Data Compromise Awareness

IANS Custom Report

February 2012

Contents

© 2012 IANS. All rights reserved. Commissioned by FireEye, Inc. For more information, write to ians@iansresearch.com.

Executive Summary

Over the last several years, the data breach landscape has evolved to include threat scenarios more advanced than any seen before. In many cases, advanced malware and exploits were involved, and many breached organizations did not realize they had been compromised until it was far too late. This is a huge and persistent problem, with some troubling trends that should concern everyone in information security - namely, with the techniques most organizations are employing, data breaches are still occurring at an alarming rate. Several examples of modern data breaches that involved advanced malware include:

- The DataLossDB chronicles hundreds of thousands of compromises involving malware in 2011 alone[1]
- In April and May of 2011 the Massachusetts Office of Labor and Workforce Development discovered a recurring Qakbot infection that exfiltrated 1200 or more employer records.[2] In addition, over 210,000 Massachusetts citizens' records were exposed with roughly 1500 systems infected.[3]
- The San Francisco PUC (Public Utilities Commission) had an infected server that exposed over 180,000 customer records.[4]
- The 2011 Verizon Data Breach Report indicated that 49% of breaches involved malware. In addition, three of the top five threat events recorded for breach data analysis incorporated malware as well.[5]

Most organizations feel that they have a sound defense-in-depth strategy to combat malware, and many teams dedicate staff or some operations time to malware analysis. However, based on all the data compromises happening, organizations have something to worry about in reality. With growing investor concern about the impact of cyber attacks on public companies' bottom lines, the Securities and Exchange Commission formally issued guidance[1] in October on the types of cyber attack data that should be disclosed, such as cyber events that could lead to financial losses. Data breach protection, especially for public companies is becoming increasingly important.[6]

Advanced malware is becoming more prevalent, but unfortunately most organizations are still using traditional host-based and network anti-malware tools to detect and combat it. Host and network intrusion prevention, next-generation application-aware firewalls, and honeypots are also in use, but not as frequently as other tools. The majority of solutions employed rely on signatures with some level of reputation analysis and behavior monitoring, which unfortunately are not as effective as companies would like to stop data compromises.

---

[1] http://datalossdb.org/search?breach_type[]=Virus&direction=desc&order=reported_date

[2] http://www.thetechherald.com/article.php/201120/7173/Qakbot-family-of-malware-blamed-for-data-breach

[3] http://www.boston.com/business/ticker/2011/05/virus_causes_da.html

[4] http://news.cnet.com/8301-27080_3-20068386-245/sf-utilities-agency-warns-of-potential-breach/

[5] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

[6] http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

© 2011 IANS. All rights reserved. Commissioned by FireEye, Inc. For more information, write to ians@iansresearch.com.

Most organizations do not believe they have been breached or that they have a current infection or compromise that involves advanced malware or targeted attacks. For those who have experienced known malware-related breaches, Web-based malware is the most common infection vector. While some organizations are looking at new tools and capabilities, only one-third of respondents are familiar with new vendors in these cutting-edge areas.

With the number of targeted attacks and advanced malware infections increasing, and data breaches becoming commonplace, many security teams will need to start looking at new technologies that can help them more effectively identify and prevent malware in the future.

© 2012 IANS. All rights reserved. Commissioned by FireEye, Inc. For more information, write to ians@iansresearch.com.

Current Security Posture and Tools in Use

The majority of large organizations currently employ a multi-layered security architecture with a variety of different network-based and host level controls. Unfortunately, this may lead many to a false sense of security, as most also believe they have not been compromised in any way! In figure 1, a fair percentage of organizations still hold the belief that attackers are capable of bypassing defenses, however. Roughly 80% of organizations employ a defense-in-depth security infrastructure, but others are at varying stages of maturity. Some acknowledge that they have gaps in their controls, but even most of these still believe they have not been compromised. This could be due to a lack of sufficient monitoring and detection capabilities, or possibly related to the advanced nature of much of today's sophisticated malware. Overall, the data suggests that over 50% of organizations know that they have gaps in security, and that attackers can potentially get in.

