



# Advanced Persistent Threat Awareness

## *Study Results*

Advanced persistent threat (APT) has been a term used frequently during security threat discussion; 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 important and have the ability to impact national security and economic stability, the study also demonstrates that the controls being used to defend against APT might not be sufficient to adequately protect enterprise networks.

*Sponsored By*



## ISACA®

With more than 100,000 constituents in 180 countries, ISACA ([www.isaca.org](http://www.isaca.org)) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT 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™) designations.

ISACA continually updates and expands the practical guidance and product family based on the COBIT® framework. COBIT helps IT professionals and enterprise leaders fulfill their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

### Disclaimer

ISACA has designed and created *Advanced Persistent Threat Awareness Study Results* (the “Work”) primarily as an educational resource for those interested in APT. 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](mailto:info@isaca.org)

**[www.isaca.org](http://www.isaca.org)**

---

### Provide feedback:

[www.isaca.org/cybersecurity](http://www.isaca.org/cybersecurity)

### Participate in the ISACA Knowledge Center:

[www.isaca.org/knowledge-center](http://www.isaca.org/knowledge-center)

### Follow ISACA on Twitter:

[www.twitter.com/ISACANews](http://www.twitter.com/ISACANews)

### Join ISACA on LinkedIn:

[www.linkedin.com/ISACAOOfficial](http://www.linkedin.com/ISACAOOfficial)

### Like ISACA on Facebook:

[www.facebook.com/ISACAHQ](http://www.facebook.com/ISACAHQ)

## ISACA Wishes to Recognize:

### Contributors

**Vilius Benetis,**  
Ph.D., CISA, CRISC, BAIP,  
Lithuania

**Jeimy J. Cano,**  
Ph.D., CFE, CMAS, Ecopetrol,  
Colombia

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

**Jo Stewart-Rattray,**  
CISA, CISM, CGEIT, CRISC,  
CSEPS, BRM Holdich,  
Australia

### Knowledge Board

**Marc Vael,**  
Ph.D., CISA, CISM, CGEIT,  
CRISC, CISSP, Valuendo,  
Belgium, Chairman

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

**Steven A. Babb,**  
CGEIT, CRISC, Betfair,  
UK

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

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

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

**Salomon Rico,**  
CISA, CISM, CGEIT,  
Deloitte LLP,  
Mexico

### ISACA Board of Directors

**Gregory T. Grocholski,**  
CISA, The Dow Chemical Co.,  
USA, International President

**Allan Boardman,**  
CISA, CISM, CGEIT, CRISC, ACA,  
CA (SA), CISSP, Morgan Stanley,  
UK, Vice President

**Juan Luis Carselle,**  
CISA, CGEIT, CRISC, Wal-Mart,  
Mexico, Vice President

**Christos K. Dimitriadis,**  
Ph.D., CISA, CISM, CRISC,  
INTRALOT S.A.,  
Greece, Vice President

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

**Tony Hayes,**  
CGEIT, AFCHSE, CHE, FACS, FCPA,  
FIIA, Queensland Government,  
Australia, Vice President

**Jeff Spivey,**  
CRISC, CPP, PSP,  
Security Risk Management Inc.,  
USA, Vice President

**Marc Vael,**  
Ph.D., CISA, CISM, CGEIT,  
CRISC, CISSP, Valuendo,  
Belgium, Vice President

**Kenneth L. Vander Wal,**  
CISA, CPA, Ernst & Young LLP (retired),  
USA, Past International President

**Emil D'Angelo,**  
CISA, CISM, Bank of Tokyo-Mitsubishi  
UFJ Ltd. (retired),  
USA, Past International President

**John Ho Chi,**  
CISA, CISM, CRISC, CBCP, CFE,  
Ernst & Young LLP,  
Singapore, Director

**Krysten McCabe,**  
CISA, The Home Depot,  
USA, Director

**Jo Stewart-Rattray,**  
CISA, CISM, CGEIT, CRISC, CSEPS, BRM  
Holdich, Australia, Director

### Guidance and Practices Committee

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

**Dan Haley,**  
CISA, CGEIT, CRISC, MCP, Johnson &  
Johnson,  
USA

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

**Aureo Monteiro  
Tavares Da Silva,**  
CISM, CGEIT, Vista Point,  
Brazil

**Jotham Nyamari,**  
CISA, Deloitte,  
USA

**Connie Lynn Spinelli,**  
CISA, CRISC, CFE, CGMA, CIA, CISSP,  
CMA, CPA, BKD LLP,  
USA

**Siang Jun Julia Yeo,**  
CISA, CPA (Australia), Visa Worldwide Pte.  
Limited, Singapore

**Nikolaos Zacharopoulos,**  
CISA, CISSP, DeutschePost-DHL,  
Germany

### Special Recognition



## Table of Contents

Introduction to the Report	05
Defining Advanced Persistent Threats	06
Description of the Population	08
Perspectives on APT	09
Awareness	09
Direct APT Experience	11
Security Controls, Processes and Responses	12
APT Impact on Policies and Practices	15
Conclusions	19

