CSX™
CYBERSECURITY NEXUS

Advanced Persistent Threat Awareness

Study Results

Advanced persistent threat (APT) is a term that has been used frequently in the course of security threat discussions; however, confusion exists as to what an APT is and how to manage the risk associated with it. Although the study reveals that a large number of respondents feel that APTs are a significant threat and have the ability to impact national security and economic stability, the study also indicates that the controls being used to defend against APTs might not be sufficient to adequately protect enterprise networks.

ISACA®
Trust in, and value from, information systems
www.isaca.org/cyber

ISACA®

With more than 115,000 constituents 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 *2014 Advanced Persistent Threat Awareness Study Results* (the "Work") primarily as an educational resource for those interested in APTs. ISACA makes no claim that any use 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, governance and assurance professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

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

Phone: +1.847.253.1545

Fax: +1.847.253.1443

Email: info@isaca.org

www.isaca.org

Provide feedback:
www.isaca.org/APT-WP

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

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

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

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

ACKNOWLEDGMENTS

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,
BAE Systems Detica,
Australia, Vice President

Robert A. Clyde
CISM, Adaptive Computing,
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, The Dow Chemical Co.,
USA, 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

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

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

Steven A. Babb
CGEIT, CRISC,
Vodafone, UK

Thomas E. Borton
CISA, CISM, CRISC, CISSP,
Cost Plus, USA

Phil J. Lageschulte
CGEIT, CPA, KPMG LLP,
USA

Anthony P. Noble
CISA, Viacom, USA

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

Guidance and Practices Committee

Phil J. Lageschulte
CGEIT, CPA, KPMG LLP,
USA, Chairman

John Jasinski
CISA, CGEIT, ISO20K, ITIL Exp, SSBB,
ITSMBP, USA

Yves Marcel Le Roux
CISM, CISSP, CA Technologies,
France

Aureo Monteiro Tavares Da Silva
CISM, CGEIT, Brazil

Jotham Nyamari
CISA, CISSP,
Deloitte, USA

James Seaman
CISM, CRISC, A. Inst. IISP, CCP, QSA,
RandomStorm Ltd., UK

Gurvinder Singh
CISA, CISM, CRISC,
Australia

Siang Jun Julia Yeo
CISA, CRISC, CPA (Australia), MasterCard
Asia/Pacific Pte. Ltd., Singapore

Nikolaos Zacharopoulos
CISA, CRISC, CISSP,
DeutschePost–DHL, Germany

Cybersecurity Task Force

Eddie Schwartz
CISA, CISM, CISSP, MCSE, PMP,
Verizon,
USA, Chairman

Manuel Aceves
CISA, CISM, CGEIT, CRISC, CISSP, FCITSM,
Cerberian Consulting,
SA de CV, Mexico

Sanjay Bahl
CISM, CIPP, India

Neil Barlow
CISA, CISM, CRISC, CISSP,
Intercontinental Exchange, Inc. NYSE, UK

Bent Conran
CISA, CISM, CISSP, USA

Derek Grocke
HAMBS, Australia

Samuel Linares
CISA, CISM, CGEIT, CRISC, CISSP, GICSP,
Industrial Cybersecurity Center (CCI), Spain

Marcus Sachs
Verizon, USA

Table of Contents

List of Figures

Introduction to the Report

In 2013, ISACA released its first study on advanced persistent threat (APT) awareness. ISACA's Guidance and Practices Committee launched the APT Awareness Study to comprehend better how well security professionals understand APTs and what is being done to prevent them. The results represented data collected in 2012 and demonstrated that although APTs had received much market attention, there was still a lack of clarity around what actually defined an APT and how to protect and defend against APTs. To determine whether the landscape had changed, ISACA repeated the survey in January of 2014.

The 2014 survey was open to ISACA member and nonmember security professionals. The sample was defined to include information security managers in different industries and organizations throughout the world. The sample population was created by inviting current Certified Information Security Managers (CISMs) and other information security professionals.

The survey, which used multiple-choice and Likert scale formats, was organized in five major sections:

- **Demographics**
- **APT Awareness**
- **Direct APT Experience**
- **Security Controls, Processes and Responses**
- **APT Impact on Policies and Practices**

Defining Advanced Persistent Threats

The year 2013 might be remembered as the year of the breach. Major cyberattacks on organizations resulted in millions of exposed records, billions spent on remediation and significant damage to many brands. While cybercriminals enjoyed a profitable year at the expense of many enterprises, the APT has continued to enjoy success stealing sensitive data in espionage attempts.

Cybersecurity issues are not decreasing. In fact, industry and vendor reports indicate that attacks are on the rise. Cybercrime, hacktivism and advanced attacks all continue to threaten enterprise networks. Some progress in defending against cyberattacks has been made: many preventive controls have emerged that have made it more difficult for those with malicious intent to penetrate networks, and detective controls have helped to identify quickly when a breach does occur. Still, some are very difficult to spot.

APTs continue to make headlines, much to the chagrin of many organizations. In 2012, APTs relied heavily on spear-phishing attempts, which often included an attachment or a link that contained malware or an exploit that would ultimately make an APT possible. However, many APTs now leverage the web as the main attack vector. Watering hole attacks have increased in frequency and often use a browser-based zero-day attack. In fact, a recent report by vendor FireEye™ states that its analysis found that web-based attacks outnumbered email-based attacks nearly three to one.[1]

There are differing opinions on what makes a threat an APT. Some state that APT is just a marketing term, while others say that there is no difference between an APT and a traditional threat, and yet others say that an APT is a nation-state sponsored activity that is geared toward political espionage. So what is true? APTs are often seen in nation-state sponsored attacks (but it is very hard to prove), and they do often use the same attack vectors that traditional threats leverage, but they also leverage different attack methodologies and have different characteristics than traditional threats.

