

State of Cybersecurity: **Implications for 2015**

An ISACA and RSA Conference Survey

Introduction to the Report

In 2014, RSA Conference and ISACA agreed to collaborate to examine variables contributing to the current state of cybersecurity. The result of the collaboration is this study, which offers a view into global activity and perceptions pertaining to cybersecurity-related issues.

In January and February 2015, 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®) designation, RSA Conference's Loyalty Plus customers and individuals registered for the 2015 RSA Conference. The data were collected anonymously through Survey Monkey.

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 seven major sections:

- Demographics
- Budgets, hiring and skills
- Hacks, attacks and flaws
- Threats
- Internet crime and fraud
- Social media
- Organizational security and governance

Perspectives on Cybersecurity

2014 was a newsworthy year in terms of cybercrime. Major enterprises like Target, Home Depot and Sony Entertainment experienced breaches that required the companies to pay hundreds of millions of US dollars to cover costs of the attacks. JP Morgan Chase and other financial institutions were affected even more severely.

While these enterprises shared the similar misfortune of experiencing incidents, the incidents themselves were not all the same. In the cases of Home Depot and Target, intrusion initially occurred via hacked third-party vendors and financial gain was the motivation. Sony was the victim of extremely sophisticated malware that was used to steal confidential information.

As breaches become more significant, they cause increased financial impact. A recent survey by the Ponemon Institute showed the average cost of cybercrime for US retail stores more than doubled from 2013 to an annual average of

US \$8.6 million per company in 2014.¹ Not only are the attacks more damaging, there also are more of them. PricewaterhouseCoopers (PwC) reported in its "Global State of Information Security Survey® 2015"² that the number of detected information security incidents has risen 66 percent year over year since 2009.

The 2014 survey further reported that the total number of security incidents detected by respondents grew to 42.8 million around the world, up 48 percent from 2013.

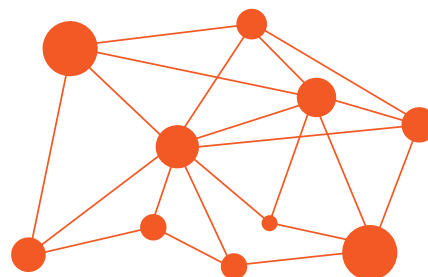
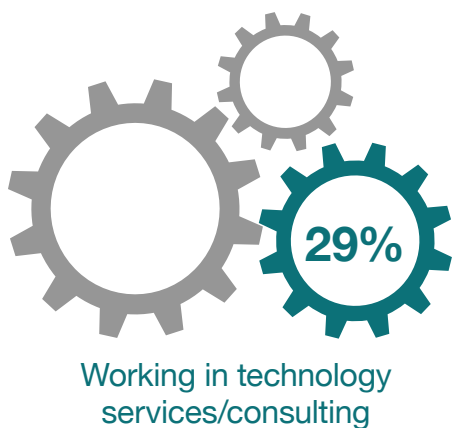
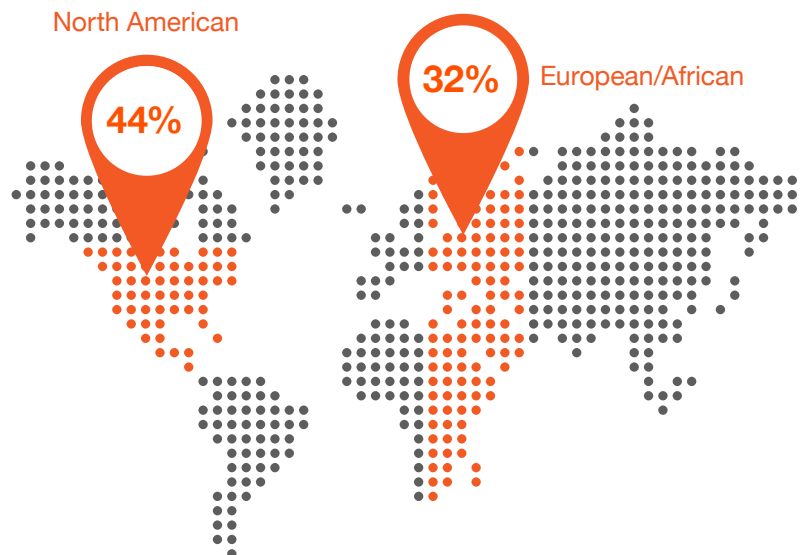
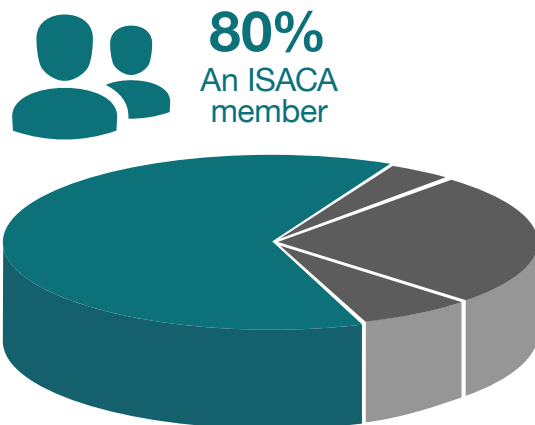
As cybersecurity incidents increase it is important to examine the issues surrounding them, hence this collaboration between ISACA and RSA Conference to explore 2014's cybersecurity issues and look at the variables contributing to the impact that cyberattacks are having on enterprises. The study examined issues such as current hacks, attacks and flaws, and delved into organizational security structures, budgets and policies.

¹Ponemon Institute, "2014 Cost of Cyber Crime Study: United States," 30 October 2014, www.ponemon.org/library/2014-global-report-on-the-cost-of-cyber-crime

²PwC, "The Global State of Information Security® Survey 2015," www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml#

Description of the Population

The survey was sent to 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 1,500 individuals participated and 649 completed the entire survey. A typical respondent can be described as:



66%
Someone whose main function is in cybersecurity or information security



66%
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 of the characteristics of respondents that are not in the majority. Among those surveyed, respondents hailed from more than 20 industries (**figure 1**) and five major global regions, including, in addition to the majority areas, Latin America, Asia and Oceania (**figure 2**).

Figure 1—Industry Representation

In which of the following industries are you employed?

	FREQUENCY	PERCENT	VALID PERCENT	CUMULATIVE PERCENT
Advertising/marketing/media	7	0.6	0.6	0.6
Aerospace	12	1.0	1.0	1.6
Education/student	46	3.8	4.0	5.6
Financial/banking	260	21.3	22.4	28.0
Government/military—National/ state/local	162	13.3	14.0	41.9
Health care/medical	30	2.5	2.6	44.5
Insurance	42	3.4	3.6	48.1
Legal/law/real estate	5	0.4	0.4	48.6
Manufacturing/engineering	68	5.6	5.9	54.4
Mining/construction/ petroleum/agriculture	22	1.8	1.9	56.3
Pharmaceutical	9	0.7	0.8	57.1
Public accounting	17	1.4	1.5	58.6
Retail/wholesale/distribution	26	2.1	2.2	60.8
Technology services/consulting	357	29.3	30.7	91.6
Telecommunications/ communications	57	4.7	4.9	96.5
Transportation	18	1.5	1.6	98.0
Utilities	23	1.9	2.0	100.0
Total	1161	95.2	100.0	
Missing	59	4.8		
Total	1220	100.0		

