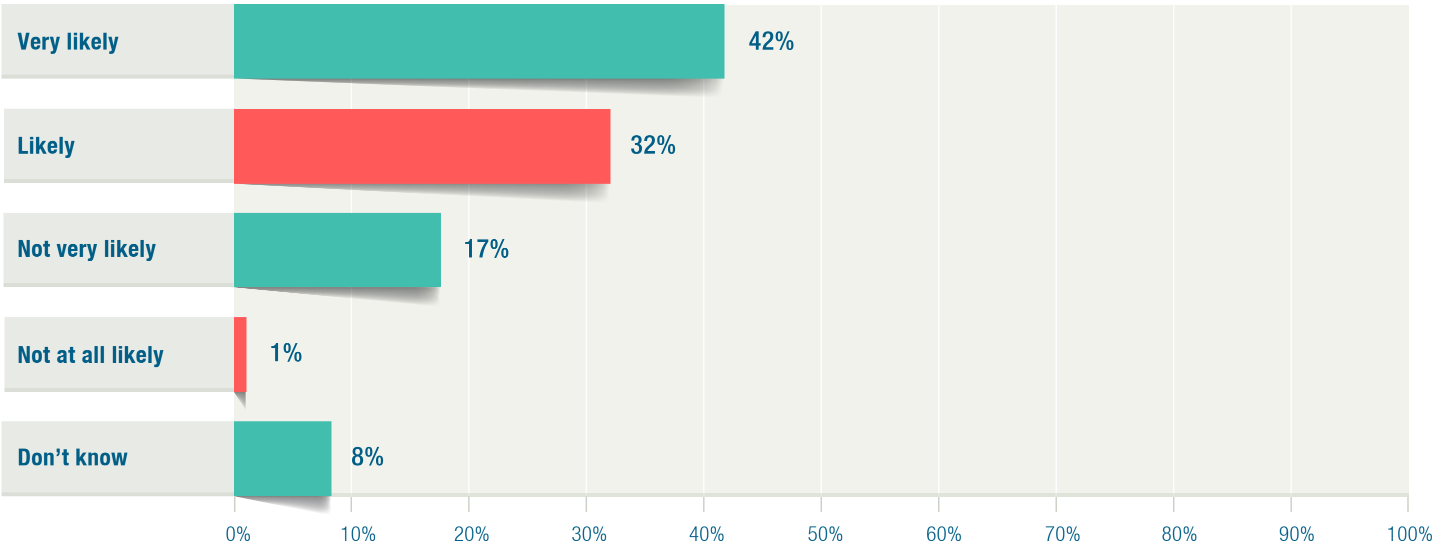
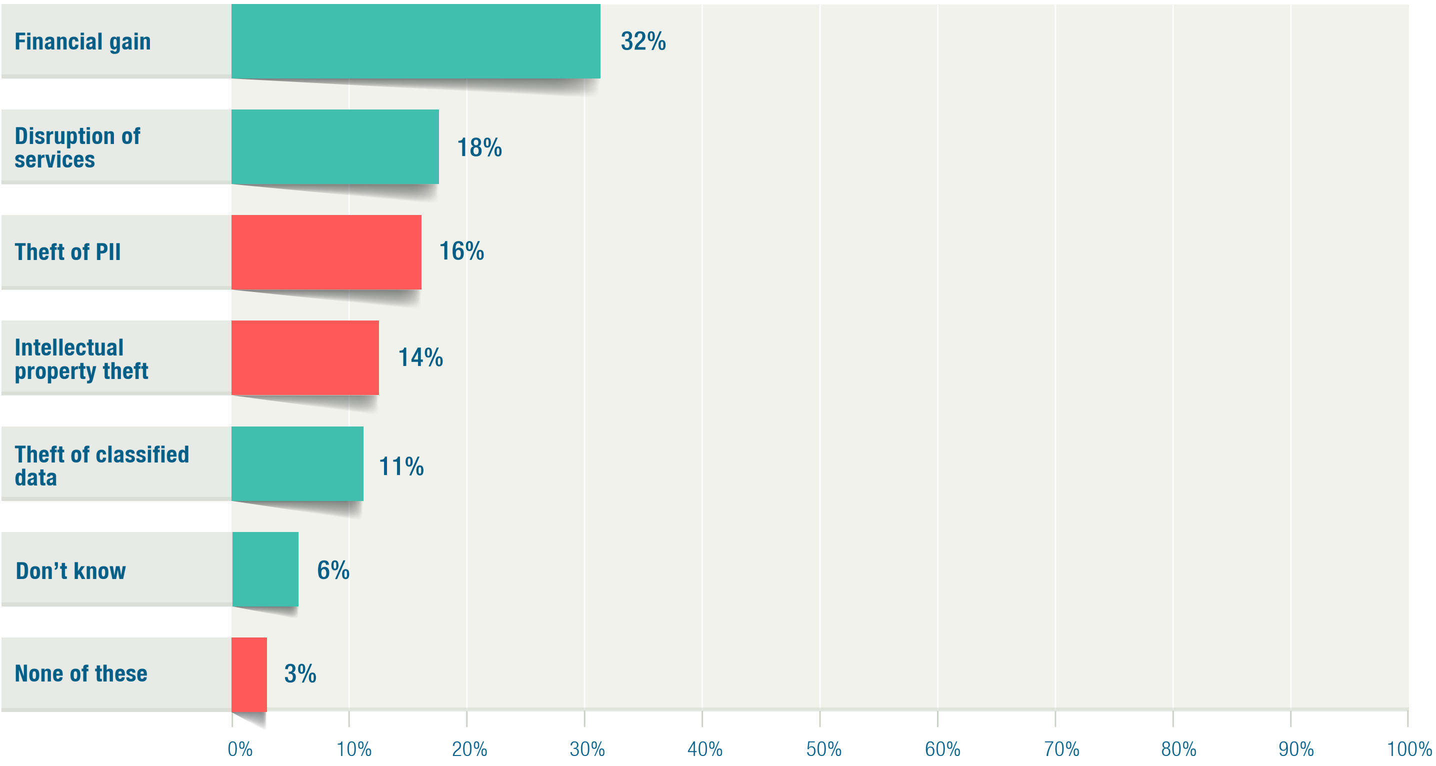