Because so many differing opinions of what constitutes an APT exist in the market, establishing the definition for the initial study was critical. In the follow-up survey, ISACA retained the definition used in the original study. APTs are often aimed at the theft of intellectual property (espionage) as opposed to achieving immediate financial gain and are prolonged, stealthy attacks. This aligns with the definition of the US National Institute of Standards and Technology (NIST), which states that an APT is:

> **An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.[2]**

1 FireEye, *Advanced Threat Report: 2013,* USA, 2014, *www.fireeye.com*

2 National Institute of Standards and Technology (NIST), Special Publication 800-39, *Managing Information Security Risk, Organization, Mission, and Information System View,* USA, 2011

This definition provides a good base from which to understand the differences between traditional threats and APTs. Interaction with a command and control center, repeated pursuit of objectives, adaptation to defenders, and persistence differentiate APTs from a typical attack. There is a "who" behind the APT—it is not just a random spray of malware; someone is specifically targeting the enterprise. Primarily, the purpose of the majority of APTs is to extract information from systems—this could be critical research, enterprise intellectual property or government information, among other things.

APTs are advanced and stealthy, often possessing the ability to conceal themselves within the enterprise network traffic, interacting just enough to get what they need to accomplish their job. This ability to disguise themselves and morph when needed can be crippling to security professionals' attempts to identify or stop APT attacks.

In addition to this stealthiness and adaptability, persistence characterizes this class of threat. For example, traditional cyberthreats often try to exploit a vulnerability but will move right on to something less secure if they cannot penetrate their initial target, whereas APTs do not stop. The single-minded persistence of APTs on pursuing their target and their repeated efforts to complete the job they have been created to do means they will not go away after one failed attempt. They will continually attempt to penetrate the desired targets until they are mitigated and removed or they meet their objectives. This occurs because the people and groups behind APT attacks are determined to achieve success and have the resources to be persistent and to obtain and launch zero-day attacks on enterprises.

APTs are advanced and stealthy, often possessing the ability to conceal themselves within the enterprise network traffic, interacting just enough to get what they need to accomplish their job.

Description of the Population

Because the study's purpose was to measure information security characteristics such as knowledge of APTs, knowledge of internal controls, internal incidents, policy adherence and management support, the study surveyed those who deal with those issues every day: professionals with information security responsibilities. The study's global sample included those who hold ISACA's Certified Information Security Manager (CISM) credential and other information security professionals with whom ISACA interacts.

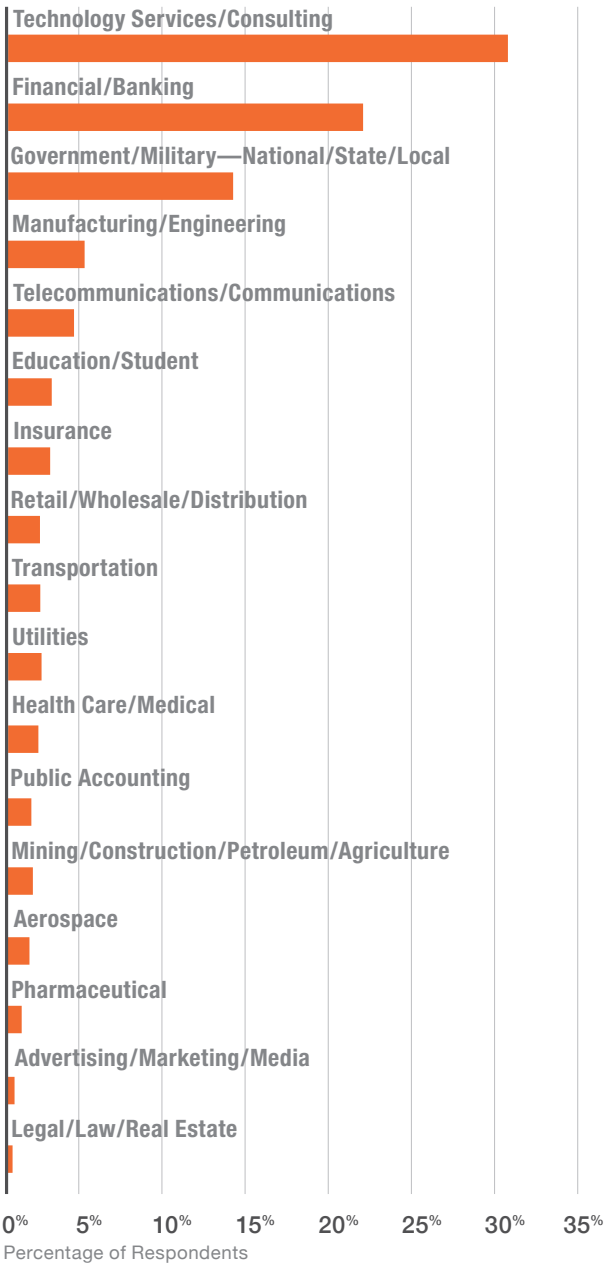
SurveyMonkey (*www.surveymonkey.com*) was used to collect the data from 1,220 individuals globally, 93.0 percent of whom were members of ISACA.

More than 20 industries were represented in the study; the majority of respondents (31.0 percent) were from the technology services and consulting field **(figure 1).**

FIGURE 1

Industry Distribution

WITHIN WHICH OF THE FOLLOWING INDUSTRIES ARE YOU EMPLOYED?



