Advanced Persistent Threat Awareness

Study Results

ISACA®

Trust in, and value from, information systems

The Advanced Persistent Threat

The 2010 Google Aurora attack forever changed the way we look at Internet security. This large-scale, sophisticated attack showed us that all sectors, from private to public, are vulnerable to a new class of security breach:

ADVANCED, STEALTHY AND CHAMELEON-LIKE

in its adaptability, APTs were once thought to be limited to attacks on government networks.

Following the Google attacks* similar targeted intrusions quickly followed, garnering media scrutiny – and growing concern that the APT was more damaging than it seemed.

**Google attacks affected nearly three dozen well-known tech, finance and defense enterprises*

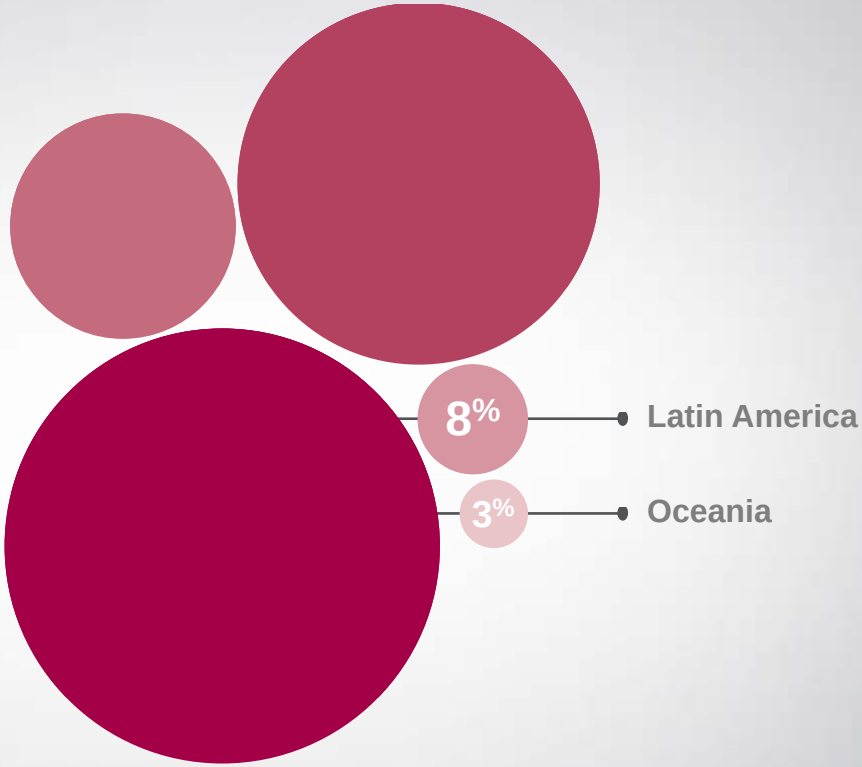
How well do security professionals understand APTs?

How are they affecting different industries and organizations throughout the world?

What is being done to prevent them?

In Q4 of 2012, ISACA launched the APT Awareness Survey to find out.

So ISACA asked **1,500 people** worldwide – from tech service consultants, to people in the banking industry – about APTs.