## List of Figures

Figure 01	Industry Distribution	08
Figure 02	Geographic Distribution	08
Figure 03	Familiarity With APTs	09
Figure 04	Comparison of APTs and Traditional Threats	10
Figure 05	Highest Enterprise Risk of Successful APT Attack	10
Figure 06	Enterprise Perceived Likelihood of Becoming APT Target	11
Figure 07	Enterprise Ability to Deal With APT Attack	11
Figure 08	Correlation Between Likelihood of and Preparedness for an APT Attack	12
Figure 09	Technical Controls Used to Protect Against APT Attacks	13
Figure 10	Correlation Between Likelihood of APT Attack and Use of Technical Controls	14
Figure 11	Correlation Between Familiarity With APTs and Update of Third-party Agreements	15
Figure 12	Correlation Between Likelihood of APT Attack and Executive Involvement	16
Figure 13	Correlation Between Likelihood of APT Attack and Executive Actions Taken	17
Figure 14	Adjustment of Incident Response Plans	17
Figure 15	Increase in Awareness Training	18



## Introduction to the Report

The Advanced Persistent Threat (APT) Awareness Study was undertaken by ISACA in the fourth quarter of 2012. APTs have made headlines in the last few years for breaching some of the most well-known enterprise networks. Once thought to be limited to attacks on government networks, the Google Aurora attack in 2010 made it very clear that APTs are not just government threats. Large-scale breaches followed and made international headlines. RSA's 2011 breach was classified as being caused by an APT and, of course, awareness of Stuxnet and Flame is widespread. 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 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 information security professionals through LinkedIn.

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

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



# Defining Advanced Persistent Threats

Information security breaches resulting in lost data, financial damage to companies, disruption of services and reputational damage are nothing new. Enterprises have faced malicious activity directed at them as well as threats from nonmalicious users ever since they networked systems. Malware, social engineering, hacking, SQL injections and denial of service are attack vectors that many security professionals wish they had not experienced, but, unfortunately, have. Many preventive controls have emerged that have made it more difficult for those with malicious intent to penetrate networks, while detective controls have helped to identify quickly when a breach does occur.

Recent large-scale security breaches have highlighted a new class of threat to networks. APTs have made global headlines, to the dismay of many enterprises. Traditionally considered as nation-state-sponsored activities aimed at government networks, the threats have become problematic for enterprises as well. RSA, Google, NASA and the Iranian government have experienced large security breaches due to APTs, demonstrating that APTs effectively target both enterprise and government networks.

APTs differ significantly from traditional threats, yet they leverage many of the same attack vectors. Because so many different opinions of what constitutes an APT exist in the market, establishing

the definition for the study was critical. APTs are often aimed at the theft of intellectual property (espionage) as opposed to achieving immediate financial gain and are prolonged, stealthy attacks. This report 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.<sup>1</sup>*

This definition provides a good base from which to understand the differences between traditional threats and APTs. Repeated pursuit of objectives, adaptation to defenders and persistence differentiate APTs from a typical attack. 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 differ significantly from traditional threats, yet they leverage many of the same attack vectors.**