The majority of respondents reside in Europe/Africa (36.0 percent), followed by North America (33.0 percent) **(figure 2).**

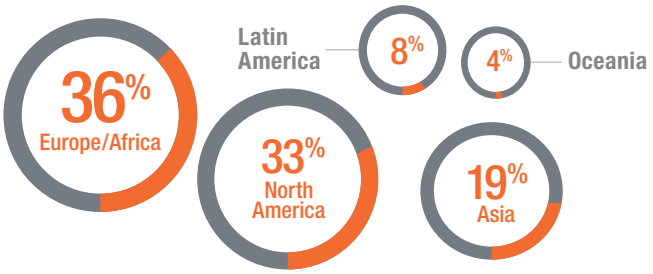
Based on these three demographic factors, a typical participant can be described as:

- An ISACA member
- European/African or North American
- Belonging to the technology services consulting industry or the financial services/banking industry

FIGURE 2

Geographic Distribution

IN WHICH OF THE FOLLOWING AREAS DO YOU RESIDE?



Perspectives on APT

The 2014 analysis reveals that there appears to be more awareness regarding APTs than was reflected in the 2013 study. In the earlier results, the data showed that although 96.0 percent claimed familiarity with APTs, they were not doing much to adapt their security practices. This current study reports a significantly larger percentage of respondents who are adjusting practices in vendor management, security awareness and incident response.

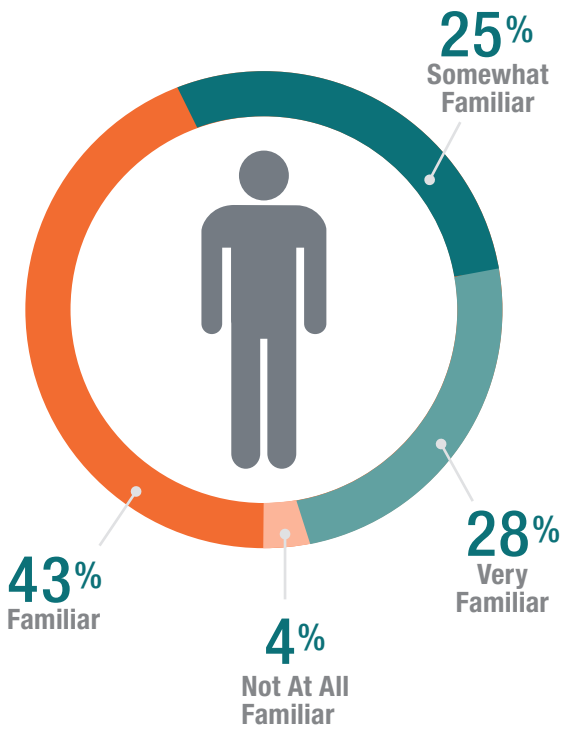
Awareness

The survey results reveal that 28.0 percent of respondents are very familiar with APTs, with a total of 96.0 percent expressing that they are at least somewhat familiar **(figure 3).**

FIGURE 3

Familiarity With APTs

HOW FAMILIAR ARE YOU WITH APTS?



The degree of familiarity appears to be a positive indicator; however, the data still show that only 50.0 percent see APTs as a unique threat type **(figure 4).**

While the percentage has shifted slightly since 2013 to more respondents believing that APTs are unique, the finding is still troubling because it implies that confusion remains regarding the nature of an APT and its difference from a traditional threat. If security professionals do not understand the differences between the threat classes, it is logical that they could find it difficult to properly identify, defend against and respond to APTs. With 92.0 percent of respondents reporting that they believe that APTs represent a credible threat to national security and economic stability, the importance of having a clear understanding of what APTs are is self-evident.

OTHER AWARENESS HIGHLIGHTS INCLUDE:

- 92.0 percent of respondents believe that the use of social networking sites increases the likelihood of a successful APT attack.
- 88.0 percent think that "bring your own device" (BYOD), combined with rooting (Android manipulation by the owner of the device to gain more access to OS and hardware functions) or jailbreaking (iOS manipulation by the owner of the device to evade vendor limitations), makes a successful APT attack more likely.

While there was a high level of agreement among respondents that APTs are cause for concern, there was less agreement on the biggest risk to the enterprise in the event of a successful APT attack. The top two issues switched spots with 2013's results. Loss of personally identifiable information regarding employees or customers (2013's second-rated risk) ranked as the highest risk at 27.0 percent followed by 2013's top risk, enterprise intellectual property, at 24.0 percent **(figure 5).**

FIGURE 4

Comparison of APTs and Traditional Threats

DO YOU BELIEVE THAT APTS ARE SIMILAR OR UNIQUE TO HISTORICAL THREATS?

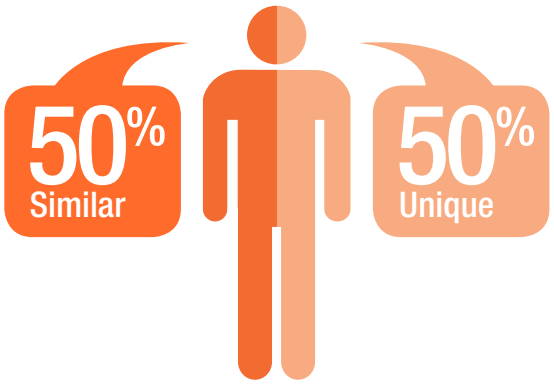
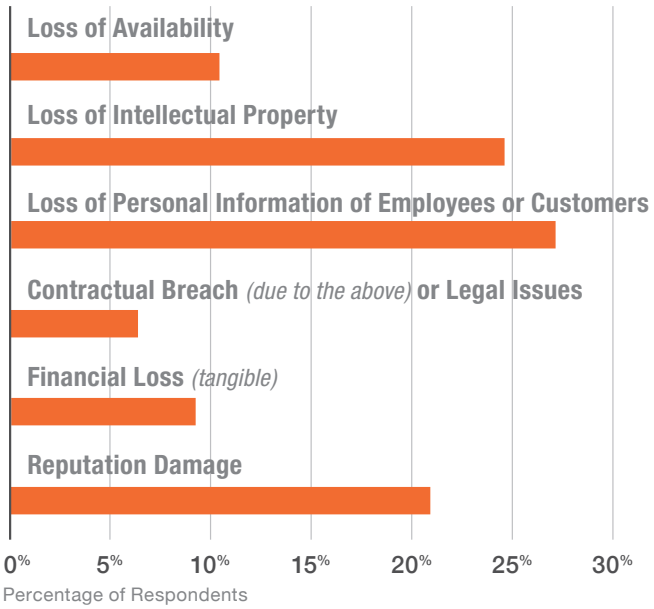