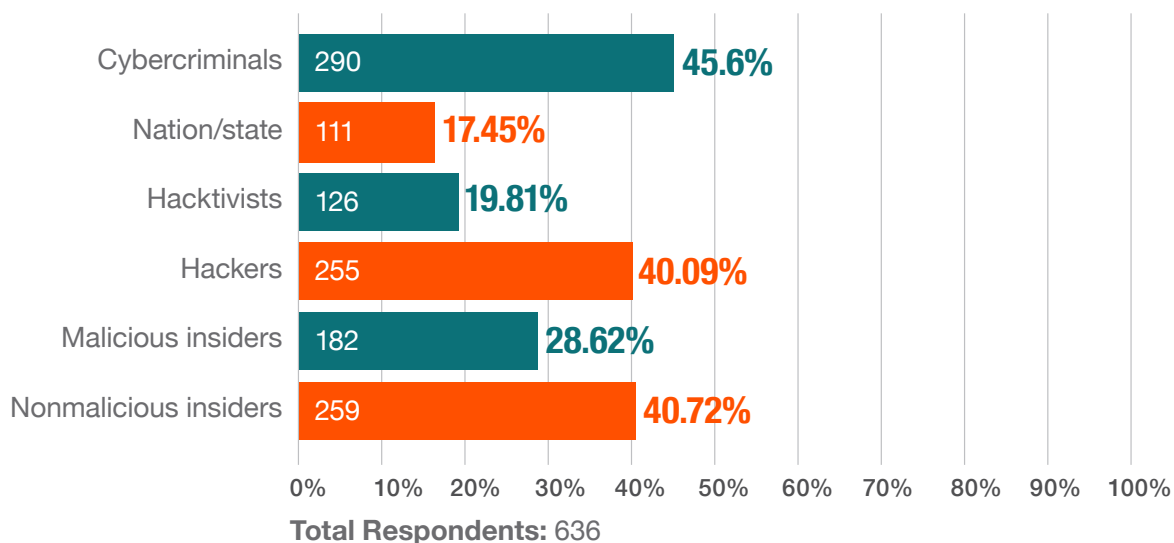
Figure 2—Geographic Representation
In which region do you reside?

	FREQUENCY	PERCENT	VALID PERCENT	CUMULATIVE PERCENT
Area 1 (Asia)	244	20.0	20.1	20.1
Area 2 (Latin America)	87	7.1	7.2	27.3
Area 3 (Europe/Africa)	441	36.1	36.4	63.7
Area 4 (North America)	390	32.0	32.2	95.9
Area 5 (Oceania)	50	4.1	4.1	100.0
Total	1212	99.3	100.0	
Missing	8	0.7		
Total	1220	100.0		

Hacks, Attacks and Flaws

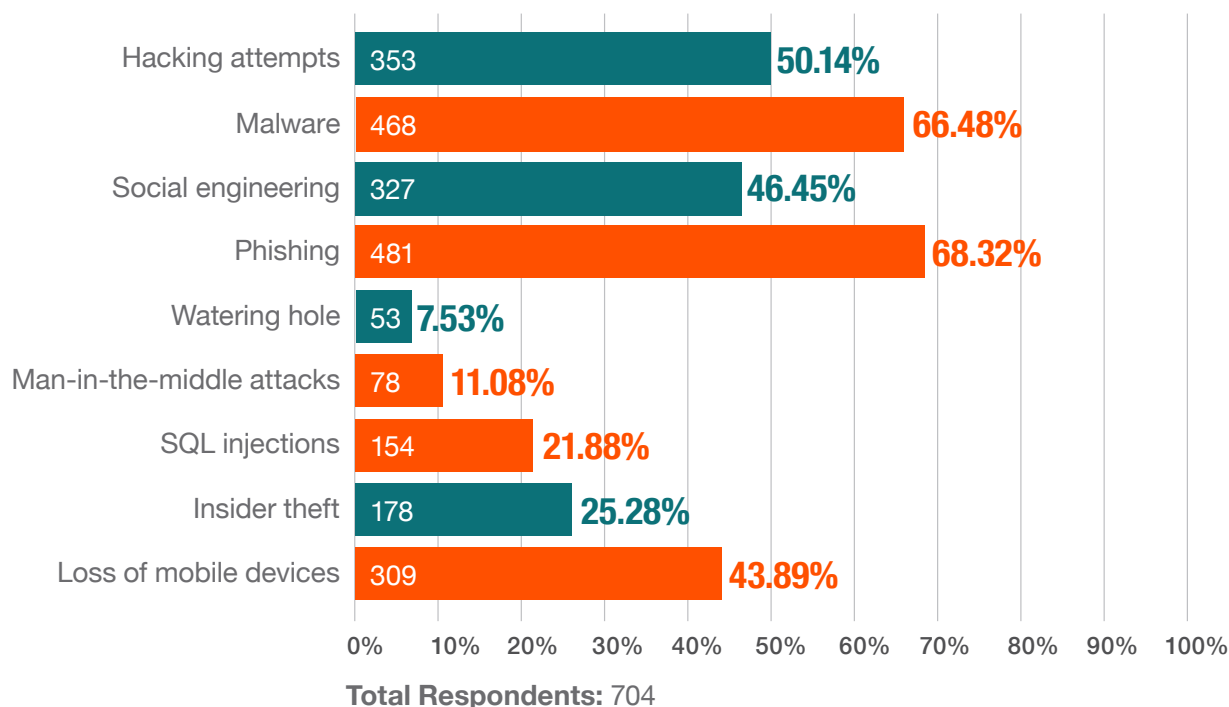
While attacks are becoming more sophisticated and the motivations behind them seem to evolve on a daily basis, the perpetrators can be fairly clearly categorized. The data demonstrate that the threat actors that are most frequently penetrating enterprise security include cybercriminals, hackers and nonmalicious insiders (**figure 3**).

Figure 3—Threat Actors
Which of the following threat actors exploited your enterprise in 2014?



Survey questions also asked respondents to indicate which attack types most commonly penetrated enterprise networks. The data collected show that many of the most prevalent successful attack types hinge on the human factor. As shown in **figure 4**, the attack types that most frequently successfully exploited respondents' enterprises in 2014 are (in order) phishing, malware, hacking attempts and social engineering.

Figure 4—Successful Attack Types
Which of the following attack types have exploited your enterprise in 2014?



While technical and administrative controls can aid in preventing or at least delaying many of these attack types, often the human 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, 72 percent believed it to be effective.

However, the data tell a different story. The survey results indicate that the enterprises that are not leveraging awareness training are actually faring better than the ones that are. **Figure 5** shows that the enterprises that have an awareness program in place actually have a higher rate of human-dependent incidents such as social engineering, phishing and

loss of mobile devices. Additionally, threat actors are more frequently penetrating enterprise security among enterprises that have an awareness program in effect (**figure 6**). Especially troublesome is the percentage of nonmalicious insiders that are impacting enterprise security: It is 12 percent higher in enterprises that have an awareness program in place than in those that do not.

Figure 5—Successful Attack Types in Enterprises With Awareness Programs
Does your company have a security awareness program?