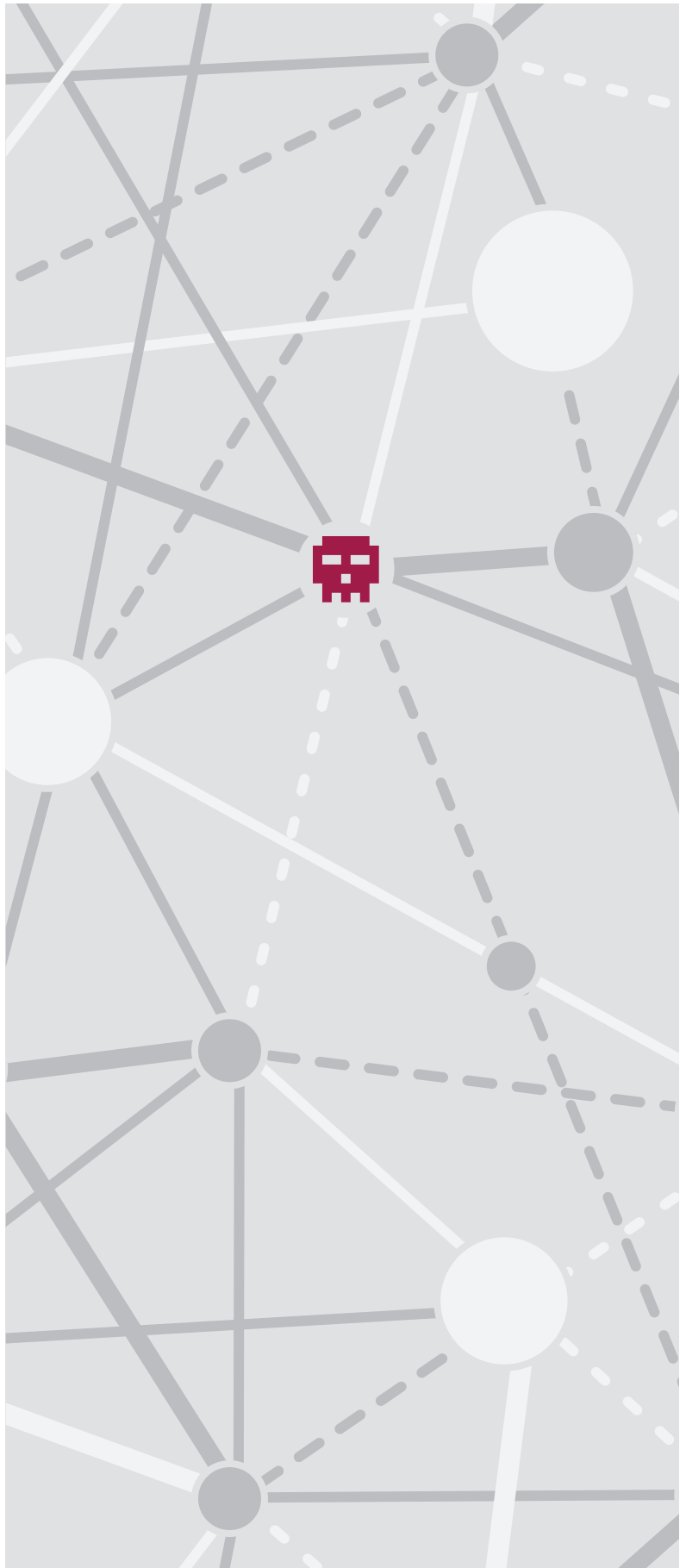
---

<sup>1</sup> National Institute of Standards and Technology (NIST), Special Publication 800-39, Managing Information Security Risk, Organization, Mission, and Information System View, USA, 2011

The APT is advanced and stealthy, often possessing the ability to conceal itself within the enterprise network traffic, interacting just enough to get what it needs to accomplish its job. This ability to disguise itself and morph when needed can be crippling to security professionals' attempts to identify or stop an APT attack. The APT's single-minded persistence on pursuing its target and repeated efforts to complete the job it has been created to do means it will not go away after one failed attempt. It will continually attempt to penetrate the desired target until it meets its objective.

Stealthiness, adaptability and persistence characterize 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 the APT does not stop. The people and groups behind APT attacks are determined and have the resources to be able to launch zero-day attacks on enterprises. This makes it hard to defend against them.

Spear phishing has become a very common method used by those launching APTs as an entry point to an enterprise. Often email filters are not effective enough to identify these well-designed spear phishinges and then it takes only a single user to click a link and open an attachment for an APT to begin to execute its first phase of an attack. Adding the human factor to a threat class that does not prey on known vulnerabilities makes defense and prevention even more challenging.



# 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 purposive global sample included those who hold ISACA's CISM credential and information security professionals within groups on LinkedIn focused on cybersecurity and APTs.

SurveyMonkey ([www.surveymonkey.com](http://www.surveymonkey.com)) was used to collect the data from 1,551 individuals globally, 93.1 percent of whom were members of ISACA.

More than 20 industries were represented in the study, the majority of respondents (30.9 percent) were from the technology services and consulting field (**figure 01**).

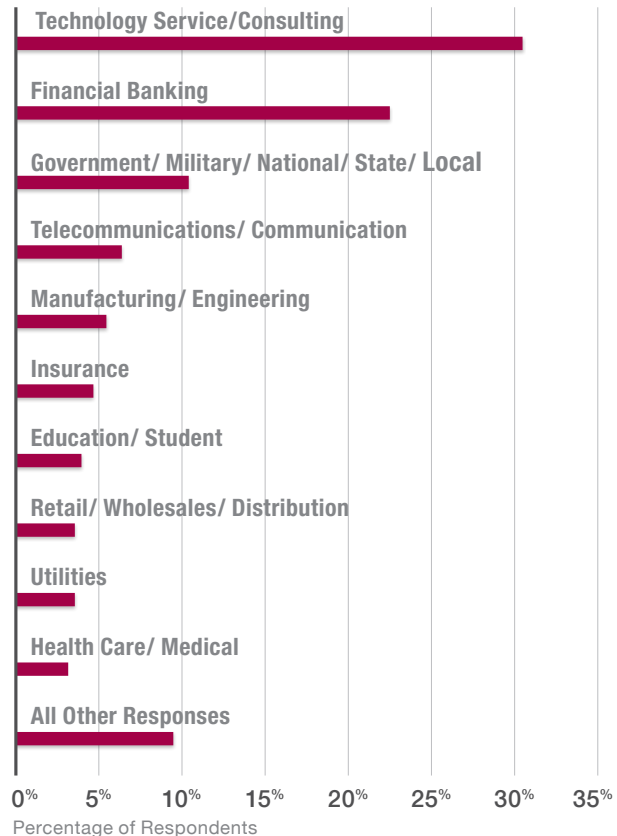
The majority of respondents reside in Europe/Africa (38.3 percent), followed by North America (32.0 percent) (**figure 02**).

## A TYPICAL PARTICIPANT CAN BE DESCRIBED AS:

- An ISACA member (1,434)
- European/African (591) or North American (493)
- Belonging to the technology services consulting industry (457) or the financial services/banking industry (340)

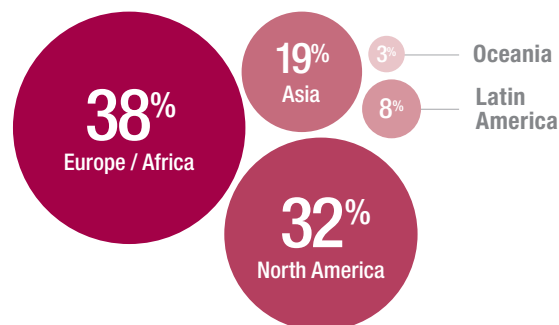
## FIGURE 01 Industry Distribution

WITHIN WHICH OF THE FOLLOWING INDUSTRIES ARE YOU EMPLOYED?



## FIGURE 02 Geographic Distribution

IN WHICH OF THE FOLLOWING AREAS DO YOU RESIDE?





# Perspectives on APT

Many positive indicators were identified throughout the study, but it should also be noted that responses seemed to conflict as further analysis was completed. Positives such as increased management attention, security budgets and policy enforcement conflicted with respondents' indications that they are not increasing security awareness nor changing the way they deal with third parties.