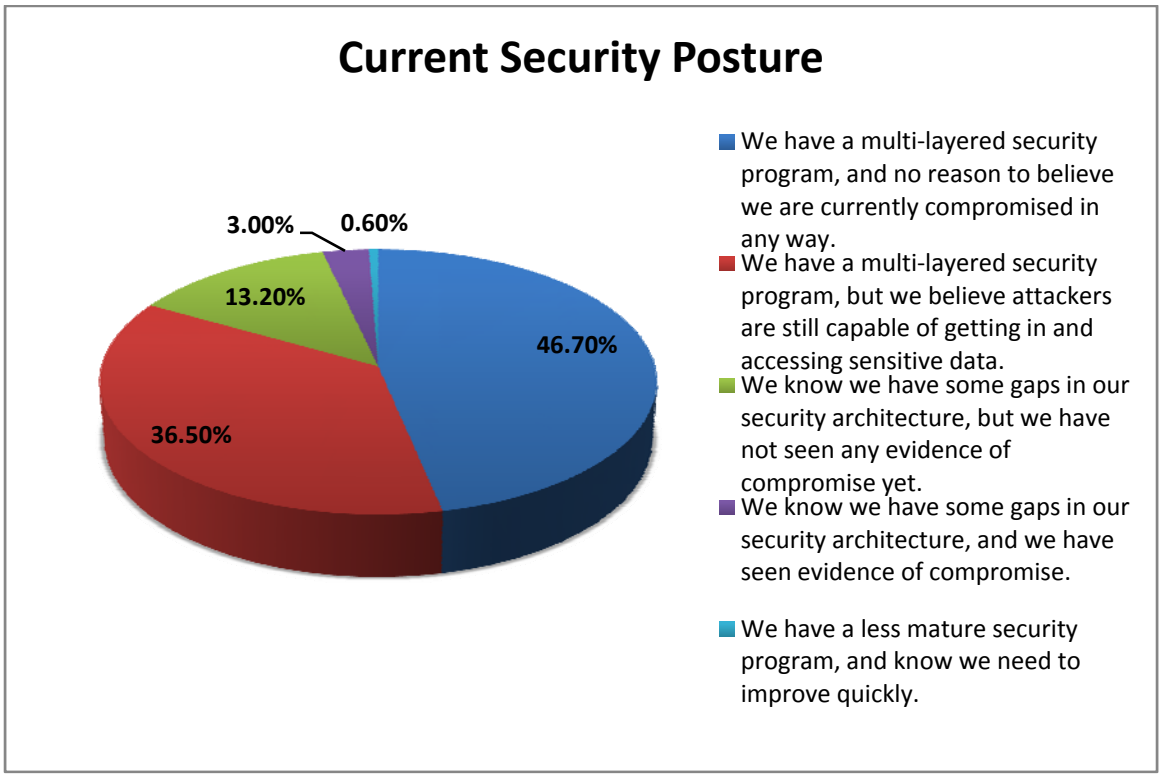

Figure 1 - Current security posture

© 2011 IANS. All rights reserved. Commissioned by FireEye, Inc. For more information, write to ians@iansresearch.com.

As organizations' security teams and controls mature, there is obviously a heightened awareness of the prevalence of malware. In figure 2, over 84% of companies have dedicated or partially dedicated malware analysts on the Information Security team. A smaller percentage of teams outsource to a security partner or managed services provider. Few organizations are lacking completely in malware analysis skills altogether, likely due to the need for human analysis and intervention given the complexity and prevalence of malware-based threats today:

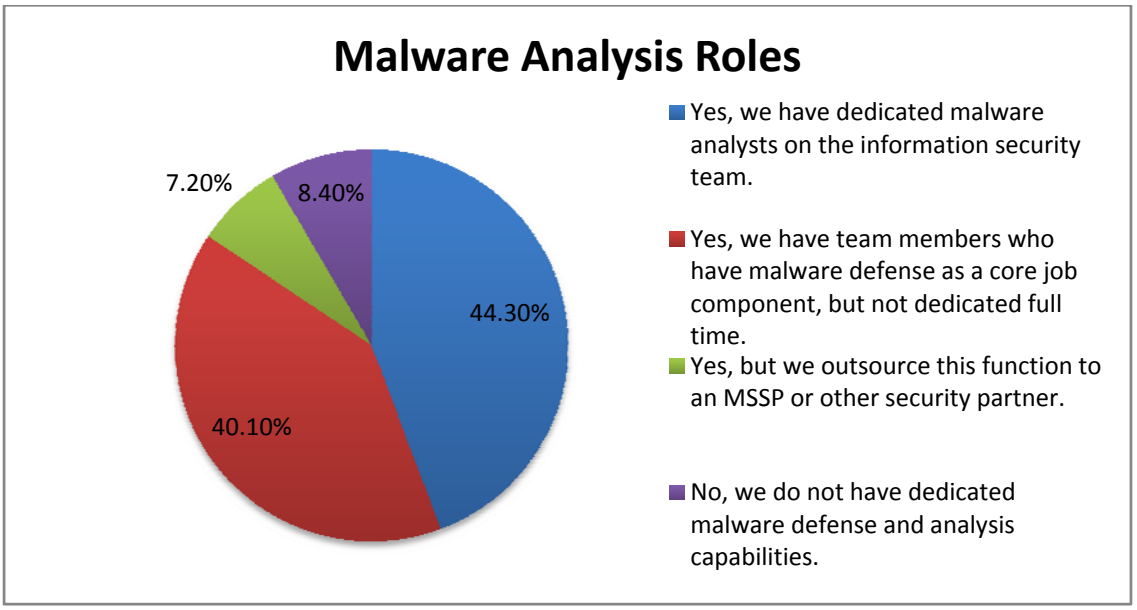

Figure 2 - Malware analysis roles

© 2012 IANS. All rights reserved. Commissioned by FireEye, Inc. For more information, write to ians@iansresearch.com.

From figure 3, most organizations are currently using a combination of network and host-based anti-malware products to combat viruses, worms, bots, and custom malware variants. Some are also making use of host-based and network-based IDS/IPS, as well as more progressive tools like next-generation firewalls and honeypots.

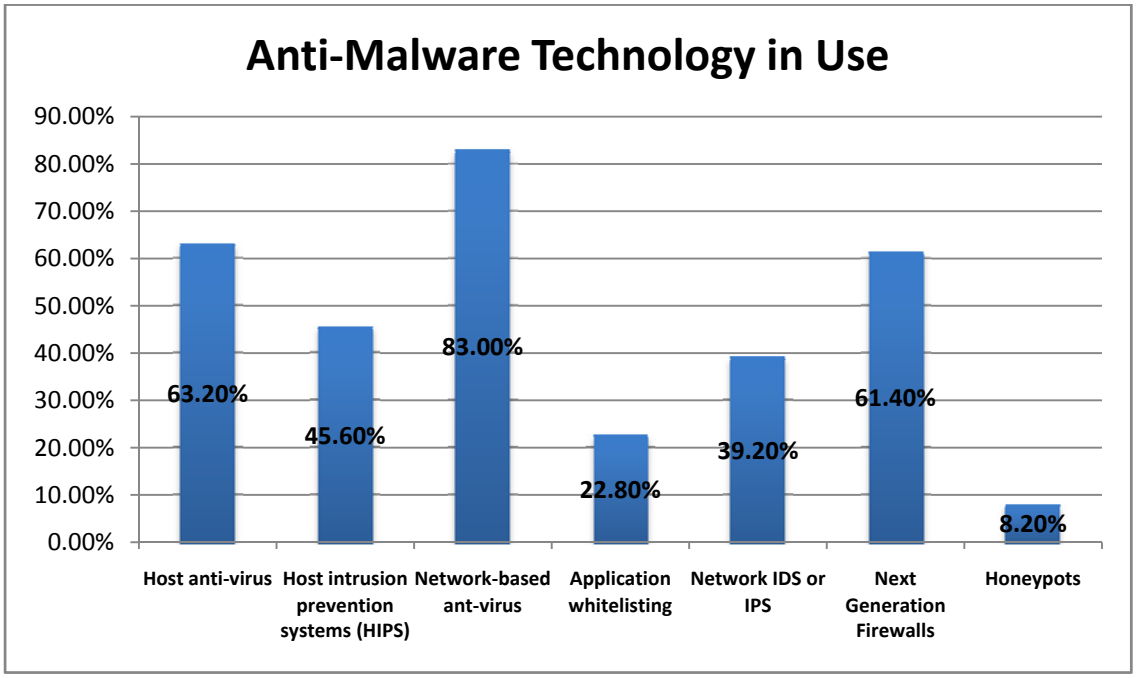

Figure 3 - Respondent Technologies in Use

© 2011 IANS. All rights reserved. Commissioned by FireEye, Inc. For more information, write to ians@iansresearch.com.