	Hacking Attempts	Malware	Social Engineering	Phishing	Watering Hole	Man-in-the middle Attacks	SQL Injections	Insider Theft	Loss of Mobile Devices	Total
Q27: Yes	51.82% 313	66.89% 404	49.34% 313	69.21% 418	7.95% 48	11.26% 68	23.01% 139	26.66% 161	45.53% 275	2,124
Q27: No	39.18% 38	64.95% 63	28.87% 28	61.86% 60	5.15% 5	10.31% 10	15.46% 15	16.49% 16	34.02% 33	268
Total Respondents	351	467	326	478	53	78	154	177	308	701
	Other (please specify)						Total			
Q27: Yes	40						40			
Q27: No	4						4			

Figure 6—Successful Threat Actors in Enterprises With Awareness Programs
Does your company have a security awareness program?

	Cybercriminals	Nation/State	Hacktivist	Hackers	Malicious Insiders	Nonmalicious Insiders	Total
Q27: Yes	46.36% 255	18.55% 102	21.09% 116	41.27% 227	28.73% 158	42.18% 232	1,090
Q27: No	41.67% 35	10.71% 9	11.90% 10	30.95% 26	28.57% 24	30.95% 26	130
Total Respondents	290	111	126	253	182	258	634
	Other (please specify)				Total		
Q27: Yes	52				52		
Q27: No	11				11		

Curiously, respondents are not positive whether they have been exploited by some large-scale threats. When asked about Shellshock, 20 percent responded that they do not know if they had been made vulnerable; likewise, 30 percent do not know if they had become victimized by an advanced persistent threat (APT). In addition, 23 percent of respondents reported that they do not know whether they had any corporate assets hijacked for botnet use or if they had any user credentials stolen in 2014.

Those results are quite concerning because, if respondents do not know there is a susceptibility, they are unlikely to have created a mitigation strategy for it. This lack of recognition appears to be a common concern among those staffing security organizations. Ernst & Young's (EY) "Global Information Security

Survey 2014" points out that it is "very difficult to hire the specialists necessary to perform the analysis on threat intelligence data, draw relevant and actionable conclusions, and enable decisions and responses to be taken.

Threats

It is no surprise that the cyberthreat is real. Enterprises are finding cyberattacks to have increased in both frequency and impact. More than three-quarters of the survey respondents (77 percent) reported an increase in attacks in 2014 over 2013 (figure 7). Even more—82 percent—predicted that it is "likely" or "very likely" they will be victimized in 2015 (figure 8).

Figure 7—Number of Cyberattacks in Respondents' Enterprises in 2014 vs. 2013

In 2014 has your enterprise experienced an increase or decrease in security attacks as compared to 2013?

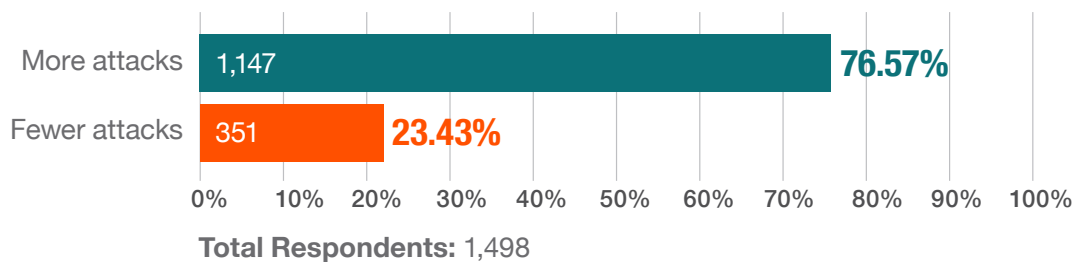
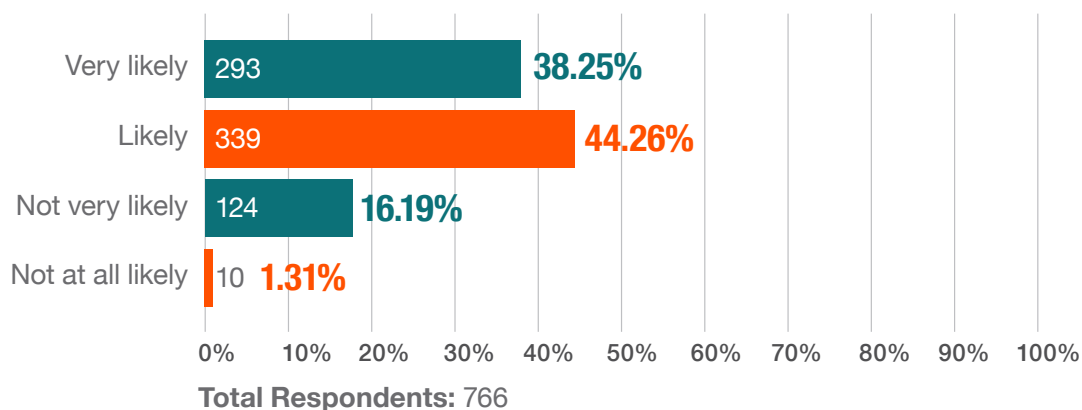


Figure 8—Likelihood of Cyberattacks in Respondents' Enterprises in 2015

How likely do you think it is that your organization will experience a cyberattack in 2015?



Reasons for attacks vary, but respondents voiced their opinion that financial gain is the most prevalent motive for cyberattacks (**figure 9**).

Figure 9—Motivations for Attacks

Do you think the incident motivation is:

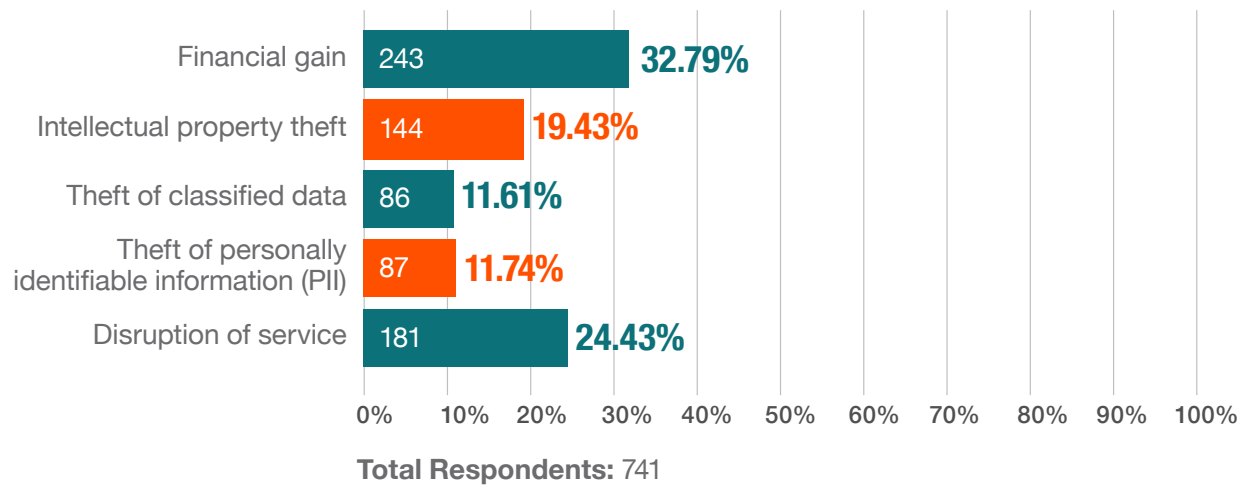


Figure 10 shows, however, that the industry in which the respondents work greatly affects their opinion about the motivation for attacks. Financial gain remains the most frequently cited motivation by respondents in industries such as education, banking/financial services and transportation, while a very different picture is painted by respondents in industries such as government, telecommunications and utilities, who selected disruption in service as the leading motive.