Figure 15—Motivation for Attack
What do you think the cyberattack motivation will be?

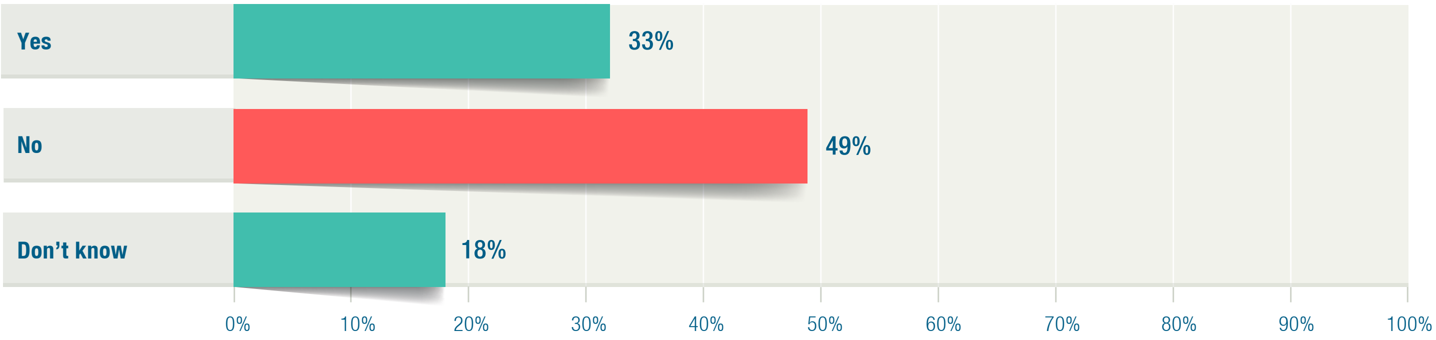


Crime should not be considered separately from other cybersecurity attacks for the purpose of identifying and prioritizing incidents. However, as in 2015, this survey carved out a specific, focused view of crime to determine how enterprises are handling the issue. While 31 percent of respondents state that cybercriminal activity is the biggest threat to enterprise cyber resiliency, almost half (49 percent) of respondents reported that their enterprise was not a victim of a cybercrime in 2015 **(figure 16)**, which is a decrease of 10 percent from the previous year. However, 33 percent confirmed that they experienced cybercrime in 2015 with 18 percent responding that they did not know if their enterprise was a victim of a crime.