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

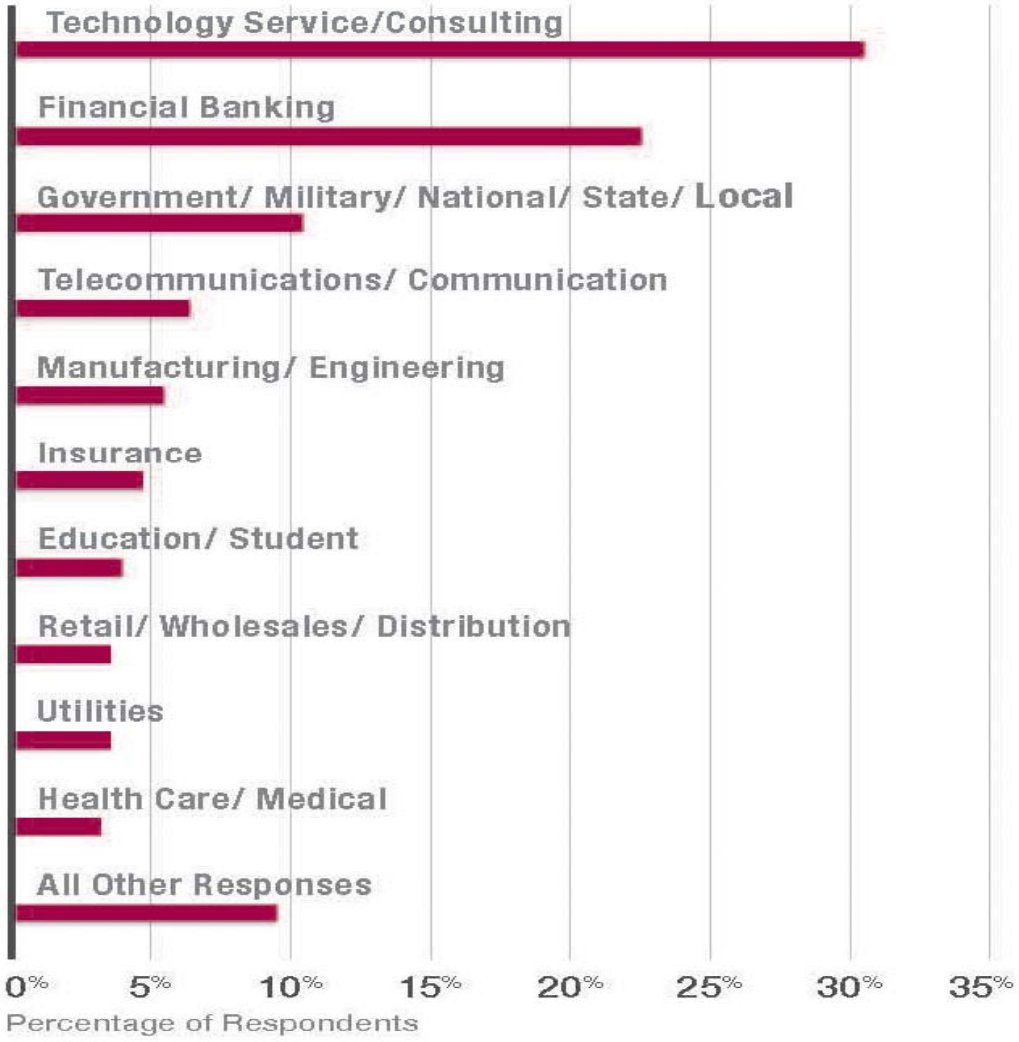
APT Defined
NIST SP 800-39

- 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.

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.

FIGURE 01 Industry Distribution

WITHIN WHICH OF THE FOLLOWING INDUSTRIES ARE YOU EMPLOYED?



AWARENESS

42.5% of respondents were familiar…

28.6%, somewhat familiar…

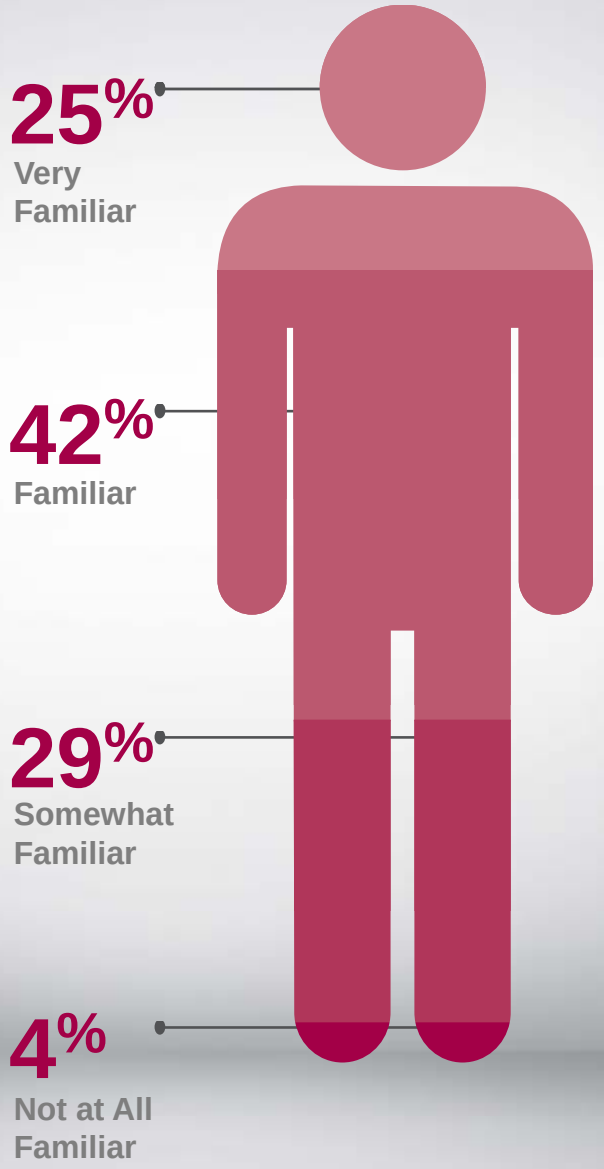
And only **25.1%** very familiar about APTs.

Overall, **96.2%** were somewhat familiar with APTs…

But most importantly:

93.6%

of respondents understood APTs as a very credible, serious threat to national security and economic stability.



Just **46.6%** of respondents believed that APTs were a unique threat.

And more than half **(53.4%)** believe this advanced set of threats is no different to what they've been dealing with in the past.

WHAT DOES THIS MEAN?

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?

There’s a huge disconnect in the IT industry about APTs …

A lack of understanding and education.

Highest Risks on Enterprises from APTs

87.3% BELIEVE THAT

JAILBREAKS, ROOTING & BYOD GREATLY INCREASE THE CHANCES OF AN APT OCCURRING.