Figure 10—Motivation by Industry

In which of the following industries are you employed?

Industry	Financial Gain	Intellectual Property Theft	Theft of Classified Data	Theft of PII	Disruption of Service	Total
Q3 Aerospace	33.33% 3	22.22% 2	22.22% 2	22.22% 2	0.00% 0	9
Q3 Education/student	34.78% 8	26.09% 6	4.35% 1	17.39% 4	17.39% 4	23
Q3 Financial/banking	54.84% 102	8.06% 15	10.75% 20	10.22% 19	16.13% 30	186
Q3 Government/military-National/state/local	12.82% 10	10.26% 8	19.23% 15	15.38% 12	42.31% 33	78
Q3 Health care/medical	22.22% 8	11.11% 4	8.33% 3	36.11% 13	22.22% 8	36
Q3 Insurance	48.00% 12	4.00% 1	4.00% 1	28.00% 7	16.00% 4	25
Q3 Legal/law/real estate	12.50% 1	25.00% 2	12.50% 1	25.00% 2	25.00% 2	8
Q3 Manufacturing/engineering	22.50% 9	47.50% 19	15.00% 6	2.50% 1	12.50% 5	40
Q3 Mining/construction/petroleum/agriculture	60.00% 9	26.67% 4	0.00% 0	0.00% 0	13.33% 2	15
Q3 Pharmaceutical	14.29% 1	42.86% 3	28.57% 2	0.00% 0	14.29% 1	7
Q3 Public accounting	33.33% 1	33.33% 1	0.00% 0	0.00% 0	33.33% 1	3
Q3 Retail/wholesale/distribution	43.75% 7	0.00% 0	0.00% 0	12.50% 2	43.75% 7	16
Q3 Technology services/consulting	26.40% 47	30.34% 54	11.24% 20	9.55% 17	22.47% 40	178
Q3 Telecommunications/communications	26.92% 14	13.46% 7	15.38% 8	7.69% 4	36.54% 19	52
Q3 Transportation	50.00% 6	8.33% 1	8.33% 1	0.00% 0	33.33% 4	12
Q3 Utilities	7.14% 1	28.57% 4	7.14% 1	7.14% 1	50.00% 7	14
Total respondents	239	131	81	84	167	702

Although loss of mobile devices, phishing, social engineering and malware were at the high end of successful attack attempts, 83 percent of respondents reported that their enterprises provide employees with mobile devices (**figure 11**). In a worrisome corollary, when they were asked about lost physical assets in 2014, more than 90 percent acknowledged that mobile devices were lost during the year (**figure 12**).

Figure 11—Enterprises Providing Employees With Mobile Devices
Do you provide employees with mobile devices?

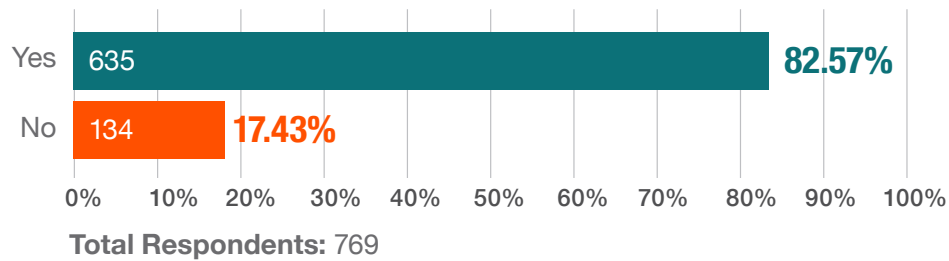
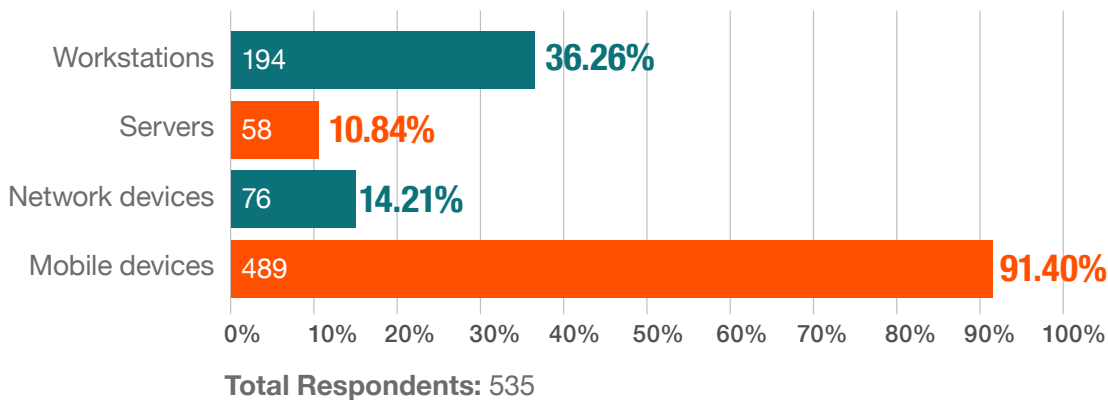
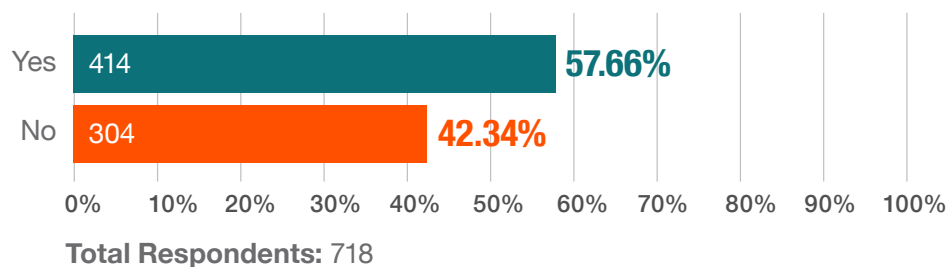


Figure 12—Lost Physical Devices
Has your organization experienced physical loss of assets in 2014?
What type of assets?



With regard to the threats that are exploiting enterprise security, it is interesting to see that only 55 percent of respondents' enterprises restrict USB access and even fewer (42 percent) restrict access to social media (**figure 13**).

Figure 13—Enterprises Restricting Access to Social Media
Do you restrict access to social media in your organization?

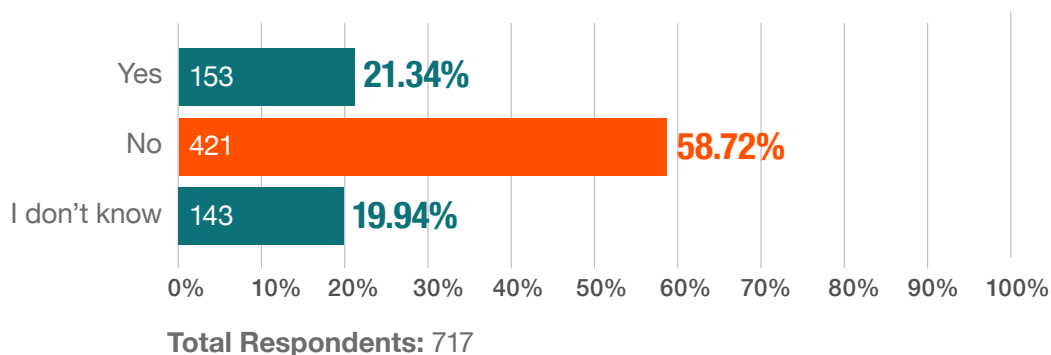


Internet Crime

Crime should not be considered separately from other cybersecurity attacks for the purpose of identifying and prioritizing incidents. However, this survey carved out a specific, focused view of crime to determine how enterprises are handling the issue. More than half (59 percent) of respondents reported that their

enterprise had not been a victim of a cybercrime in the previous year. However, 20 percent responded that they do not know if their enterprise had been a victim of a crime, a figure that is just one percentage point less than the respondents who knew that their enterprise had been (**figure 14**).