Attacks and Breaches

Most organizations today are concerned that they will be the specific targets of a sophisticated cyber attack (classified as one that is not wholly generic in nature and uses advanced methods and customized malware commonly associated with 'Advanced Persistent Threats,' or 'APTs'), with over 20% admitting attackers have already targeted them. Only a third of organizations are not concerned about targeted attacks in general. In all likelihood, most organizations are aware that these kinds of attacks can happen to anyone, but some may be more focused on different priorities currently. Along these same lines, **roughly 50% of organizations responding to the survey feel that they have been attacked using advanced malware**, with the other half not feeling as though they've experienced this particular threat to date.

For detected malware, most security teams only experienced a small number of variants likely stemming for signature-based technologies inability to detect dynamic threats. From figure 5, the vast majority of organizations identified fifty or fewer different types of malware in infections within the past year. A smaller percentage encountered up to 100 variants, and a minority saw over 100 different malware varieties in a single calendar year:

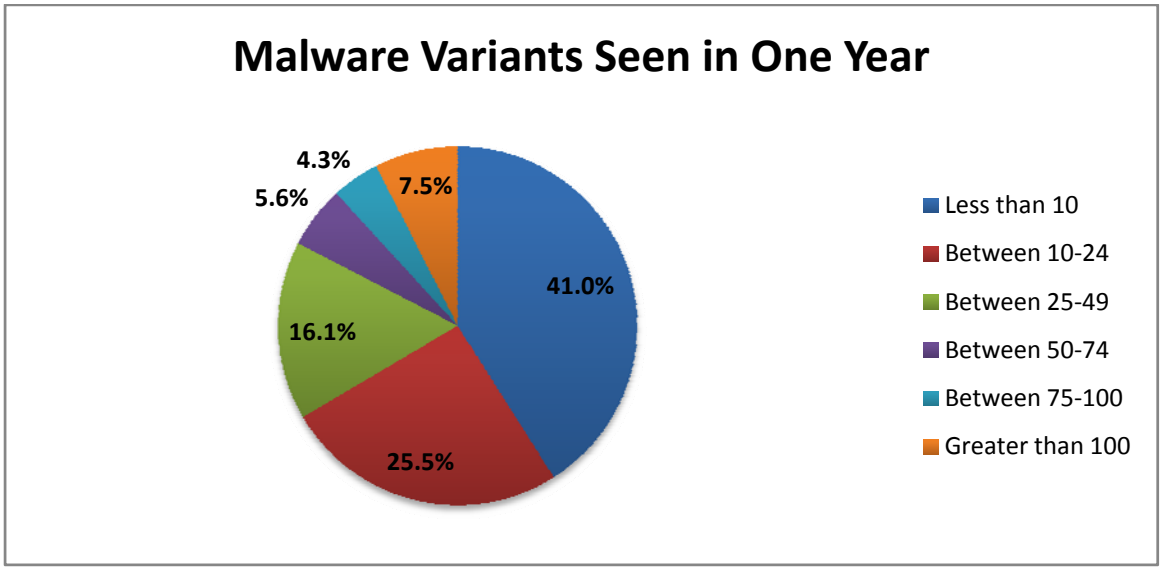

Figure 4 - Malware Variants Seen in One Year

Among respondents, approximately 35% stated that they had experienced a security incident in the last 24 months that successfully bypassed functional anti-malware controls. Forty-four percent stated malware had not bypassed controls, while another 21% were not sure if the incidents had bypassed malware detection and prevention capabilities. Among those who have experienced advanced attacks bypassing anti-malware controls, a number of attack vectors have been seen:

- **Web-based malware and "drive-by downloads"**: Web-based malware is one of the most prevalent attack vectors seen today. The Aurora attacks that compromised Google and other organizations in 2009-2010 leveraged Web-based exploits to drop malware onto systems, and malicious embedded advertisements (known as "malvertising") have been seen on well-known sites like the New York Times. Malicious iframes and embedded JavaScript are often known to drop malware onto systems as well.

© 2012 IANS. All rights reserved. Commissioned by FireEye, Inc. For more information, write to ians@iansresearch.com.