Other key highlights

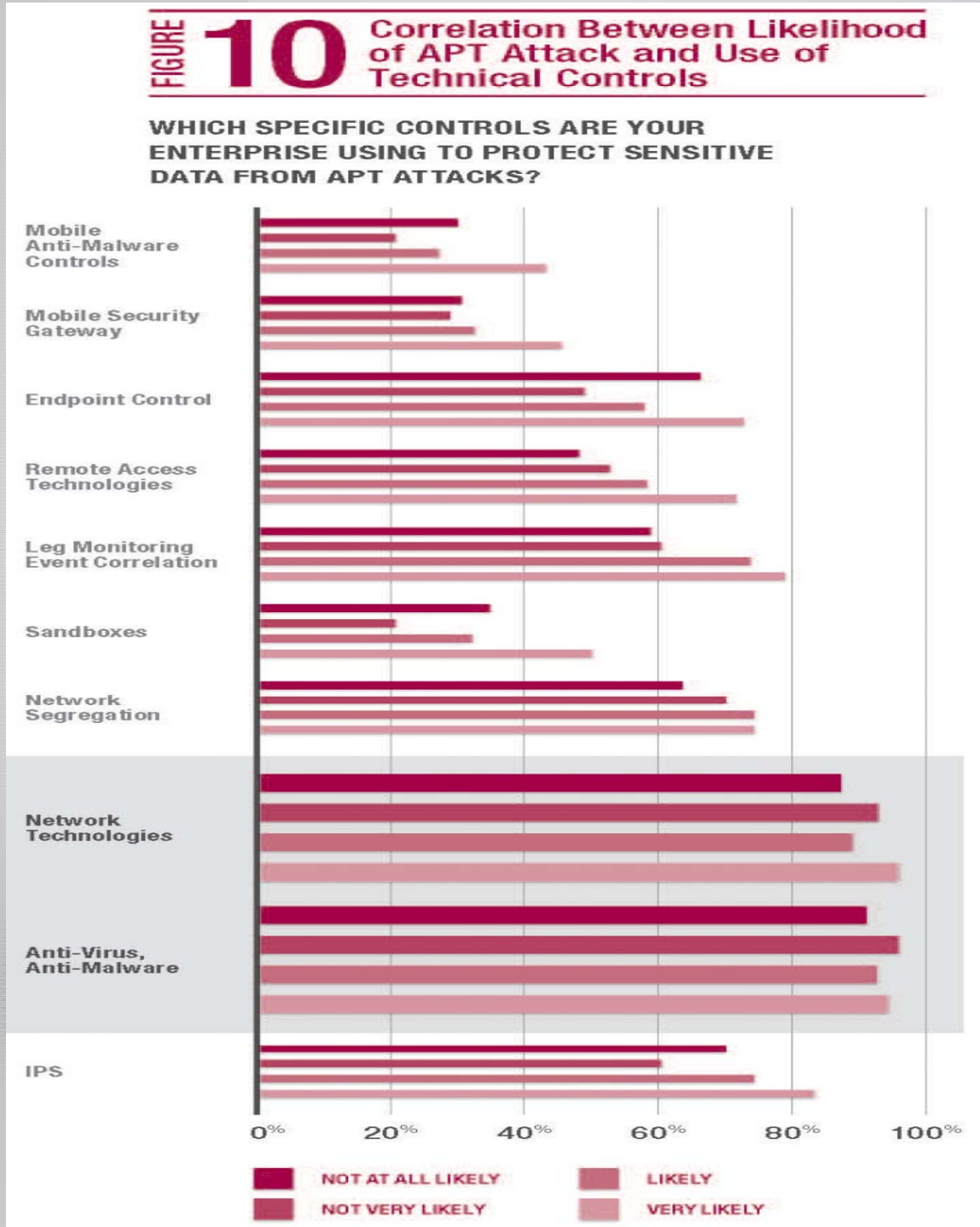
89.7% of respondents believe the use of social networking sites like Facebook or Twitter increases the likelihood of a successful APT attack.

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.

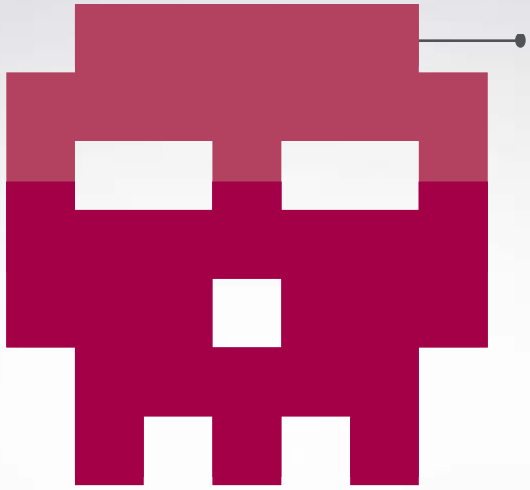
FIGURE 10 Correlation Between Likelihood of APT Attack and Use of Technical Controls



Suffering with an APT

Although just **21.6%** of respondents reported having been victims of an APT attack

63% – three times that amount – believe it's only a matter of time before their business is targeted.



63%

BELIEVE IT'S ONLY A MATTER OF TIME BEFORE THEIR BUSINESS IS TARGETED.