Figure 14—Enterprises Victimized by a Cybercrime
Has your organization been part of a cybercrime during 2014?



A deeper dive into the enterprise cybercrimes reported by 21 percent of respondents reveals that 82 percent of the crimes were identified by an internal source. Almost 90 percent of the affected enterprises managed to avoid having corporate assets seized as a result of the crime. While most enterprises have not been part of a crime, all are clearly aware of the risk and are taking steps to avoid it: 60 percent of all enterprises reflected in this survey reported routinely collaborating with law enforcement.

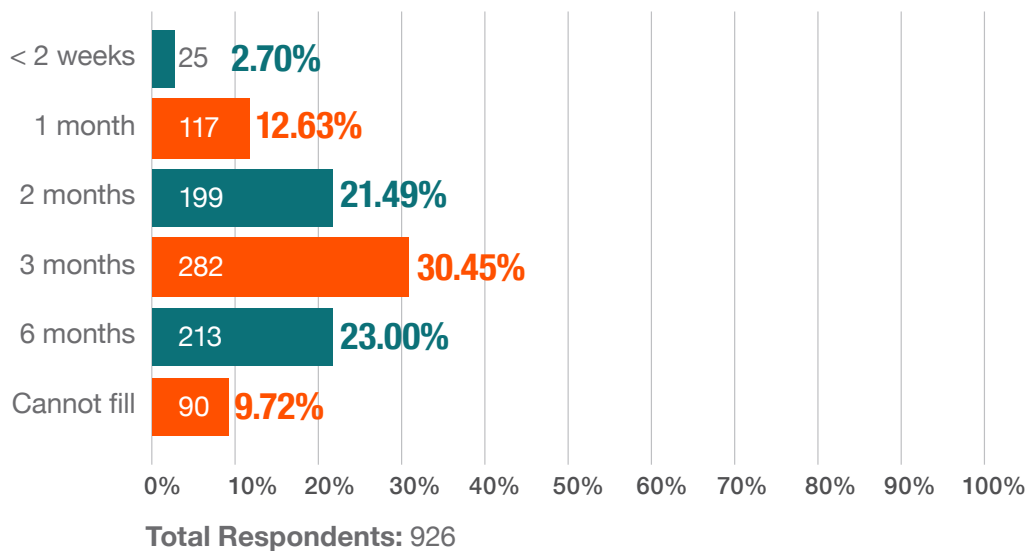
The data support the horror stories that haunt organizations relative to cybersecurity. Enterprises continue to struggle with traditional security threats such as lost devices, insider threats, malware, hacks and social engineering, while simultaneously trying to keep sophisticated attacks by nontraditional threat actors at bay. In such an environment, it is important to understand how enterprises are staffing and managing security. What challenges are security professionals having hiring and retaining strong candidates? How are organizations supporting their security professionals?

Organizational Security, Budgets, Hiring and Skills

In order to understand how computer network defense is adapting to the increased persistence and frequency of attacks, it is important to understand how enterprises are leveraging resources. Global reports indicate that cybersecurity is faced with a skills crisis. 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 2013 (ISC)² Global Information

Security Workforce Study,” sponsored by Frost & Sullivan and (ISC)², concludes that there is a dangerous shortage of skilled professionals in the cybersecurity profession and this shortage is negatively impacting organizations and their customers, leading to more frequent and costly data breaches.³ The survey data in this ISACA/ RSA Conference study seem to confirm that enterprises are having a difficult time hiring skilled people as it takes 53% of organizations between 3 and 6 months to fill a position and 10% cannot fill them at all (**figure 15**).

Figure 15—Time to Fill Security Positions
On average, how long does it take you to fill a security position?

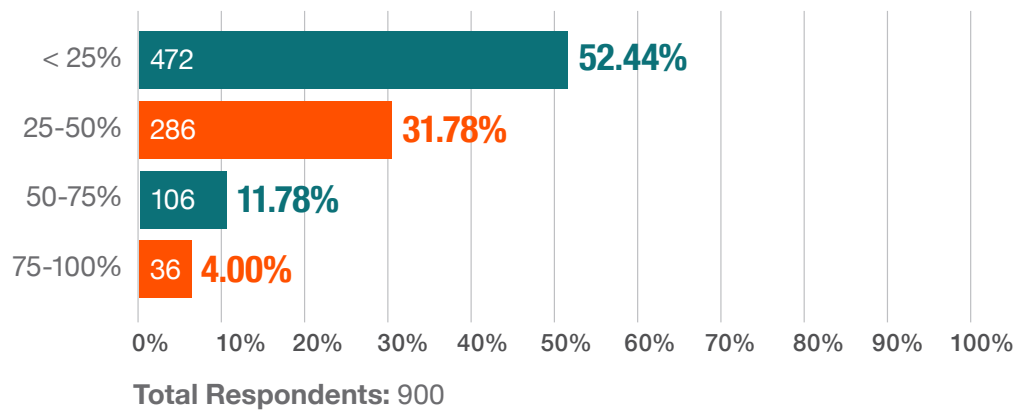


While enterprises eventually are able to hire professionals, most applicants submitting resumes do not have adequate skills to meet the needs of the business. In fact, more than 50 percent of the survey respondents reported that less than one-quarter of applicants are truly qualified for the open positions (**figure 16**).

³ (ISC)², Frost & Sullivan, “The 2013 (ISC)² Global Information Security Workforce Study,” www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf

Figure 16—Qualified Applicants

On average, how many applicants are qualified?



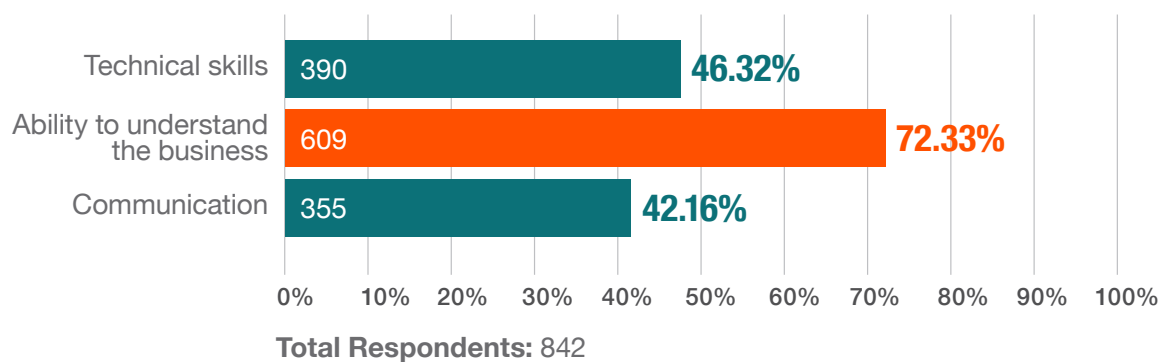
Respondents reported that, among the factors that support a candidate's qualification for a position, hands-on experience is the most important. Working against the candidate is lack of a certification—the second most frequently reason for considering a candidate not qualified. Of course, even candidates who are considered qualified are not always hired. When asked why qualified candidates may not be hired, respondents

reported that the flexibility of the job requirements and starting salaries are the two biggest roadblocks to obtaining skilled new employees.