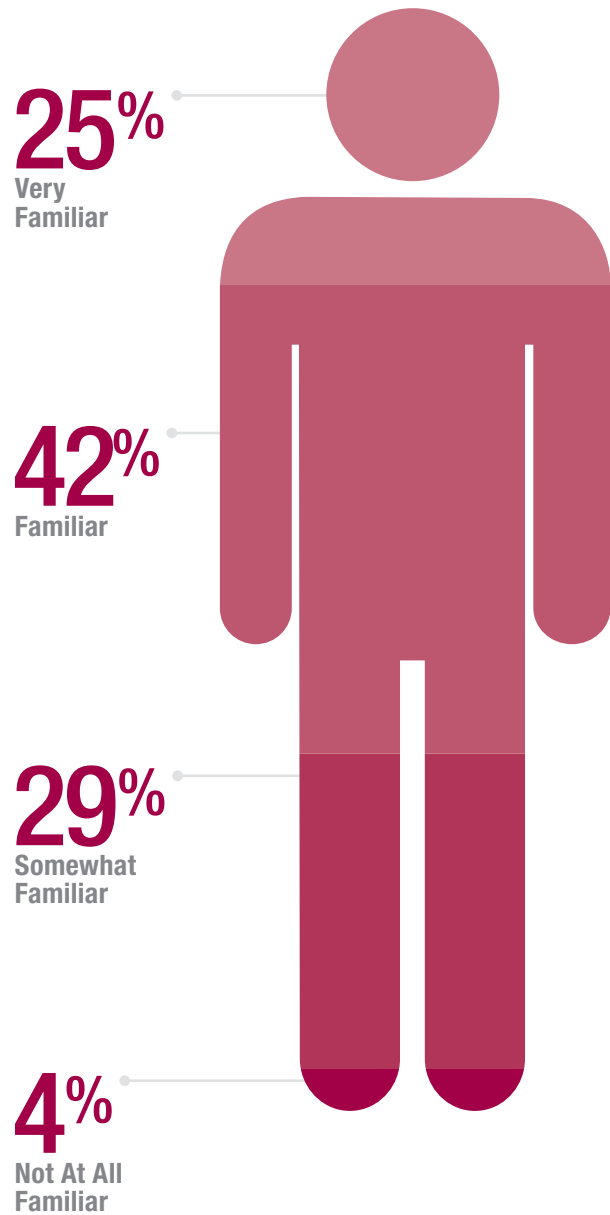
**53.4% of respondents indicated that they do not believe APTs differ from traditional threats.**

## Awareness

The survey results reveal that 25.1 percent of respondents are very familiar with APTs, with a total of 96.2 percent expressing that they are at least somewhat familiar (*figure 03*).

## FIGURE 03 Familiarity With APTs

HOW FAMILIAR ARE YOU WITH APTs?



While this degree of familiarity with APTs is a positive indicator, it appears to be negated by the 53.4 percent response indicating that survey participants do not believe APTs differ from traditional threats (*figure 04*).

This finding is troubling because it implies that confusion does exist 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, they will find it difficult to properly identify, defend against and respond to an APT. With 93.9 percent of respondents report that they believe that APTs represent a credible threat to national security and economic stability, the importance of having a clear understanding of what they are is self-evident.

**OTHER AWARENESS HIGHLIGHTS INCLUDE:**

89.7 percent of respondents believe that the use of social networking sites increases the likelihood of a successful APT attack.

87.3 percent think that “bring your own device” (BYOD), combined with rooting (Android manipulation by the owner of the device to gain more access to operating system (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. Loss of enterprise intellectual property was the highest response, at 25.5 percent, and loss of customer or employee personally identifiable information (PII) finished next, at 23.6 percent (*figure 05*).

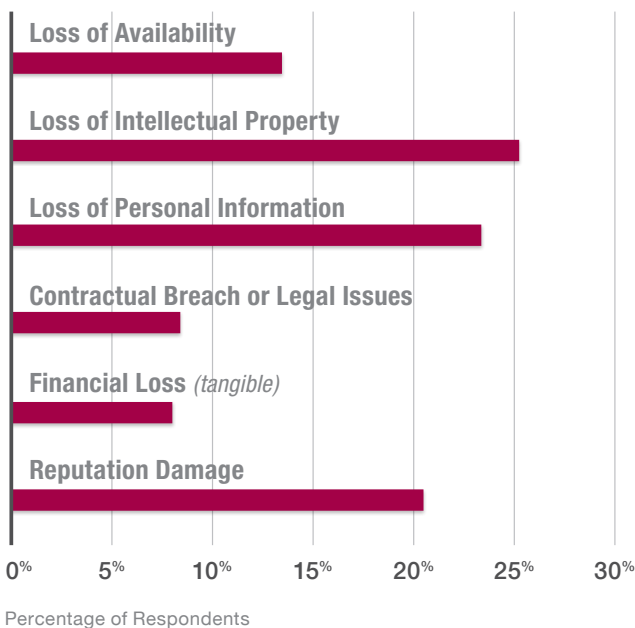
## FIGURE 04 Comparison of APTs and Traditional Threats

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



## FIGURE 05 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 the 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 21.6 percent of respondents reported having been subject to an APT attack. Of those, 26.2 percent were employed in the technology services and consulting field, followed by 22.7 percent working in financial services. Additionally, those who had been subject to attack were asked if they were able to identify the source of the attack; 65.4 percent answered affirmatively.