FIGURE 06 Enterprise Perceived Likelihood of Becoming APT Target

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

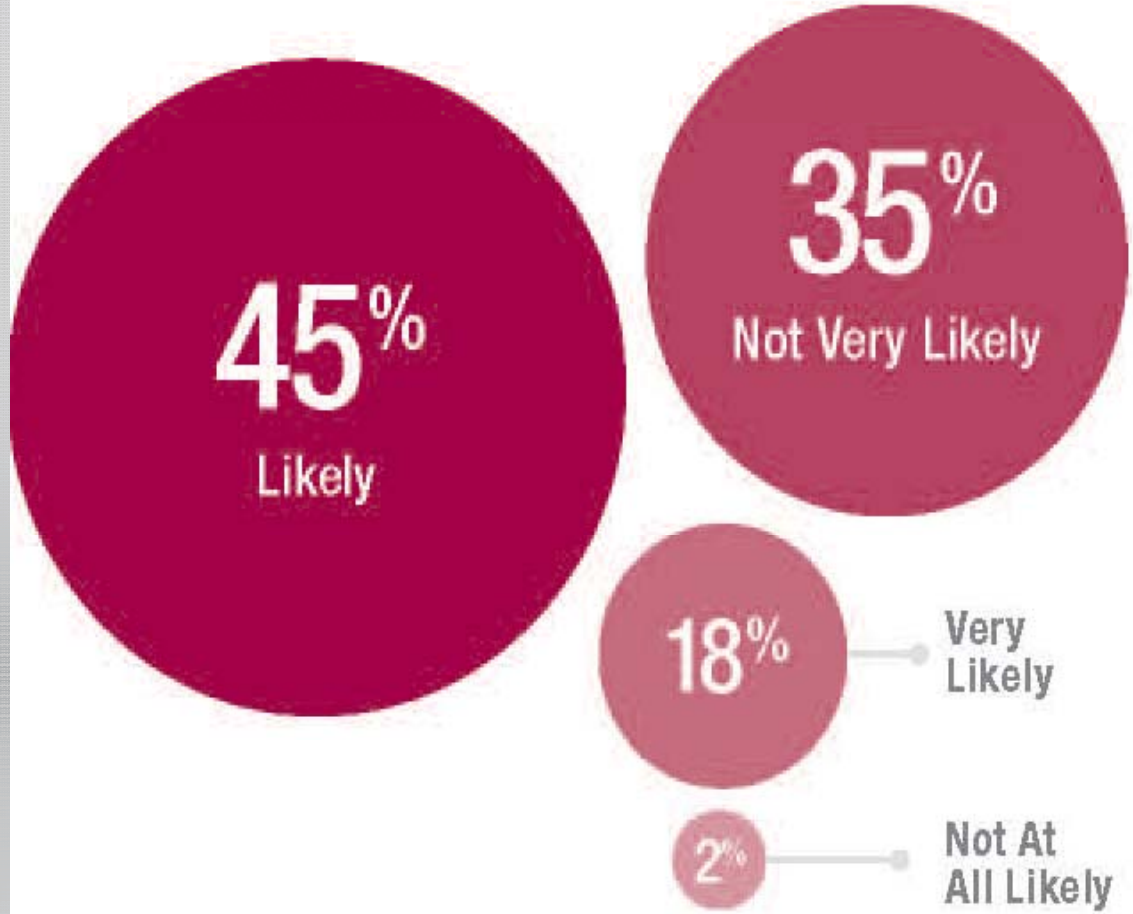


FIGURE 08 Correlation Between Likelihood of and Preparedness for an APT Attack

CORRELATION BETWEEN LIKELIHOOD OF AND PREPAREDNESS FOR AN APT ATTACK.

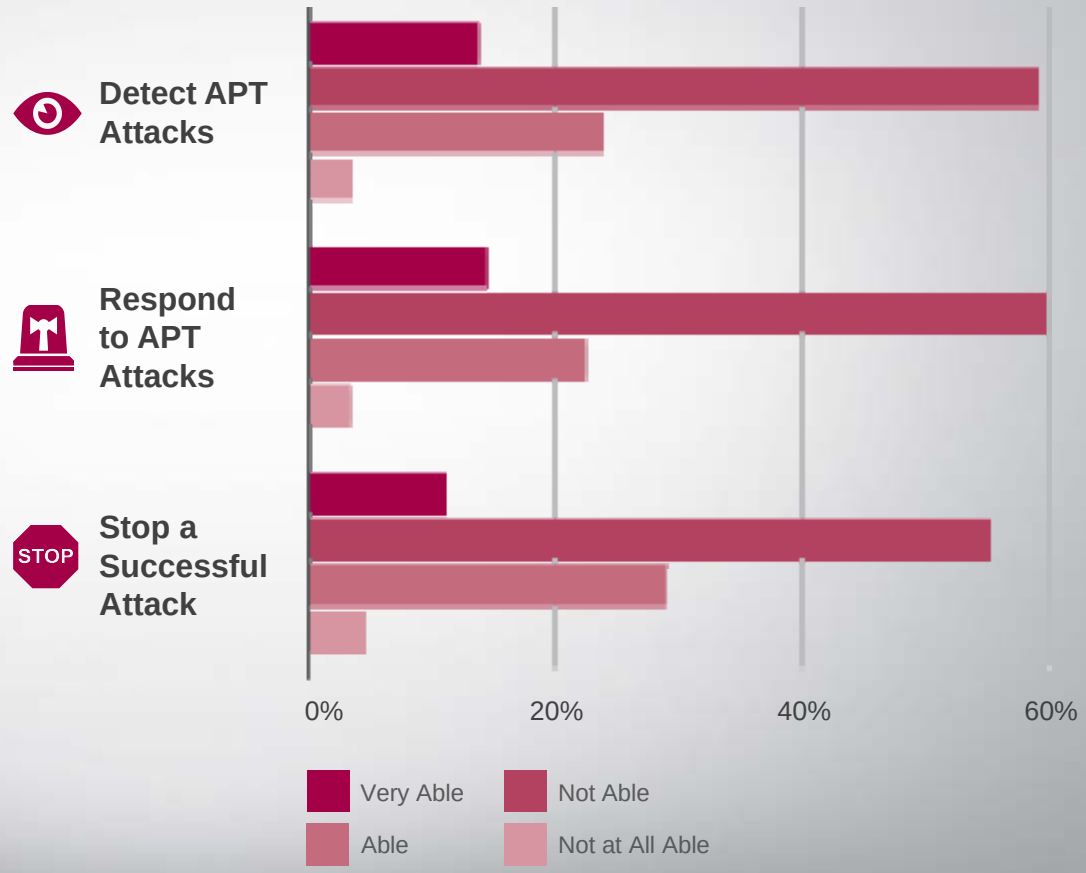
	How likely do you feel that your organization will be the target of an APT?			
	Very Likely	Likely	Not Very Likely	Not at all Likely
Very prepared We have a documented and tested plan in place for APT	31.1% (69)	14% (90)	4.8% (21)	23.1% (6)
Prepared But incident management does not specifically cover 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)

The majority of survey takers – up to **60%** – believed that they have the ability to ID, respond to and stop a successful APT attack.