Among hired individuals, security professionals continue to see a skills gap. Survey participants overwhelmingly reported that the largest gap exists in security practitioners' ability to understand the business; this is followed by technical skills and communication (figure 17).

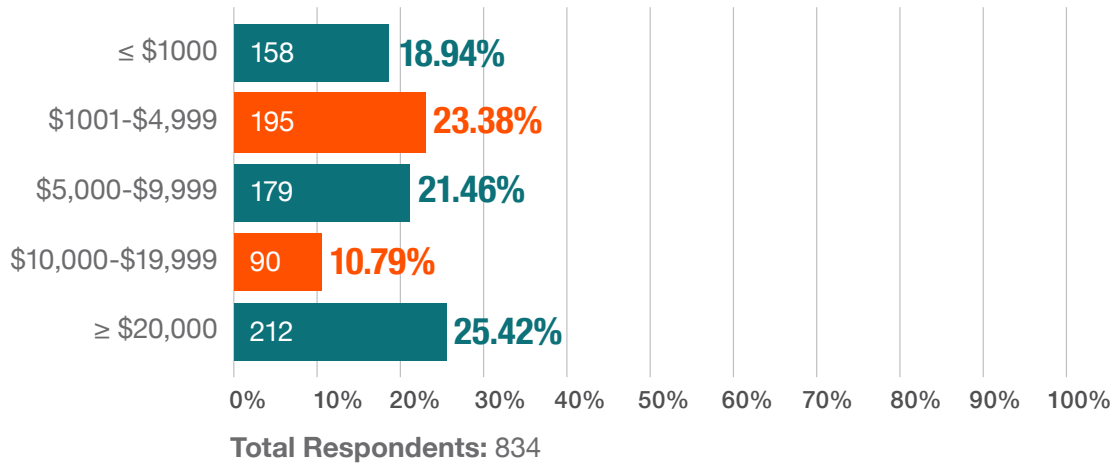
Figure 17—Gaps in Security Skills

What is the biggest skill gap you see in today's security professionals?



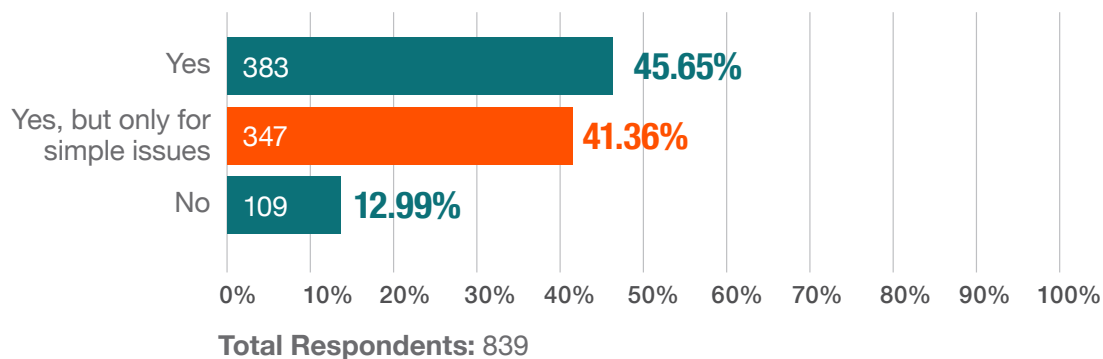
Enterprises seem to recognize the gaps in skills and knowledge among their security staff and they demonstrate willingness to help bridge those gaps by investing in continuing professional development for security personnel (figure 18).

Figure 18—US Dollars Spent on Continuing Education for Security Staff in 2014
How much did your organization spend on continuing education opportunities for security professionals (e.g., training, conferences, etc.)?



Despite the perceived skills gap, survey data also demonstrate that 95 percent of respondents' enterprises have staffs that average at least three years' experience, and 70 percent average more than five years of experience. Additionally, 87 percent of respondents reported that they are confident in their security teams' ability to detect and respond to incidents. However, that confidence comes with conditions. Of the 87 percent, 41 percent are confident only if the incident is simple (figure 19).

Figure 19—Confidence in Security Teams' Ability to Identify and Respond to Incidents
Are you comfortable with your security team's ability to detect and respond to incidents?



Security staffing size varies according to the size of the organization. However, it is interesting to note that organizational size does not significantly affect the number of staff dedicated to security until the organization becomes fairly large: The number of security staff hovers in the range of one to five employees until the enterprise head count exceeds 5,000 employees, when it jumps significantly to 20-plus staff members **(figure 20)**.

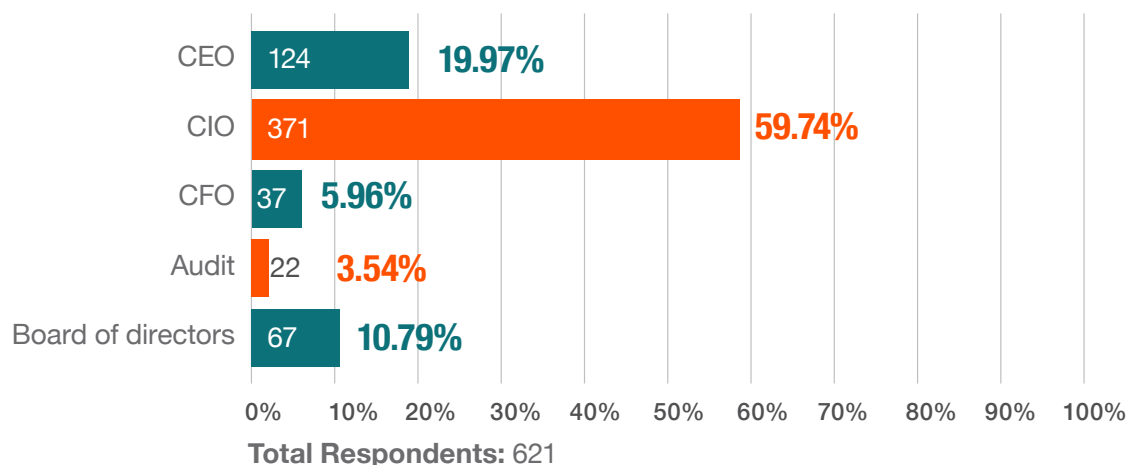
Figure 20—Security Staff Size Compared to Organization Size
How many people are employed within your enterprise?