The ability of enterprises to detect criminal activity on their network seems to have dramatically decreased. Respondents reveal that 40 percent of their organizations' cybercrimes were identified by an internal source as opposed to 82 percent of those responding to the same question in 2014. This result is alarming as it is imperative that enterprises have the ability to detect and subsequently contain and mitigate malicious or criminal cyber activity.

Figure 16—Incidents of Cybercrime

Was any part of your organization a victim of a cybercrime-related incident during 2015?



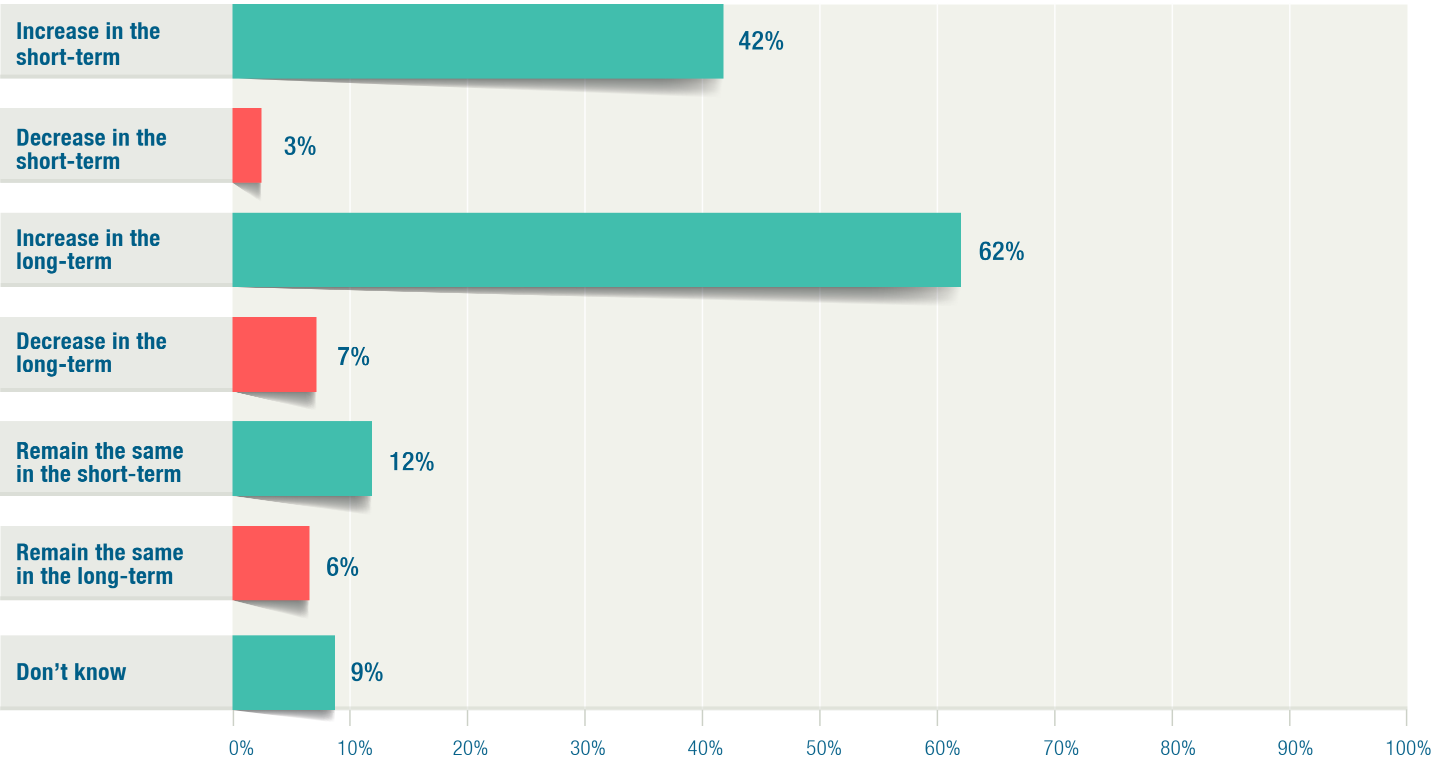
Emerging Industry Trends

In addition to examining the current state of cybersecurity, the project teams at ISACA and RSA Conference asked survey respondents about new and emerging areas of cybersecurity and evolving concerns facing organizations. These questions focused on key issues: the emergence of artificial intelligence (AI) and the expansion of the Internet of Things (IoT).