31.1% said they have incident management plans in place to fight an APT.

49.5% are prepared, but without a concrete solution.

How able is your enterprise to deal with an APT attack?



How are people handling the threats?

Most respondents are using technology in a risk based layered approach to prevent and combat APTs.

94.9% **Anti-Virus / Anti-Malware**

92.8% **Network Tech** (Firewalls, etc.)

71.2% **IPS**

FIGURE 09 Technical Controls Used to Protect Against APT Attacks

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

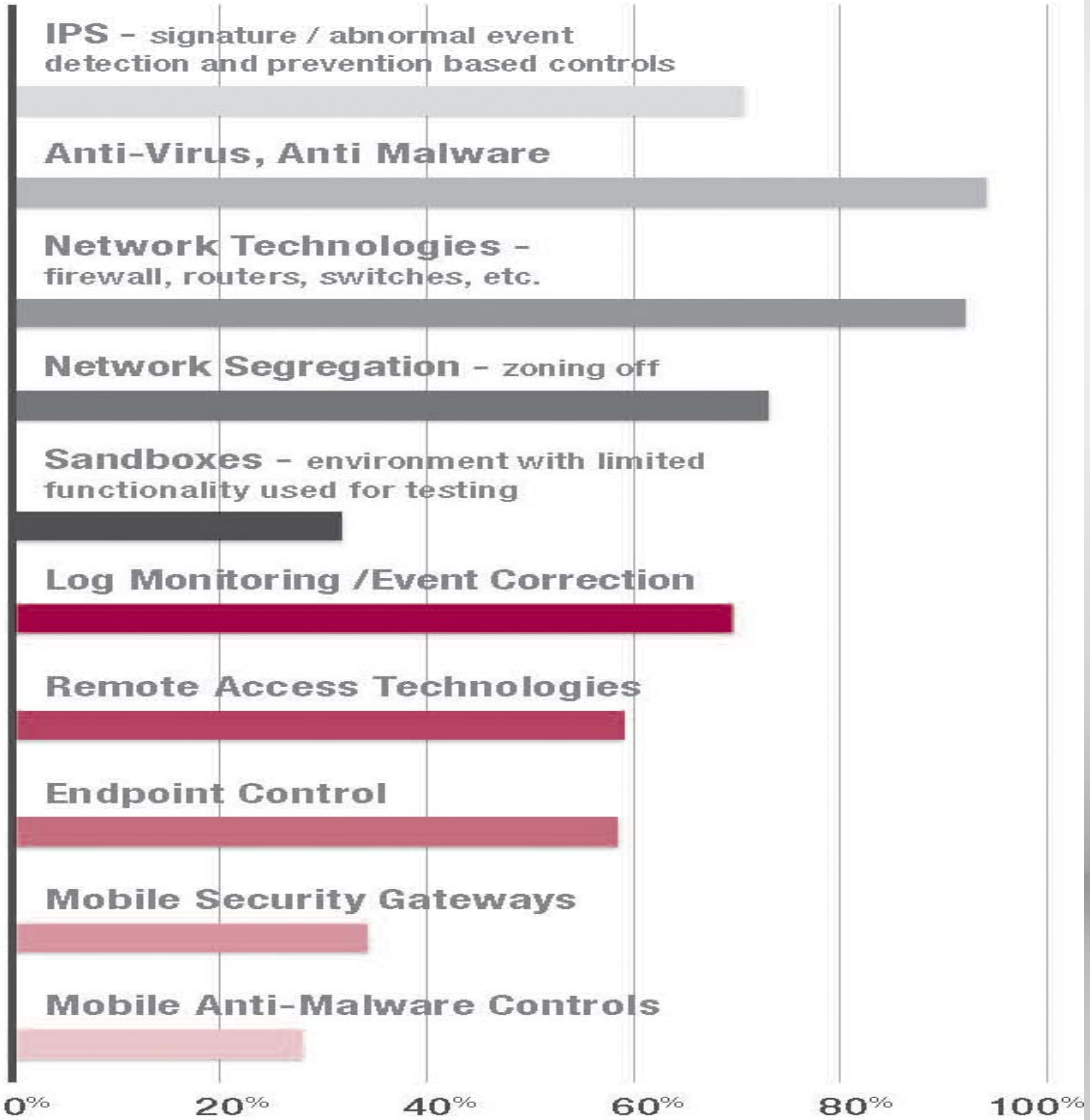


FIGURE 11 Correlation Between Familiarity With APTs and Update of Third-party Agreements