FIGURE 5

Highest Enterprise Risk of Successful APT Attack

WHAT DO YOU BELIEVE TO BE THE HIGHEST RISK TO YOUR ENTERPRISE ASSOCIATED WITH A SUCCESSFUL APT ATTACK?



Direct APT Experience

While respondents have identified the risk scenarios of a successful APT attack, most have not yet had to deal with the actuality of an attack. Only 21.0 percent of respondents reported having been subject to an APT attack. Of those, 25.0 percent were employed in the technology services and consulting field, followed by 19.0 percent working in government or military (national/state/local). Additionally, among those who had been subject to attack, 65.0 percent were able to identify its source.

Although only 21.0 percent of respondents reported that their enterprise has already been victimized by an APT, roughly three times that number—66.0 percent—believe that it is only a matter of time before their enterprise is targeted **(figure 6).**

All respondents were asked whether they considered their enterprise prepared to deal with the threat of an APT. The majority indicated their belief that they do have the ability to detect, respond to and stop an APT attack **(figure 7).**

Overall, nearly 60 percent of respondents believe that they are ready to respond to APT attacks.

FIGURE 6 Enterprise Perceived Likelihood of Becoming an APT Target

HOW LIKELY DO YOU FEEL IT IS THAT YOUR ORGANIZATION WILL BE THE TARGET OF AN APT?

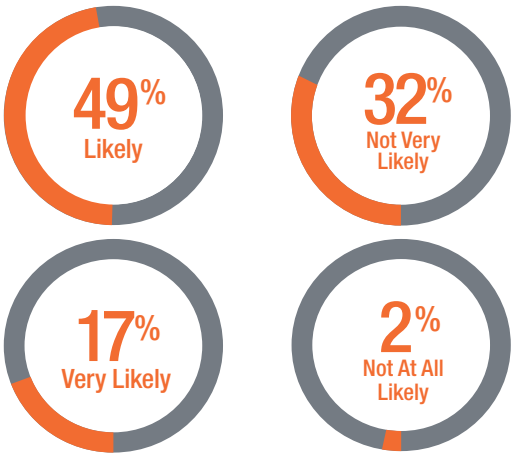
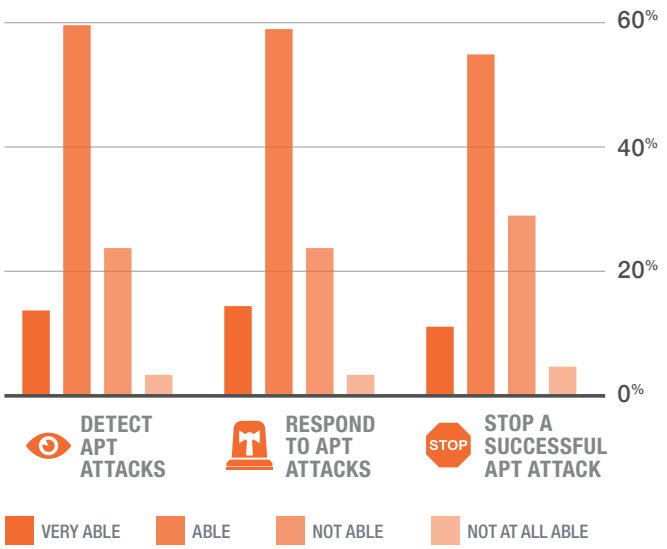


FIGURE 7 Enterprise Ability to Deal With an APT Attack

HOW ABLE IS YOUR ENTERPISE TO DEAL WITH AN APT ATTACK?



Security Controls, Processes and Responses

As noted previously, the majority of respondents believe that they are well positioned to identify, respond to and stop an APT attack. What controls and countermeasures are needed to ensure that this is true?

Throughout the survey, patterns emerge to indicate that although confusion exists on what an APT is and is not, enterprises seem to be taking a risk-based approach to planning for an APT. Controls are more prevalent in enterprises that believe that they could be targeted for an APT attack than in those that do not perceive a high likelihood of becoming an APT target. This is true not only of technical controls; throughout the study, there is a correlation between those respondents who believe that their enterprises will be targeted by an APT and those who have adjusted components in the security program (such as awareness training and incident response plans) to prepare for potential attack from an APT.

Incident Management Plans

Overall, more than 74.0 percent of respondents believe that they are ready to respond to APT attacks; this represents a 9.0 percent increase over last year's statistic of 65.0 percent. When asked the degree to which their enterprise is prepared to deal with an APT attack today, 15.0 percent responded that they are "very prepared," which was defined as having a documented and tested plan in place for APTs. Another 50.0 percent responded that they are "prepared," which signified having an incident management plan, although it does not specifically cover APTs. This leaves 35.0 percent of respondents not confident that they are prepared to deal with an event triggered by this class of threat.

Upon further analysis of the results, a relationship can be seen between the perceived likelihood of the respondent's enterprise being subject to an APT attack and the level of enterprise preparedness to deal with such an incident. Seemingly, a higher perceived likelihood of being targeted corresponds to greater enterprise preparedness.