- **Social engineering**: Social engineering is often involved in the most insidious advanced attack scenarios. During the RSA breach that occurred in 2011, the initial attack vector was identified as a phishing email to RSA employees that included an attached Excel file with a zero-day Flash exploit.
- **Zero-day vulnerabilities/exploits**: Although not nearly as prevalent or detectable as typical malware or known attacks, 2010 and 2011 saw an uptick in incidents involving zero-day vulnerabilities as an avenue of exploit. The Stuxnet malware included multiple critical 0-day exploits, and the same attackers who compromised RSA were apparently unleashing similar zero-day attacks on multiple Fortune 500 companies prior to that breach.
- **Insider attack vectors**: Insider attacks can come in two primary forms, intentional and accidental. Employees who plug in an infected USB drive without understanding the potential repercussions may accidentally unleash malware to the organization. In select cases, employees may be disgruntled or inclined to commit fraud or data theft, perhaps leveraging malware to accomplish this.

The percentage of attack vectors by respondent is shown here:

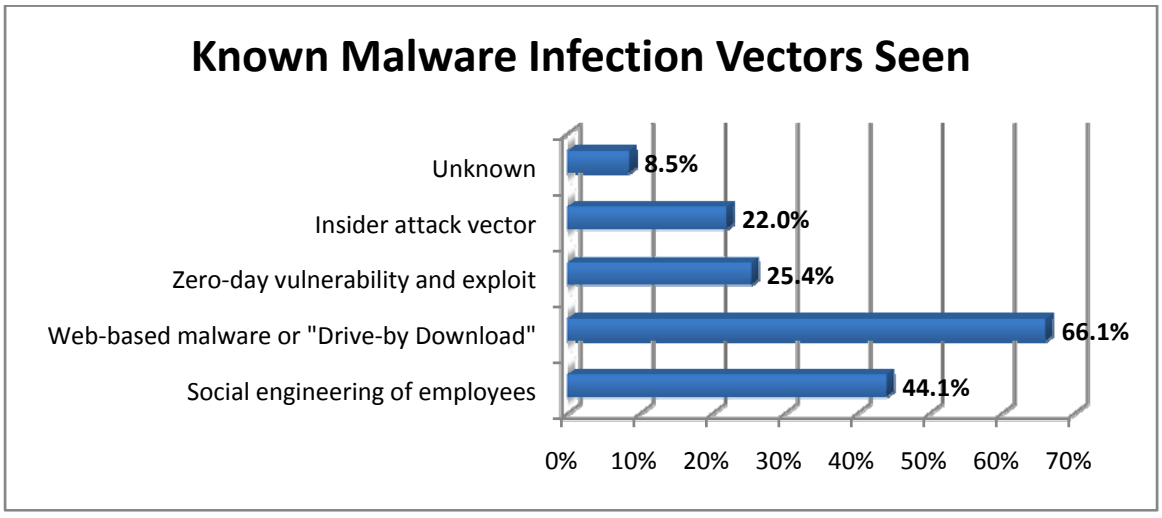

Figure 5–Known Malware Infection Vectors Seen

© 2011 IANS. All rights reserved. Commissioned by FireEye, Inc. For more information, write to ians@iansresearch.com.

Malware Defense Today and Tomorrow

Most organizations are still relying on antivirus vendors to develop tools for them. Some use network monitoring and reputation analysis while others treat all attachments and Web objects as suspicious and analyze them. Approximately a third of responding organizations are using some form of application whitelisting as well. A handful of organizations were not sure what tools were in place or used homegrown defenses.

Tools and Services Used	% of Organizations
We rely on our antivirus vendors to develop signatures and tools for defense.	59.1%
We use reputation analysis tools for network traffic.	51.2%
We rely on network IDS/IPS and firewalls to detect this.	48.2%
We treat all attachments and Web object as suspicious and analyze them for malicious behavior.	43.9%
We use application whitelisting tools for host-based security.	32.3%
Homegrown/Don't Know	3.0%

Table 1: Percentage of organizations using specific tools/services to combat malware

Forty percent of respondents felt that the tools listed in the above table are enough to detect and block any malware attack, while another 40% disagreed and are actively deploying next-generation security technologies. The remaining 20% are investigating options to defend against advanced malware and targeted APT attacks.

What kinds of attacks and malware are most organizations focusing on? Responding organizations prioritized the following list of threats, and the results are somewhat surprising (ranked from most critical to least critical areas of malware focus based on responses):

1. Web-based malware that exploits vulnerabilities in browsers and local clients
2. Traditional worms and viruses
3. Web-based malware that relies on social engineering, such as Fake AV
4. More sophisticated bots and "crimeware" kits like Zeus and SpyEye
5. General "information stealing" categories of malware
6. Zero-day exploits and malware that are tailored to our organization
7. Targeted social engineering attacks such as spear phishing
8. Traditional remote exploits that compromise server and application resources

© 2012 IANS. All rights reserved. Commissioned by FireEye, Inc. For more information, write to ians@iansresearch.com.