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

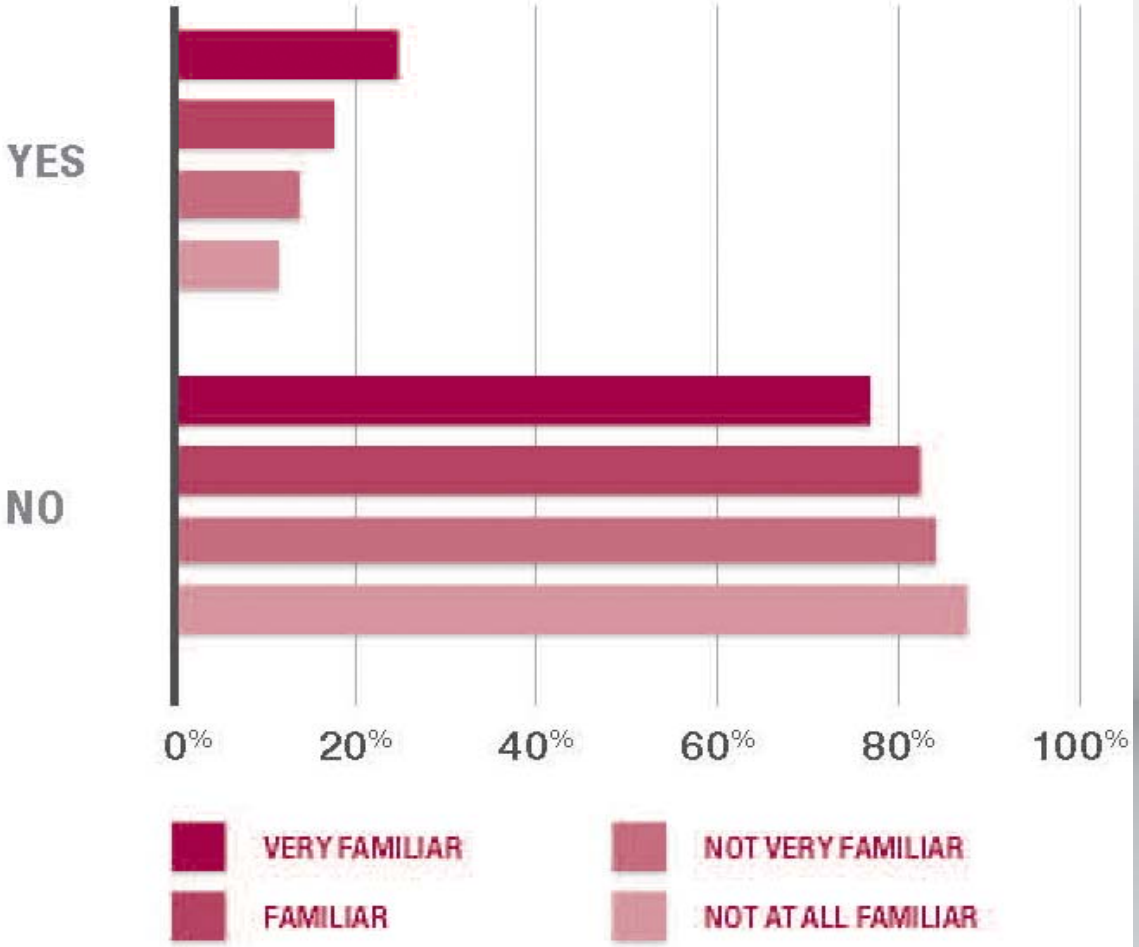


FIGURE 12 Correlation Between Likelihood of APT Attack and Executive Involvement

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

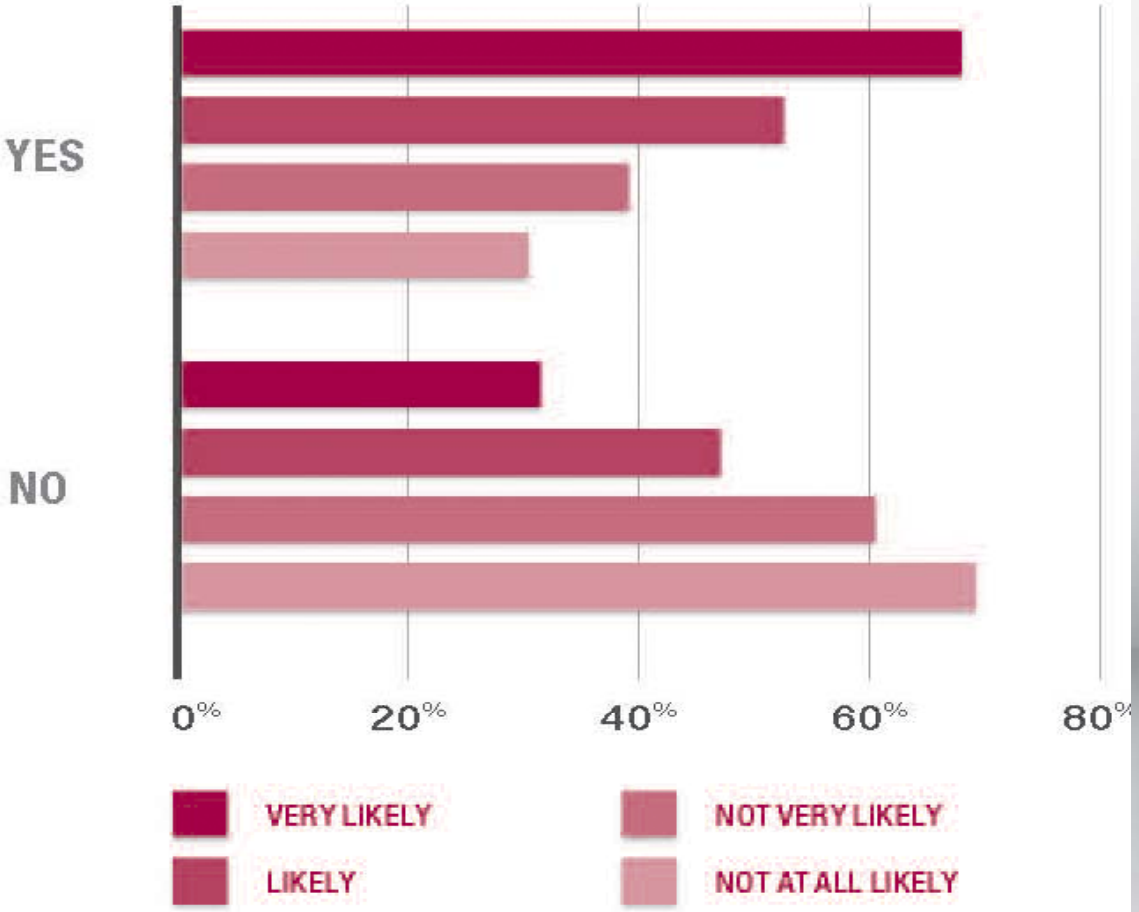


FIGURE 13 Correlation Between Likelihood of APT Attack and Executive Actions Taken