Among the 17.0 percent of respondents who felt it was "very likely" that their organization would be the target of an APT attack, 34.0 percent identified themselves as being in the "very prepared" category and 41.0 percent placed themselves in the "prepared" category. This demonstrates that 75.0 percent of those who characterize their enterprise as "very likely" to be targeted are ready to deal with APTs. Likewise, those that identified their enterprise as a "likely" target (49.0 percent) stated that they, too, are ready to deal with an attack, with 13.0 percent considering themselves "very prepared" and 58.0 percent claiming that they are "prepared" (total of 71.0 percent). While the total "prepared" percentage for this group is not as high as the "very likely" group, this population has a lower likelihood expectation as well.

The correspondence between likelihood and preparation continues in the lower likelihood categories. Among those in the group responding as "not very likely" that their enterprise would be targeted by an APT, 51.0 percent report feeling at least prepared for an attack, and among the "not at all likely" group, only 43.0 percent consider themselves prepared **(figure 8).**

Technology

Respondents are leveraging a variety of preventive, detective and investigative controls to help reduce the likelihood of a successful breach. A very high percentage of those surveyed responded that they are using antivirus and anti-malware (96.0 percent) and/or traditional network perimeter technologies (to thwart APTs), but much lower scores were seen for critical controls for mobile devices, remote access technologies (RATs) and logging/event correlation **(figure 9).**

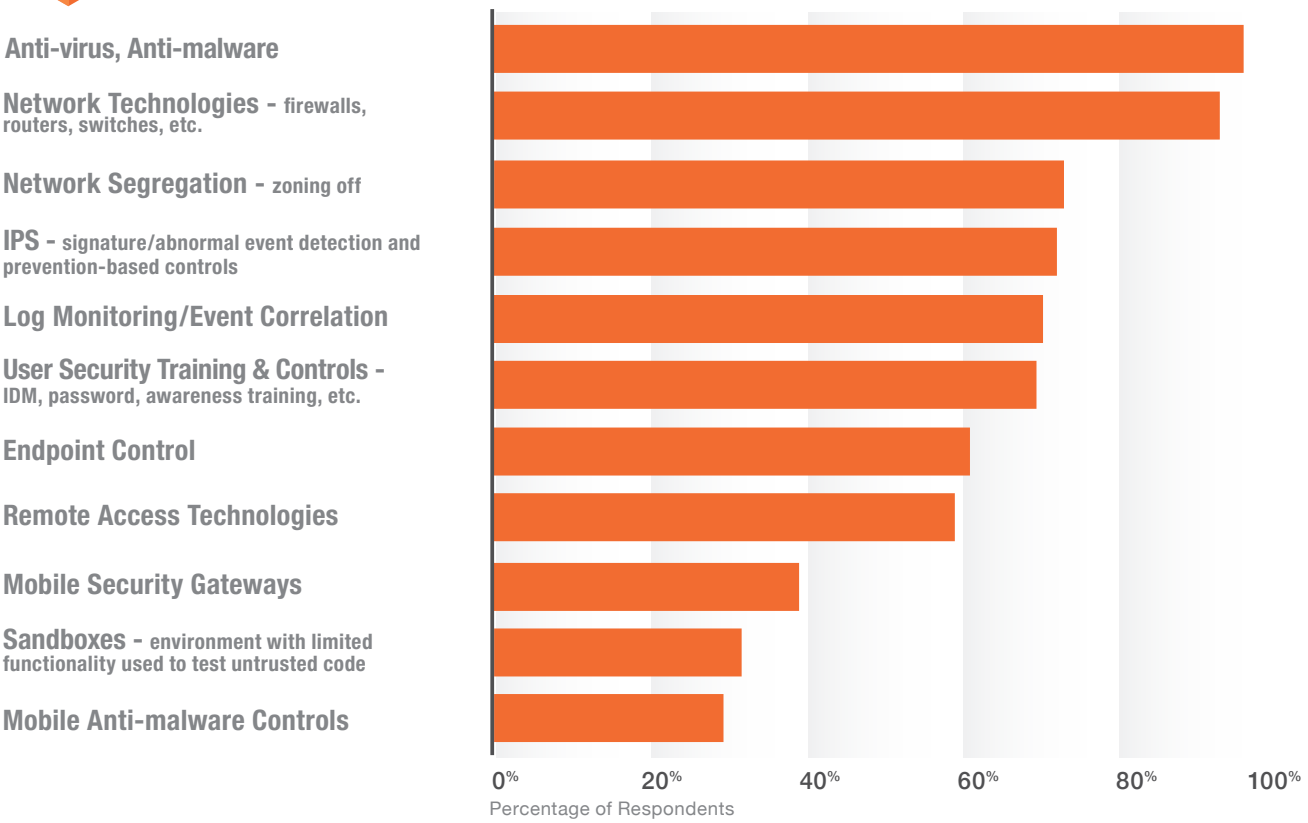
In addition to these technical controls, 69.0 percent of those surveyed responded that they are using training and education to help prevent against attacks such as spear phishing and social engineering, which specifically attempt to exploit the human factor.

FIGURE 8 Correlation Between Likelihood of and Preparedness for an APT Attack

	Very Likely	Likely	Not Very Likely	Not at all Likely
Very Prepared—We have a documented and tested plan in place for APT.	33.73% (57)	13.37% (65)	7.36% (24)	17.39% (4)
Prepared—But incident management does not specifically cover APT.	41.42% (70)	58.02% (282)	43.87% (143)	26.09% (6)
Not Very Prepared	21.89% (37)	26.34% (128)	44.48% (145)	26.09% (6)
Not Prepared At All	2.96% (5)	2.26% (11)	4.29% (14)	30.43% (4)
Total	169	486	326	23

FIGURE 9 Technical Controls Used to Protect Against APT Attacks

WHICH SPECIFIC CONTROLS IS YOUR ENTERPRISE USING TO PROTECT SENSITIVE DATA FROM APT ATTACKS?