		Security Staff					
Number of Employees		0	1 - 5	6 - 10	11 - 20	20+	Total
	Q5: 1 - 99	4.35% 4	70.65% 65	16.30% 15	4.35% 4	4.35% 4	92
	Q5: 100 - 249	2.17% 1	80.43% 37	8.70% 4	0.00% 0	8.70% 4	46
	Q5: 250 - 499	4.26% 2	70.21% 33	8.51% 4	8.51% 4	8.51% 4	47
	Q5: 500 - 999	4.48% 3	70.15% 47	11.94% 8	10.45% 7	2.99% 2	67
	Q5: 1,000 - 4,999	0.62% 1	59.63% 96	21.74% 35	9.32% 15	8.70% 14	161
	Q5: 5,000 +	0.33% 1	24.33% 73	16.33% 49	12.67% 38	46.33% 139	300
	Total Respondents	12	351	115	68	167	713

Respondents reported that the most prevalent (60 percent) reporting structure for security is through the chief information officer (CIO) **(figure 21)**. This is unfortunate, as some chief information security officers (CISOs) continue to report through the IT business line and do not have a seat at the executive table in many enterprises. While roughly 30 percent of CISOs report to the board or CEO, 70 percent do not **(figure 21)**.

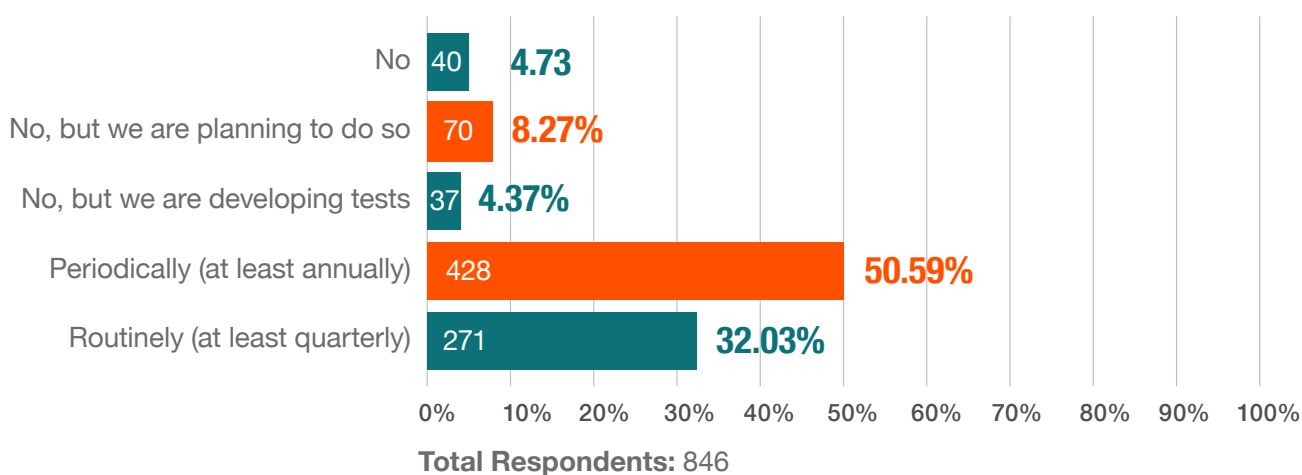


Figure 21—Reporting Structure for Cybersecurity
Where does security report to in your organization?



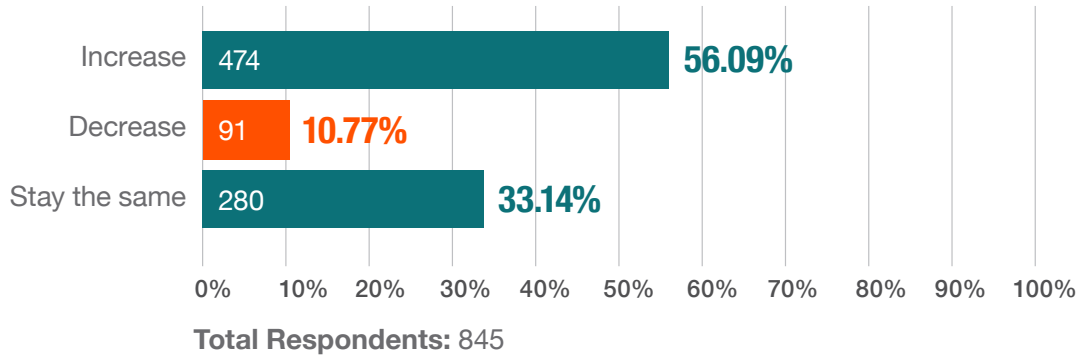
The good news is that it appears that enterprises are taking security more seriously. More than three-quarters of respondents reported having an incident response plan and roughly 80 percent test security controls at least annually (**figure 22**). Additionally, 84 percent reported having a mobile device policy and 59 percent have a policy for bring your own device (BYOD).

Figure 22—Enterprise Frequency of Security Controls Testing
Do you test security controls?



Financially, cybersecurity budgets seem to be on the upswing. While existing security budgets vary greatly based on enterprise size, respondents reported expected increases in security budgets regardless of enterprise size (**figure 23**).

Figure 23—Change to Security Budget in 2015
How will the security budget change in 2015?



It appears as though funding is not the only positive indicator that enterprises are recognizing cybersecurity as a business issue. Respondents are experiencing a better organizational approach to security, as evidenced by 79 percent reporting that the board of directors is concerned with cybersecurity (**figure 24**) and 87 percent noting that executive teams are demonstrating support for

cybersecurity through actions such as enforcing security policies (71 percent) and managing cybersecurity awareness programs (56 percent). Unfortunately, there is still room for improvement in the security behaviors of executives: Only 41 percent reported that their enterprise's executives follow good security practices themselves (**figure 25**).

Figure 24—Boards of Directors Concerned With Cybersecurity
Is your board of directors concerned with security?

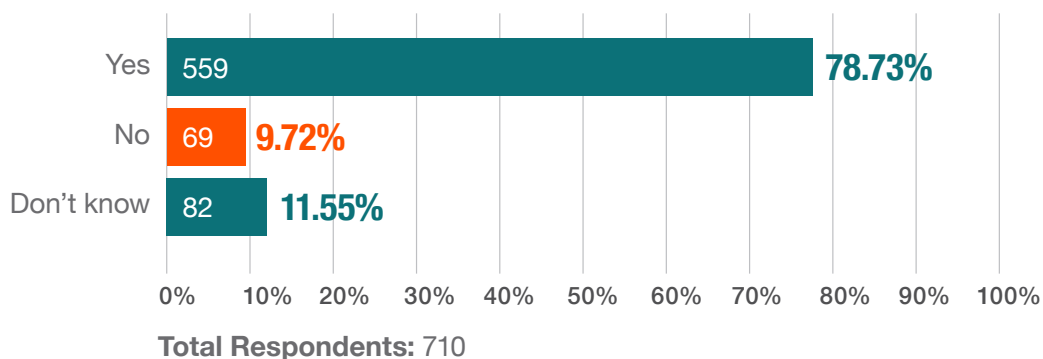
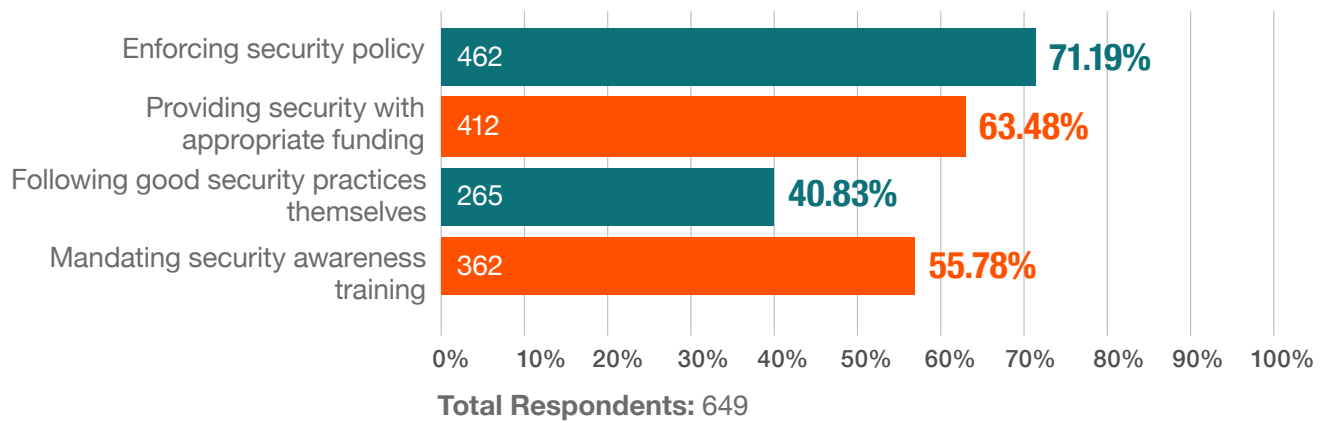