Although only 21.6 percent of respondents reported that their enterprise has already been victimized by an APT, roughly three times that number—63.0 percent—believe that it is only a matter of time before their enterprise is targeted. (figure 06)

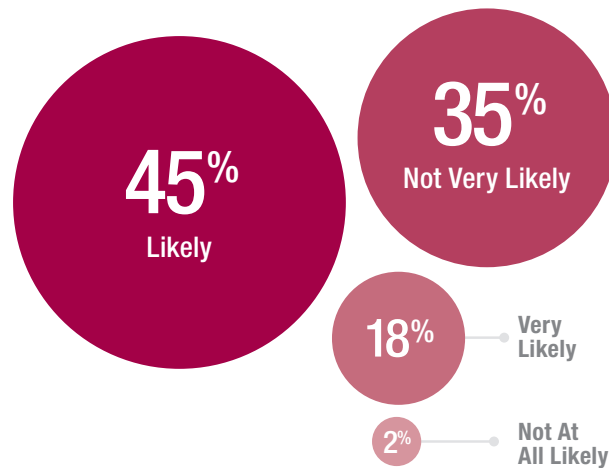
**63%** of respondents think it is only a matter of time until their enterprise is targeted by an APT.

All respondents were asked if they considered their enterprise prepared to deal with the threat of APTs. The majority indicated their belief that they do have the ability to detect, respond to and stop a successful APT attack (figure 07).

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

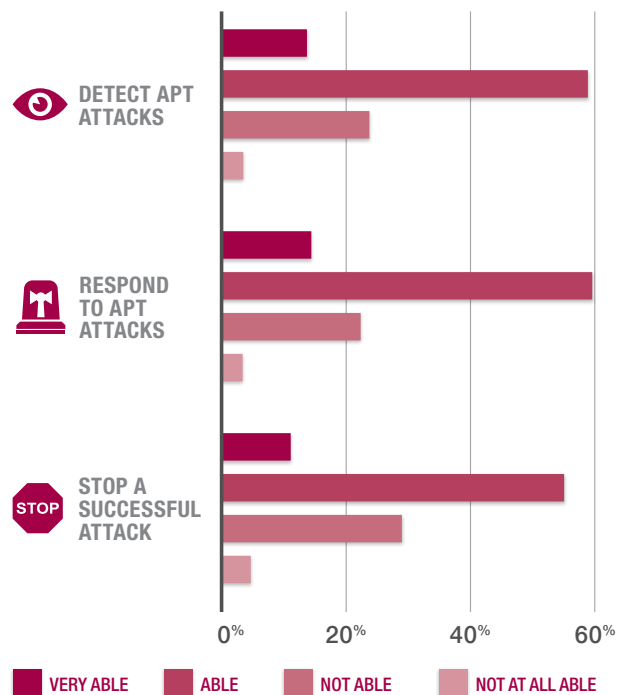
## FIGURE 06 Enterprise Perceived Likelihood of Becoming APT Target

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



## FIGURE 07 Enterprise Ability to Deal With APT Attack

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



Security Controls,  
Processes and Responses

As noted previously, the majority of respondents believe 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 APTs. Controls are more prevalent in enterprises that feel they could be targeted for an APT attack than in those that do not feel the likelihood of becoming an APT target is high.

Incident Management Plans

Overall, nearly 60 percent of respondents believe that they are ready to respond to APT attacks. When asked the degree to which their enterprise is prepared to deal with an APT attack today, 14 percent responded that they are “very prepared,” which indicated that they have a documented and tested plan in place for APT. Another 49.6 percent responded that they are “prepared,” which was defined as having an incident management plan although it does not specifically cover APT. This leaves 37.4 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 respondents’ enterprise being subject to an APT attack and the level of enterprise preparedness to deal with such an incident. Seemingly, higher perceived likelihood of being targeted corresponds to greater enterprise preparedness.

Among the 17.9 percent of respondents who felt it was “very likely” that their organization would be the target of an APT attack, 31.1 percent identified themselves as being in the

FIGURE 08 Correlation Between  
Likelihood of and Preparedness  
for an APT Attack

CORRELATION BETWEEN LIKELIHOOD OF AND  
PREPAREDNESS FOR AN APT ATTACK.

	How likely do you feel that your organization will be the target of an APT?			
	Very Likely	Likely	Not Very Likely	Not at all Likely
Very prepared We have a documented and tested plan in place for APT	31.1% (69)	14% (90)	4.8% (21)	23.1% (6)
Prepared But incident management does not specifically cover APT	49.5% (110)	53.2% (303)	46.7% (205)	26.9% (7)
Not very prepared	15.8% (35)	30.2% (172)	42.1% (185)	34.6% (9)
Not prepared at all	3.6% (8)	2.6% (15)	6.4% (28)	15.4% (4)

“very prepared” category and 49.5 percent placed themselves in the “prepared” category. This demonstrates that a healthy 80.6 percent of those who characterize their enterprise as very likely to be targeted are ready to deal with it. Likewise, those that identified their enterprise as a “likely” target (45.1 percent) state that they too are ready to deal with an attack, with 14.0 percent considering themselves “very prepared” and 53.2 percent claiming that they are “prepared” (total of 67.2 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 categories. Among those in the group responding as “not very likely” that their enterprise would be targeted by an APT, 51.5 percent report feeling at least prepared for an attack, and among the “not at all likely” group, only half consider themselves prepared (figure 08).