The survey questioned respondents' perceptions of the risk arising from AI's increasing presence in software and systems providing support to business operations. The results were contradictory to expectations. On the surface, most would think smarter technology would have a positive impact on cybersecurity risk; however, the results indicate the contrary—significant increases in both short-term and long-term risk **(figure 17).**

Figure 17—Artificial Intelligence and Cybersecurity Risk

As artificial intelligence (AI) becomes more prevalent, do you think that cybersecurity/information security risk will increase, decrease or remain the same in the short or long-term?

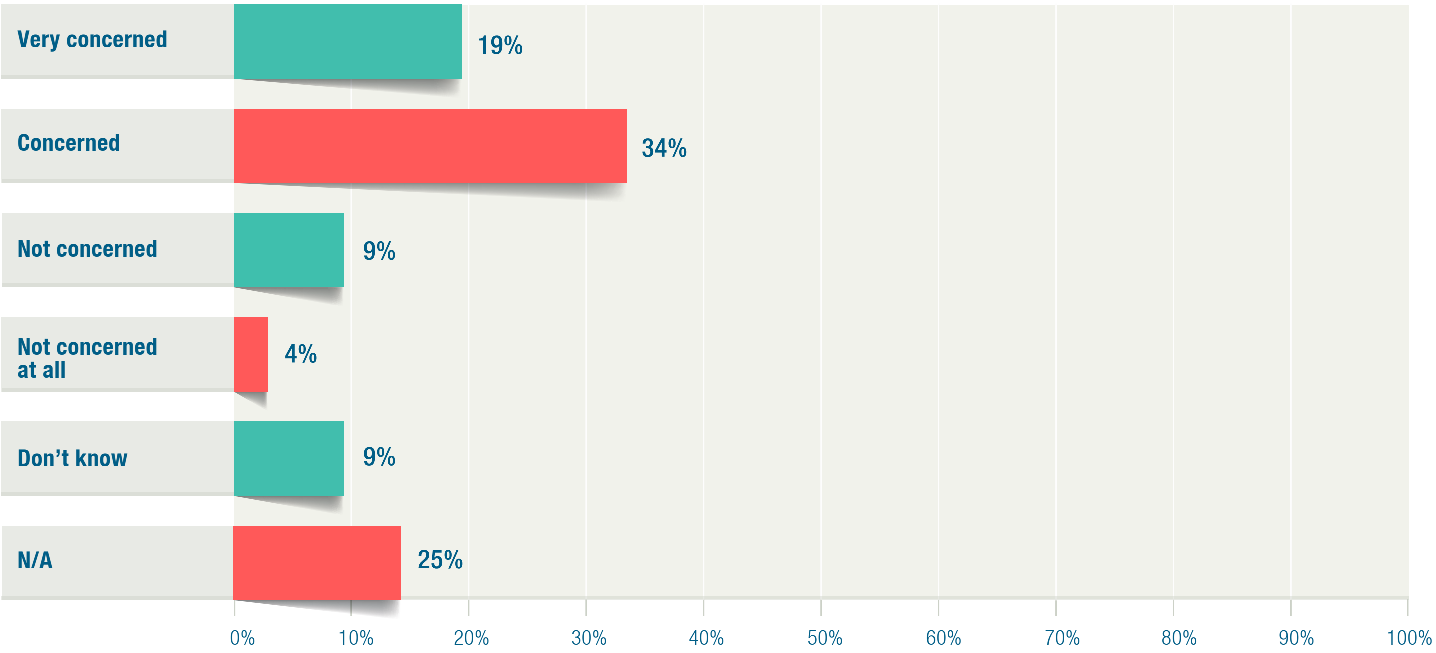


Another emerging organizational concern points to the exponential growth in the IoT—Internet protocol (IP)-enabled devices. The IoT is the network of physical objects or "things" embedded with electronics, software, sensors and network connectivity, enabling objects to collect and exchange data. The IoT provides objects remote access and control across existing network infrastructures, creating opportunities for integration between the physical world and computer-based systems that improve efficiency and accuracy and aid economic benefit.