Figure 25—Actions Executives Take to Support Security
How is the support demonstrated?



Conclusions

Cybersecurity threats are not slowing down. More than three-quarters of respondents reported an increase in attacks in 2014 over 2013 and they expect the number to rise again in 2015. The report data reveal that almost 25 percent of respondents are experiencing phishing attacks daily and 30 percent are dealing with insider damage and theft of IP at least quarterly. Additionally, the majority (over 82%) of respondents expect to experience a cyberattack in 2015. Enterprises need to address the fact that cybersecurity issues can lead to risk for the business, which could have a very negative effect both financially and reputationally.

The report relates some positive trends as well. Enterprises are beginning to look at cybersecurity as an issue for the business and not just for the security manager. Budgets are increasing, security operations centers (SOCs) are being implemented, controls are being tested and executives are demonstrating their support for the security program; all these actions help in elevating the cybersecurity program.

However, it is important to note a few issues that merit further consideration. The survey indicates that enterprises that offer awareness training do not seem to be benefitting from a corresponding decrease in successful attack types; the nature of their attacks remains human-dependent, similar to those of enterprises without a program. This could lead to areas for future studies. Also, a skills gap is being

perceived internally by security managers who believe that the ability to understand the business continues to be a problem for many security professionals. Finally, there were more than a few key survey questions that received a response of “I don’t know.” Cybersecurity cannot tolerate an inability to recognize when enterprise information assets have potentially been compromised. Less than half of the respondents indicated that their enterprise had established a SOC. A SOC can swiftly identify incidents that will impact the enterprise and respond promptly, so perhaps this offers a logical quick-win activity for enterprises wishing to enhance their security readiness. Enterprises are offering professional development to security staff, so that is a step in the right direction.

The increase in attacks has seemed to provide security governance with the push it needs to be looked at as an issue for the business. More than half of those surveyed reported that they employ a CISO. In addition, cybersecurity has gained the attention of the executives and the board of directors, which has helped those responsible for security get the increased resources they need to operate effectively.

While it is not good news to see increases in both frequency and success of attacks, the positive indication of increased resources and support should give some credibility to the notion that the security manager is not in this alone. Securing cyber resources is a business issue and is beginning to be recognized as such.





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-2015

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/ISACAOOfficial>

Like ISACA on Facebook:

www.facebook.com/ISACAHQ

ISACA®

With more than 140,000 professionals in 180 countries, ISACA (www.isaca.org) helps business and IT leaders build trust in, and value from, information and information systems. Established in 1969, ISACA is the trusted source of knowledge, standards, networking, and career development for information systems audit, assurance, security, risk, privacy and governance professionals. ISACA offers the Cybersecurity Nexus™, a comprehensive set of resources for cybersecurity professionals, and COBIT®, a business framework that helps enterprises govern and manage their information and technology. ISACA also advances and validates business-critical skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) credentials. The association has more than 200 chapters worldwide.

Disclaimer

ISACA has designed and created *State of Cybersecurity: Implications for 2015* (the "Work") primarily as an educational resource for security 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, security professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

ACKNOWLEDGMENTS

Expert Reviewers

Eddie Schwartz

CISA, CISM, CISSP, MCSE, PMP,
USA

Neil Patrick Barlow

CISA, CISM, CRISC, CISSP,
Capital One, UK

Jared Carstensen

C|CISO, Ireland

Christos K. Dimitriadis

CISA, CISM, CRISC,
INTRALOT S.A., Greece

Jo Stewart-Rattray

CISA, CISM, CGEIT, CRISC, CSEPS,
BRM Holdich, Australia

Brennan Baybeck

CISA, CISM, CRISC, CISSP,
Oracle Corporation, USA

Marc Sachs

Verizon, USA

Brent Conran

CISA, CISM, CISSP,
Intel, USA

ISACA Board of Directors

Robert E Stroud

CGEIT, CRISC,
CA, USA, International President

Steven A. Babb

CGEIT, CRISC, ITIL,
Vodafone, UK, Vice President

Garry J. Barnes

CISA, CISM, CGEIT, CRISC,
Vital Interacts, Australia, Vice President

Robert A. Clyde

CISM,
Clyde Consulting LLC, USA, Vice President

Ramses Gallego

CISM, CGEIT, CCSK, CISSP, SCPM,
Six Sigma Black Belt,
Dell, Spain, Vice President

Theresa Grafenstine

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

Vittal R. Raj

CISA, CISM, CGEIT, CRISC, CFE, CIA, CISSP, FCA,
Kumar & Raj, India, Vice President

Tony Hayes

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

Gregory T. Grocholski

CISA,
SABIC, Saudi Arabia, Past International President

Debbie A. Lew

CISA, CRISC,
Ernst & Young LLP, USA, Director

Frank K.M. Yam

CISA, CIA, FHKCS, FHKIoD,
Focus Strategic Group Inc., Hong Kong, Director

Alexander Zapata Lenis

CISA, CGEIT, CRISC, ITIL, PMP,
Grupo Cynthus S.A. de C.V., Mexico, Director

Knowledge Board

Steven A. Babb

CGEIT, CRISC, ITIL
Vodafone, UK, Chairman

Rosemary M. Amato

CISA, CMA, CPA,
Deloitte Touche Tohmatsu Ltd., The Netherlands

Neil Patrick Barlow

CISA, CISM, CRISC, CISSP,
Capital One, UK

Charlie Blanchard

CISA, CISM, CRISC, CIPP/US, CIPP/E, CISSP, FBCS,
ACA,
Amgen Inc., USA

Sushil Chatterji

CGEIT,
Edutech Enterprises, Singapore

Phil J. Lageschulte

CGEIT, CPA,
KPMG LLP, USA

Anthony P. Noble

CISA,
Viacom, USA

Jamie Pasfield

CGEIT, ITIL V3, MSP, PRINCE2,
Pfizer, UK

Ivan Sanchez Lopez

CISA, CISM, ISO 27001 LA, CISSP,
DHL Global Forwarding & Freight, Germany