## Technology

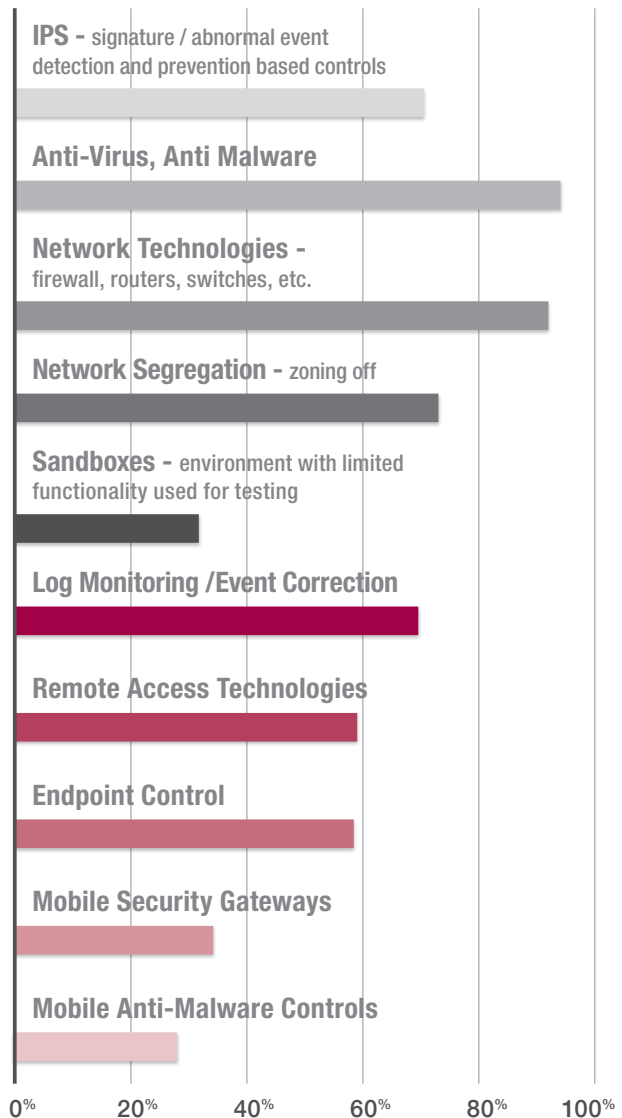
Respondents are leveraging a variety of preventive and detective technical controls as well as education, training and policy to help reduce the likelihood of a successful breach. A very high percentage of those surveyed responded that they are using antivirus and anti-malware and/or traditional network 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 09*).

In addition to these technical controls, 70.6 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.

**A very high percentage of those surveyed responded that they are using antivirus and anti-malware and/or traditional network perimeter technologies to thwart APTs.**

## FIGURE 09 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 here, in that the enterprises that are perceived to be a likely or very likely target of APT seem to be using more technical controls than those that do not classify themselves as likely targets for the threat class (figure 10).

Educational training also proved to be more prevalent as a defense within enterprises who felt it very likely (82.0 percent) or likely (74.1 percent) to become targets.

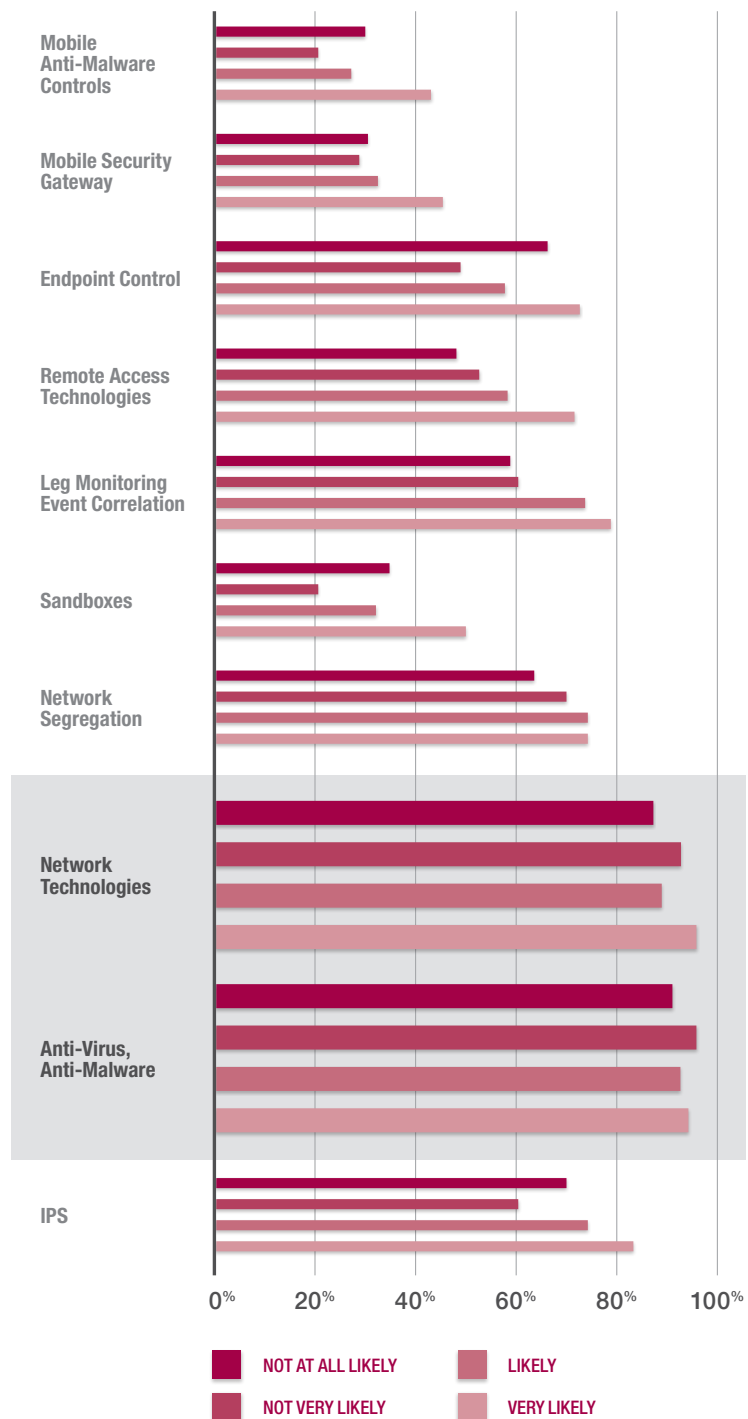
**While it is a positive sign that a higher level of perceived likelihood of an APT breach correlates to the increased use of technical and educational controls, it is concerning that network perimeter technologies and antivirus and anti-malware top the list of controls used.**