In the incident management section, a correlation was demonstrated between perceived likelihood of APT attack and degree of preparation to deal with the attack. A similar alignment is reflected in the correlation between enterprises that are perceived to be a likely or very likely target of an APT and those that seem to be using more technical controls **(figure 10).**

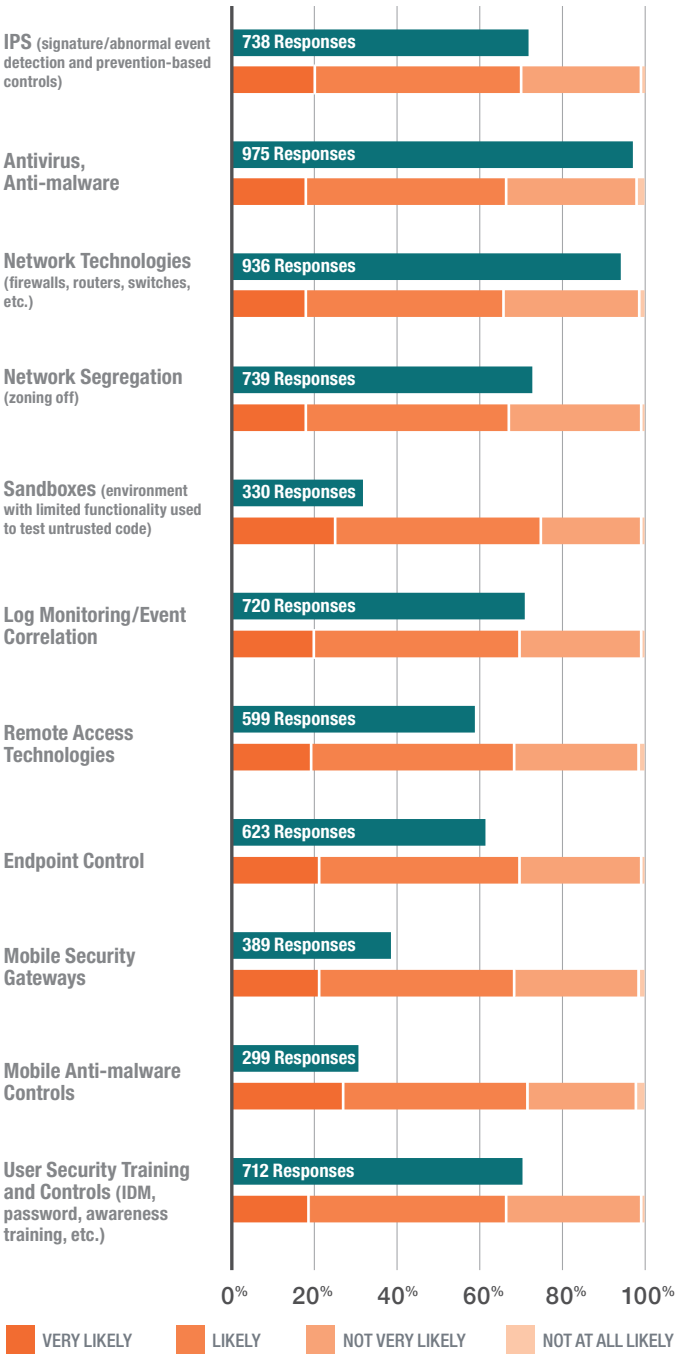
Educational training also proved to be more prevalent as a defense within enterprises that felt very likely to become targets. While it is a positive sign that a higher level of perceived likelihood of an APT breach correlates to the increased use of technical and educational controls, it is concerning that network perimeter technologies and antivirus and anti-malware top the list of controls used because APTs have been shown to leverage zero-day vulnerabilities, which render tools that look for known signatures and vulnerabilities irrelevant.

Mobile security reflects very low usage to help defend against APTs despite the fact that 88.0 percent of respondents recognized BYOD with rooting and jailbreaking as significant in the likelihood of an attack.

FIGURE 10

Correlation Between Likelihood of APT Attack and Use of Technical Controls

WHICH SPECIFIC CONTROLS ARE YOUR ENTERPRISE USING TO PROTECT SENSITIVE DATA FROM APT ATTACKS?



APT Impact on Policies and Practices

The threat of APT attack calls for many defensive approaches, among them technical controls, changes in human resource awareness training and updates to third-party agreements. Another consideration examined in the survey is the effect of APT threats on the policies in the enterprise and the practices and attitudes from executive management toward cybersecurity initiatives.

Vendor Management

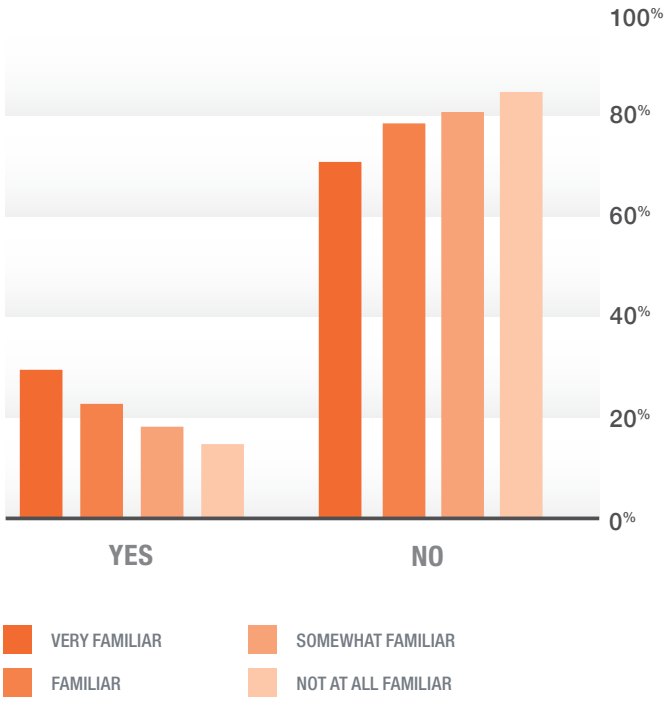
Vendor management is an important factor for protecting outsourced data. Therefore, the study examined the ongoing relationship with third parties to see whether enterprises are adjusting contract language or service level agreements (SLAs) to ensure that third parties have practiced due diligence to protect themselves from APTs and to require financial restitution in the event that—despite controls—they are breached, resulting in damage to the customer.