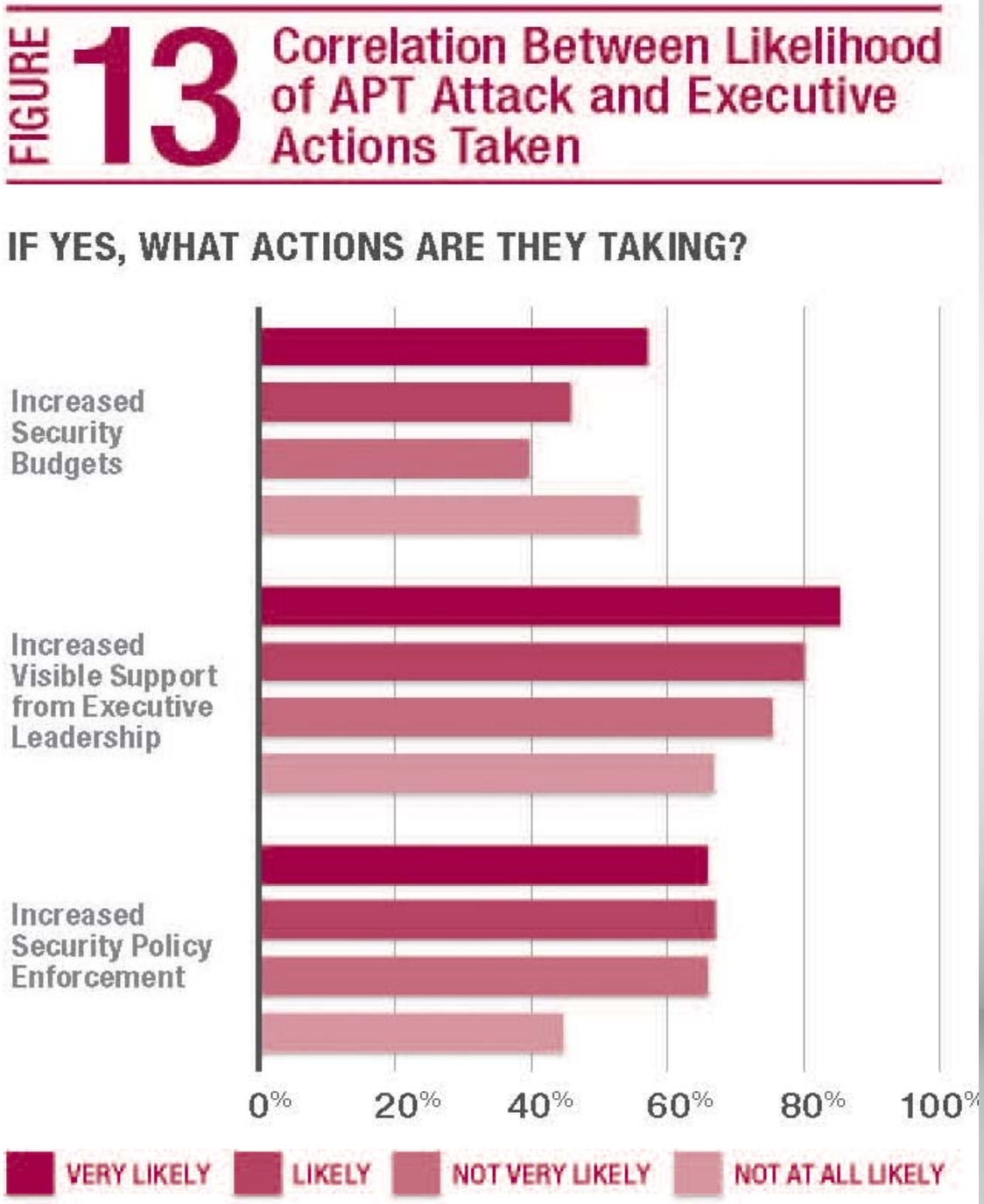


FIGURE 14 Adjustment of Incident Response Plans

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

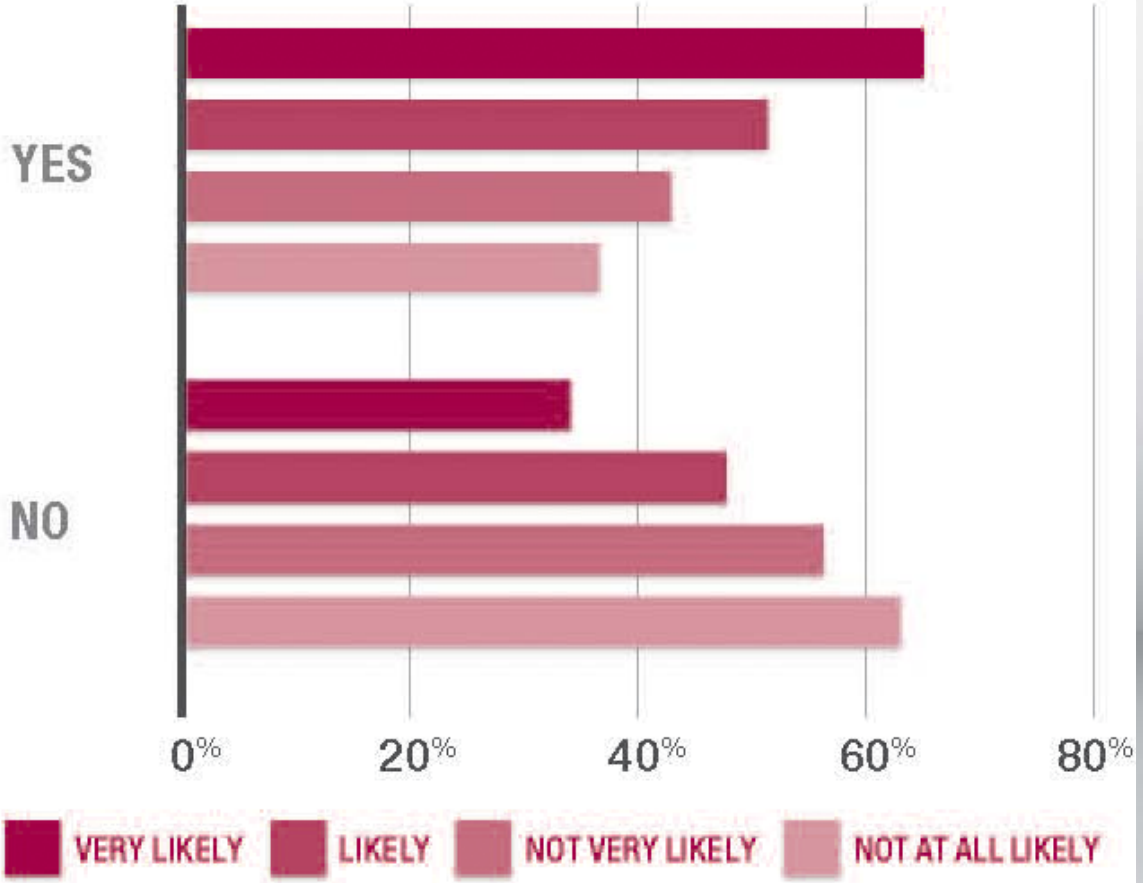


FIGURE 08 Correlation Between Likelihood of and Preparedness for an APT Attack

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)

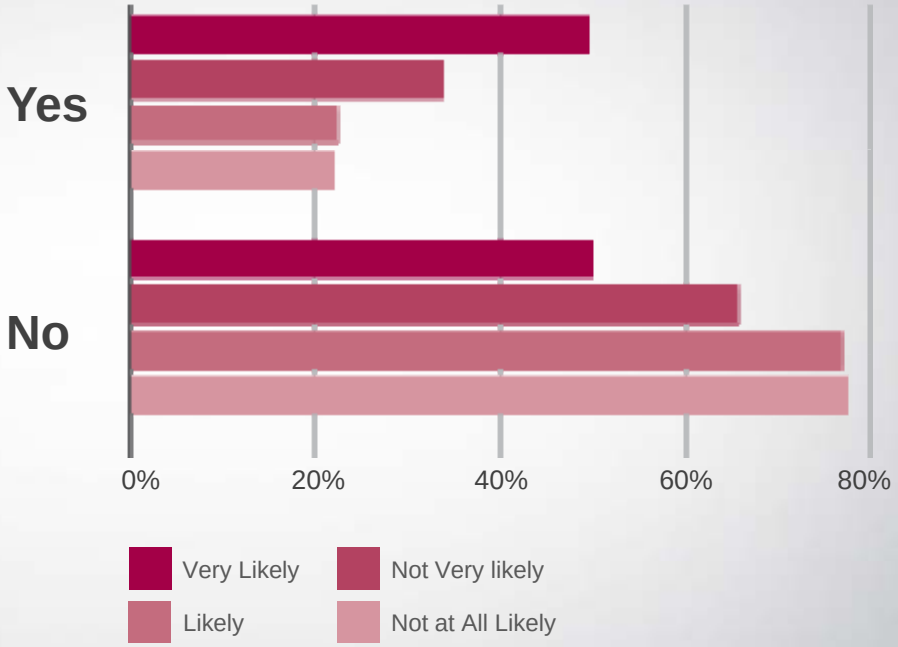
A Troubling Lack of Initiative

There aren't enough precautions being taken against the threat of an APT.

Up to **81.8%** of survey takers have not updated their agreements with vendors who provide protection against APT.

And **67.3%** reported that they haven't held any APT awareness training programs for their employees.

Has your enterprise increased security training as a result of APTs?



APTs are serious threats. We need more consideration to their consequences.

Enterprises must adopt more technology awareness training, vendor management, incident management and increased attention from executives.

Conclusion

Advanced Persistent Threats differ from the traditional, average virus, and need to be classified as such. Many enterprises and companies have made some positive inroads into fighting APTs, like better security management.

But there’s still a lack of cohesion and understanding to what APTs are and how to defend against them. Market conditions have not sufficiently changed, and the technology to fight APTs isn’t fully evolved yet.

But there’s still a lack of cohesion and understanding to what APTs are and how to defend against them.

Take Action Against APTs

ISACA is here to serve its members against any security breach – especially the Advanced Persistent Threat.

A series of educational products to address challenges in cyber security, and guard against APTs, is currently in development.

To learn more visit us at
WWW.ISACA.ORG/CYBERSECURITY

QUESTIONS & COMMENTS