As expected, more than half of the ISACA/RSA Conference survey respondents (53 percent) are "concerned" or "very concerned" that the IoT will expand attack surfaces further and exacerbate cyber risk **(figure 18).**

Figure 18—Concern About IoT

Are devices considered in the category of Internet of Things (IoT) attached to your organization's network? If so, how concerned is your organization regarding expansion of your attack surface?



Conclusions

Cybersecurity threats continue to plague enterprises. In fact, 74 percent of respondents expect to fall prey to a cyberattack in 2016. The report data reveal that almost 60 percent of respondents experienced a phishing attack in 2015 and in 30 percent of these organizations, it is occurring on a daily basis. In addition, 20 percent are dealing with insider damage and theft of intellectual property at least quarterly. This is especially problematic for many organizations that are simultaneously unable to hire or retain technical talent.

Results indicate that cybercrime is a credible threat to enterprise resiliency as are advanced persistent threat (APT) and traditional attack vectors. Traditional attack vectors appear to be as useful to adversaries as ever, with phishing, social engineering and hacking attempts being the top three attack types to successfully exploit enterprise networks in 2015. This indicates a clear need to increase awareness training for employees as phishing and social engineering attack success is dependent on humans. As emerging trends continue to evolve, security professionals will need to be able to protect against threats that might exploit enterprises; however, people are not going away and so it is important to continue to develop programs to help inspire a culture of security.

Some unsettling information can be drawn from the amount of respondents who report not knowing whether they have been breached. As all respondents were primarily responsible for security in their organizations, it is troubling that 20 to 25 percent did not know whether they had corporate assets hijacked for botnet use, became affected by an APT, had any cyber credentials stolen, and even which threat actors had exploited their organization. This fact could indicate a few issues such as a need for better monitoring, the ability to better interpret logs and other data, or potentially a need for skills enhancement. Identifying and understanding the attacks on the enterprise is a very important area and one that could use significant improvement.

However, it seems that among respondents there is a clear understanding that cybersecurity incidents can lead to significant impact to the business. These enterprises are becoming better prepared organizations and are beginning to look at cybersecurity as a business issue. Respondents indicate that board members and executives are concerned with the ability of the enterprise to withstand cyber incidents and as a result, budgets are expected to increase, sharing of threat indicator information effort continues to expand, controls are being tested, and executives are demonstrating support for security programs.

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/state-of-cybersecurity-2016

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

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

Join ISACA on LinkedIn:
ISACA (Official),
http://linkd.in/ISACAOfficial

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

ISACA®

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer

This is an educational resource and is not inclusive of all information that may be needed to assure a successful outcome. Riders should apply their own professional judgement to their specific circumstances.

ACKNOWLEDGMENTS

ISACA Board of Directors

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

Rosemary M. Amato
CISA, CMA, CPA,
Deloitte Touche Tohmatsu Ltd.,
The Netherlands, Vice President

Garry J. Barnes
CISA, CISM, CGEIT, CRISC, MAICD,
Vital Interacts, Australia, Vice President

Robert A. Clyde
CISM,
Clyde Consulting LLC, USA, Vice President

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

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

Andre Pitkowski
CGEIT, CRISC, OCTAVE, CRMA, ISO27kLA,
ISO31KLA, APIT Consultoria de Informatica Ltd.,
Brazil, Vice President

Eddie Schwartz
CISA, CISM, CISSP-ISSEP, PMP,
WhiteOps, USA, Vice President

Gregory T. Grocholski
CISA,
SABIC, Saudi Arabia,
Past International President

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

Robert E. Stroud
CGEIT, CRISC,
USA, Past International President

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

Matt Loeb
CGEIT, CAE,
ISACA, USA, Director

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

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