Overall, 77.0 percent of respondents have not updated agreements with third parties for protection against APTs. While this is still a disturbing statistic, it does show improvement over the previous year's survey in which almost 82.0 percent reported that they had not adjusted third-party agreements. The percentage improves slightly when examined against the variable of familiarity with APTs. **(Figure 11)** illustrates how familiarity with APTs and the updating of third-party agreements align.

77% of respondents have not updated agreements with third parties for protection against APTs.

FIGURE 11 Correlation Between Familiarity With APTs and Updating of Third-party Agreements

HAS YOUR ENTERPRISE CHANGED THE LANGUAGE IN SERVICE LEVEL AGREEMENTS WITH THIRD PARTIES TO ACCOMMODATE APTS?



Executive Involvement

Given the increased attention that APTs have received in recent years, it might be expected that executives would become more involved in cybersecurity activities. Survey respondents were asked to indicate whether they noted a change in executive activity within their enterprise. In a similar fashion to other findings in the study, there was a correlation between the perceived likelihood of the enterprise being an APT target and the level of executive involvement, with more likely targets reflecting increased executive involvement and less likely targets showing less executive engagement **(figure 12).**

Those who indicated seeing increased executive involvement in security initiatives were asked the types of specific actions in which executives were engaging. Given a list of possible activities that consisted of increased security budgets, increased visible support from senior executives, and increased policy enforcement, the majority (79.0 percent) reported seeing increased visible support from senior executives, while 61.0 percent noted increased policy enforcement. Half of the respondents had experienced an increase in their security budget.

However, when the responses are filtered according to the likelihood of the enterprise being targeted by APTs, the numbers shift **(figure 13).**

Although increased security budgets and increased policy enforcement are being experienced by those who consider it very likely that their enterprises will be targeted by APTs, all enterprises, regardless of perceived likelihood, seem to be benefitting from increased visible support from senior executives.

FIGURE 12

Correlation Between Likelihood of APT Attack and Executive Involvement

DO YOU BELIEVE THAT EXECUTIVE MANAGEMENT WITHIN YOUR ENTERPRISE IS BECOMING MORE INVOLVED WITH CYBERSECURITY ACTIVITIES AS A RESULT OF RECENT, VISIBLE APT ATTACKS?

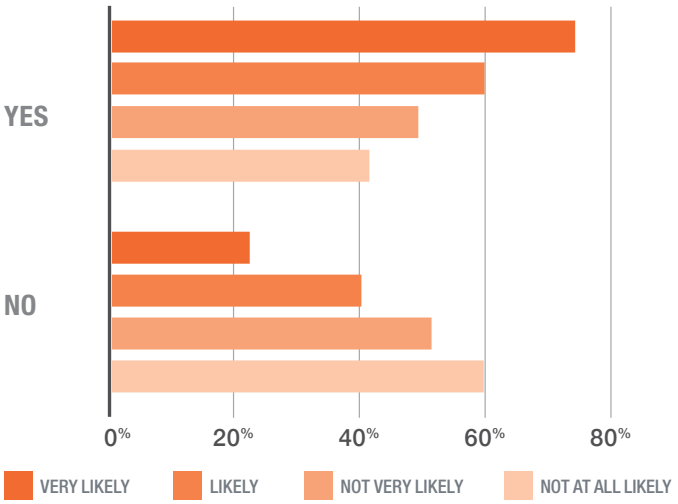
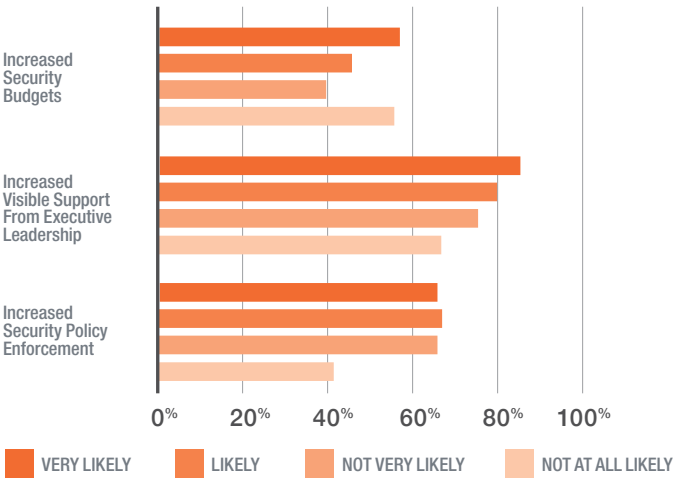


FIGURE 13

Correlation Between Likelihood of APT Attack and Executive Actions Taken

IF YES, WHAT ACTIONS ARE THEY TAKING?