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. APTs are quite advanced and are known to avoid the approaches typically caught by these controls. For example, APTs do not tend to target known vulnerabilities that have been patched nor use recognizable signatures that may be needed for intrusion detection and prevention systems.

Mobile security reflects very low usage to help defend against APTs despite the fact that 87.3 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

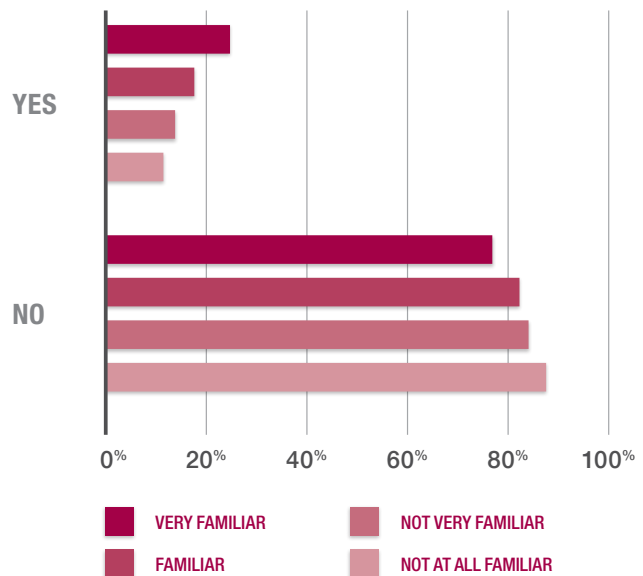
Vendor management is an important factor for protecting outsourced data. Therefore, the survey examined the ongoing relationship with third parties to see if enterprises are adjusting contract language or service level agreements (SLAs) to ensure that third parties have practiced due diligence to protect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

Overall, 81.8 percent of respondents have not updated agreements with third parties for protection against APT, a percentage that is especially surprising when more than two-thirds of respondents (67.6 percent) report familiarity with APTs. Figure 11 illustrates how familiarity with APTs and the update of third-party agreements align.

**82% of respondents have not updated agreements with third parties for protection against APTs.**

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

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



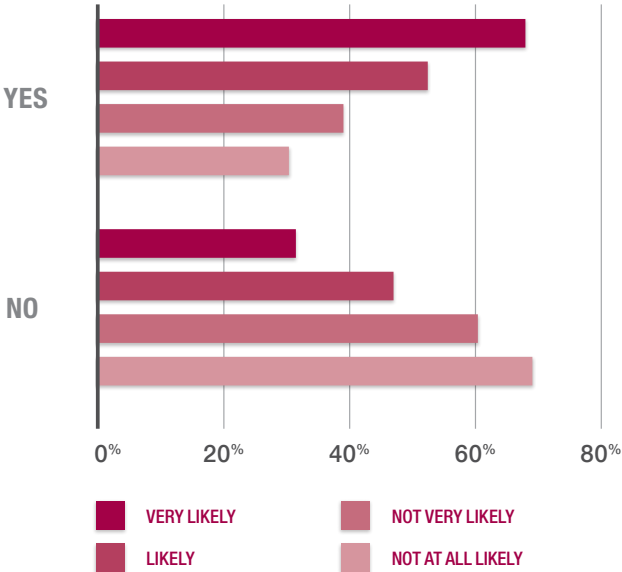
Executive Involvement

Given the increased attention APTs have received in recent years, it might be expected that executives would be becoming more involved in cybersecurity activities. The 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 (79.8 percent) reported seeing increased visible support from senior executives, while 66.0 percent noted increased policy enforcement. Less than half (46.9 percent) had experienced an increase in their security budget.

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?