Incident Management and Awareness Training

Managing a successful APT attack is not always as easy as removing the violating threat. Many APTs are adaptable and have the ability to change to suit the circumstances. Typical incident response plans designed to stop and remediate might not be suitable for APTs; the plans should be reviewed and incorporation of specific provisions for APTs considered. The 2014 survey indicates an improvement over the previous survey's level of preparedness, with 70.0 percent of those who feel that it is very likely that their enterprises will be targeted by an APT reporting that adjustments had been made to their incident response plans **(figure 14).**

Unfortunately, the same attention is not being applied to awareness training. Overall, 67.0 percent of respondents report that they have not increased awareness training relative to APTs. The percentages improve slightly for enterprises that are considered very likely or likely targets of an APT, but even in these cases, just slightly over half are increasing awareness training **(figure 15).** This statistic is troubling, as frequently targeted spear phishing and web browsers are attack vectors that could possibly be reduced with well-trained staff.

67.0% OF RESPONDENTS REPORT THAT THEY HAVE NOT INCREASED AWARENESS TRAINING RELATIVE TO APTs.

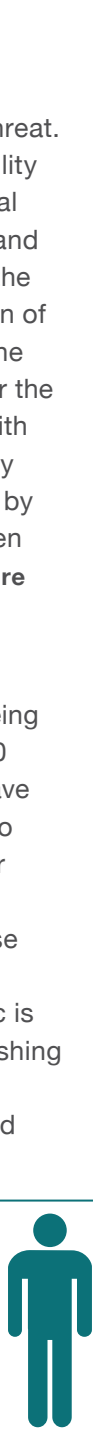


FIGURE 14

Adjustment of Incident Response Plans

ARE INFORMATION SECURITY MANAGERS ADJUSTING THEIR INCIDENT RESPONSE PLANS TO ACCOMMODATE APT ATTACKS?

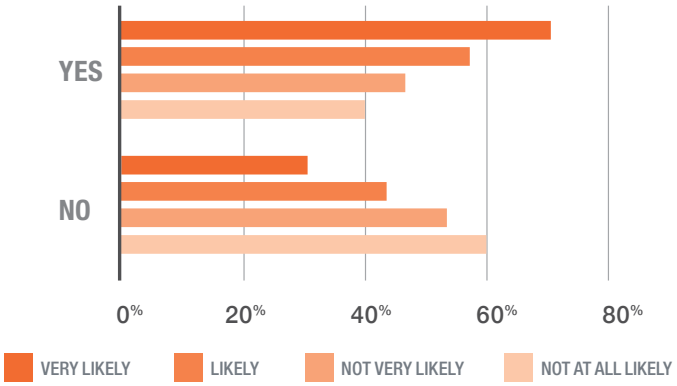
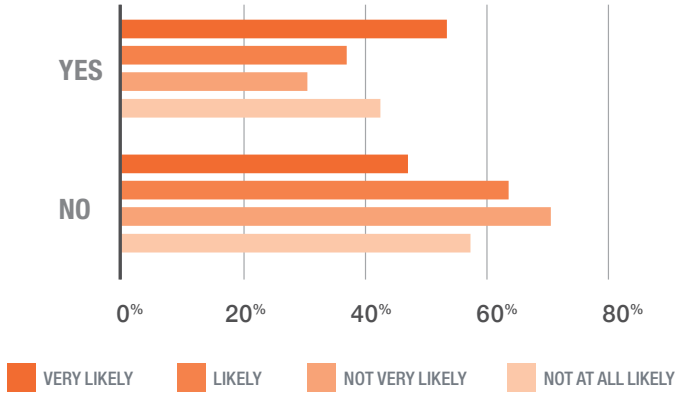


FIGURE 15

Increase in Awareness Training

HAS YOUR ENTERPRISE INCREASED SECURITY TRAINING AS A RESULT OF APTS?



Conclusions

The 2014 survey uncovered many positive findings. Overall, more people are aware of APTs than last year and are making positive changes to be more protected from APTs. The participating security professionals seem to be practicing good security management by utilizing a risk-based approach to managing APTs within their enterprise. This is shown throughout the research, as enterprises that considered themselves more likely to experience an APT seem to have adopted a layered approach to managing their enterprise security. In almost all cases, the higher the perceived likelihood of becoming a target, the more consideration is being given to APTs in terms of technology, awareness training, vendor management, incident management and increased attention from executives. This activity and corresponding effort are excellent for information protection.

However, APTs are still not clearly understood. They are different from traditional threats and need to be considered as a different class of threat. There is still a gap in the understanding of what APTs are and how to defend against them. This is demonstrated by the number of respondents who label themselves as at least familiar with APTs (70.0 percent) as compared to those who feel that APTs are similar to traditional threats (50.0 percent).

Additional data show that enterprises have not really changed the ways in which they protect against APTs. The technical controls most often identified as being used to prevent APTs are network perimeter technologies such as firewalls and access lists within routers, as well as anti-malware and antivirus. While these controls are proficient for defending against traditional attacks, they are probably not as well suited for preventing APTs for a number of reasons: APTs exploit zero-day threats, which leverage unknown vulnerabilities, and many APTs enter the enterprise through well-designed spear-phishing attacks. This indicates that additional controls—and perhaps an increased focus on email security and user education—could be beneficial.

Finally, 75.0 percent of respondents noted that there is a lack of guidance in the market focused on APTs. As part of its continual effort to serve its members and other constituents, ISACA has created the Cybersecurity Nexus (CSX) program to provide resources to help professionals address challenges in cybersecurity, one component of which will concentrate on APTs.

Finally, 75 percent of respondents noted that there is a lack of guidance in the market focused on APTs. As part of its continual effort to serve its members and other constituents, ISACA has created the Cybersecurity Nexus (CSX) program to provide resources to help professionals address challenges in cybersecurity, one component of which will concentrate on APTs.

To learn more visit us at
www.isaca.org/cyber