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

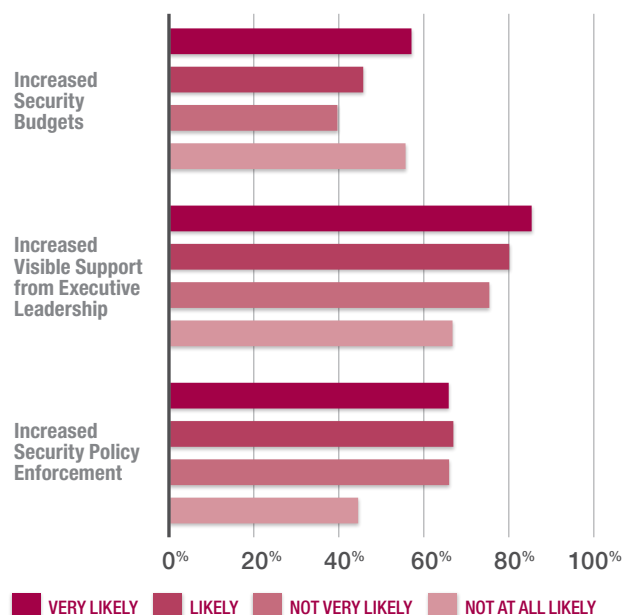
It is interesting that the highest incidences of increased security budgets are occurring in not only the enterprises that find it very likely that they will be targeted by APTs, but also in those who find it not at all likely. Likewise, increased policy enforcement is occurring at a similar rate in enterprises that find it not very likely to be targets (65.9 percent) as in enterprises that find it very likely (65.8 percent).

### 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 an APT; the plans should be reviewed and incorporation of specific provisions for APTs considered. This survey indicates that many respondents have made a start in this area: More than half of the respondents who believe their enterprise is a likely target for APT have considered that the existing incident management plans may need adjustment (*figure 14*).

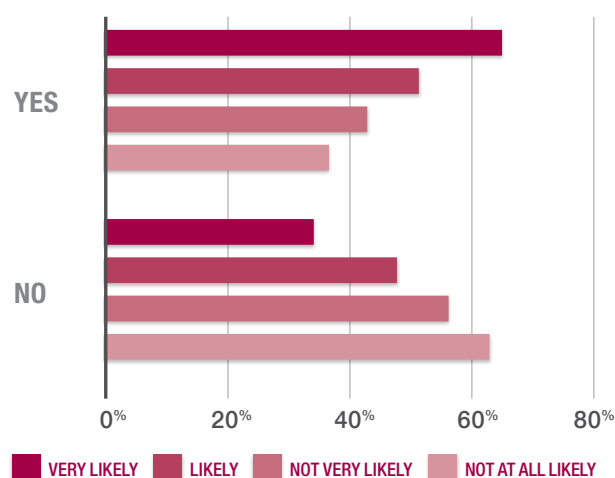
## FIGURE 13 Correlation Between Likelihood of APT Attack and Executive Actions Taken

IF YES, WHAT ACTIONS ARE THEY TAKING?



## FIGURE 14 Adjustment of Incident Response Plans

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



Regrettably, the same consideration is not being given to user awareness training. Overall, 67.3 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, less than half are increasing awareness training (*figure 15*).

67%

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


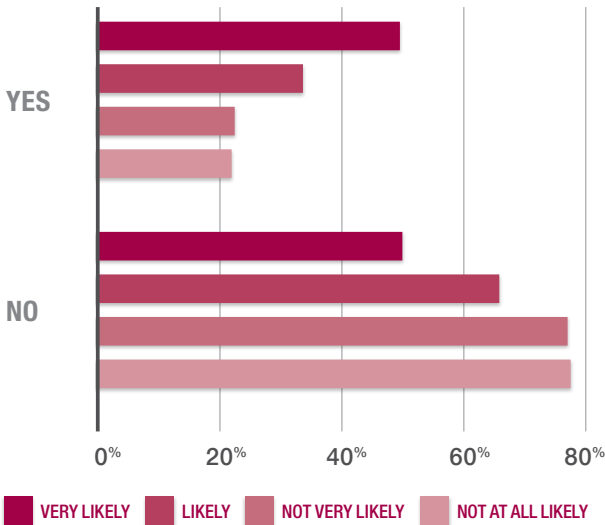


FIGURE 15 Correlation Between Perceived Likelihood of APT Attack and Increase in Awareness Training

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



# Conclusions

The survey demonstrated many positive findings. 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 new to the market. 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 (67.6 percent) as compared to those who feel that APTs are similar to traditional threats (53.4 percent).

Additional data show that the market has not really changed the ways in which it protects against APTs. The technical controls most often identified as being used to prevent against 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 suited for preventing APTs. This is true for a number of reasons: APTs exploit zero-day threats, which are often unknown vulnerabilities, and many APTs enter the enterprise through well-designed spear phishing attacks. This indicates that additional controls - such as

network segregation and perhaps an increased focus on email security and user education could be beneficial. Additionally, the lack of consideration being given to third parties is troubling. Enterprises must be sure that the data they outsource are protected—even if the provider itself experiences an APT attack.

---

**Finally, 79.1 percent of respondents noted that there is a lack of guidance in the market focused on APT. As part of its continual effort to serve its members and other constituents, ISACA is creating a series of products to address challenges in cybersecurity, one component of which will concentrate on APTs.**

---

To learn more visit us at  
[WWW.ISACA.ORG/CYBERSECURITY](http://WWW.ISACA.ORG/CYBERSECURITY)



# Fight Back Against Your Attackers with a Custom Defense

Standard security products simply can't cope with the custom nature of targeted attacks, not to mention their dedicated perpetrators. **The Trend Micro Custom Defense** arms you with a full spectrum of custom detection and intelligence. By weaving your security infrastructure into a tailored and adaptable defense, this unique solution equips you to discover and rapidly respond to your attackers.

Learn more at [www.trendmicro.com/apt](http://www.trendmicro.com/apt)

© 2013 Trend Micro, Inc. All rights reserved. Trend Micro and the t-ball logo are trademarks or registered trademarks of Trend Micro, Inc.