Given the prevalence of Web-based malware, it is not surprising to see it in the number one spot. Web-based malware that relies on social engineering is in the third spot, which also makes sense. However, more traditional social engineering that can be used to install malware is next to last! Given the high number of breaches involving social engineering, this seems unusual. In addition, traditional worms and viruses were the second priority, which is also unexpected given that they are fewer and farther between today.

© 2011 IANS. All rights reserved. Commissioned by FireEye, Inc. For more information, write to ians@iansresearch.com.

Survey Demographics and Information

Of 308 survey respondents, 209 in the United States and the rest in Europe, the representation of industries was fairly even across major sectors, with slightly higher numbers in the financial, manufacturing, government, and hi-tech fields. This graph depicts the industry breakdown:

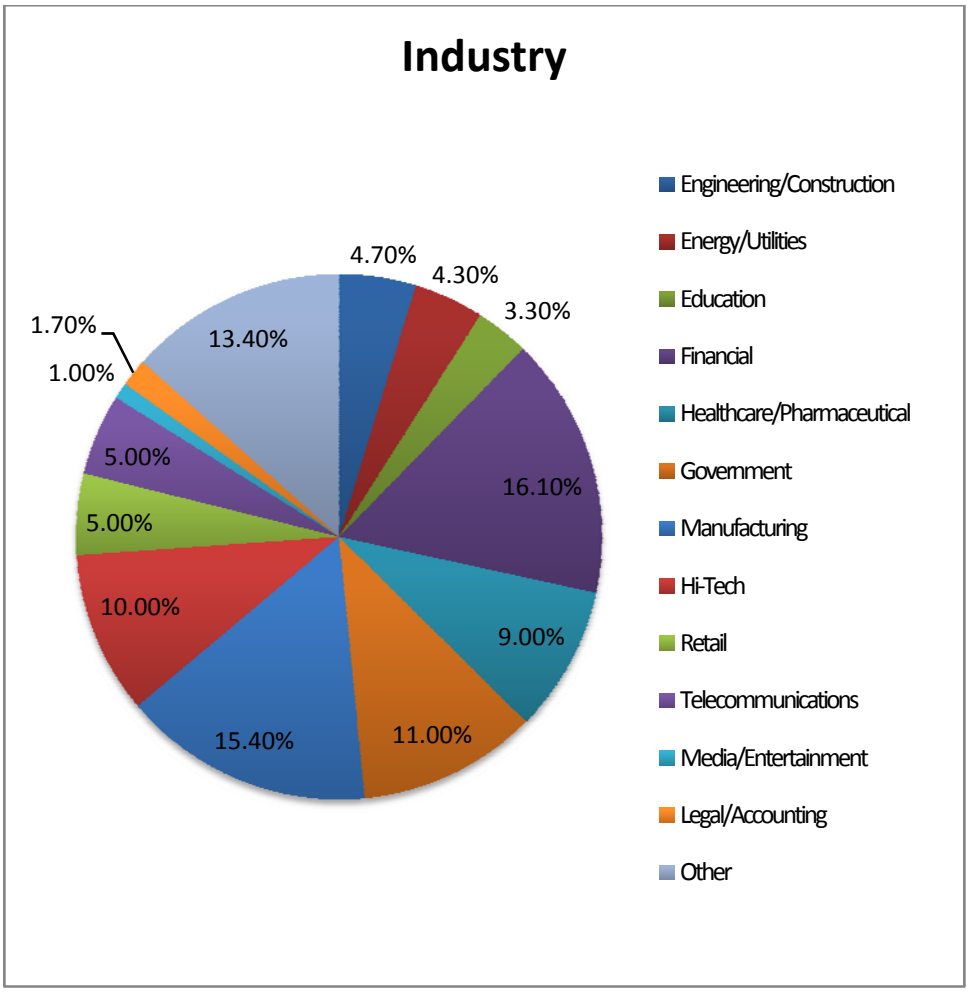

Figure 6–Participant Industry Representation

Most participants are involved directly in security strategy and decision making, with only 5.7% responding that they were “not very involved” or “not involved” in the process:

© 2012 IANS. All rights reserved. Commissioned by FireEye, Inc. For more information, write to ians@iansresearch.com.

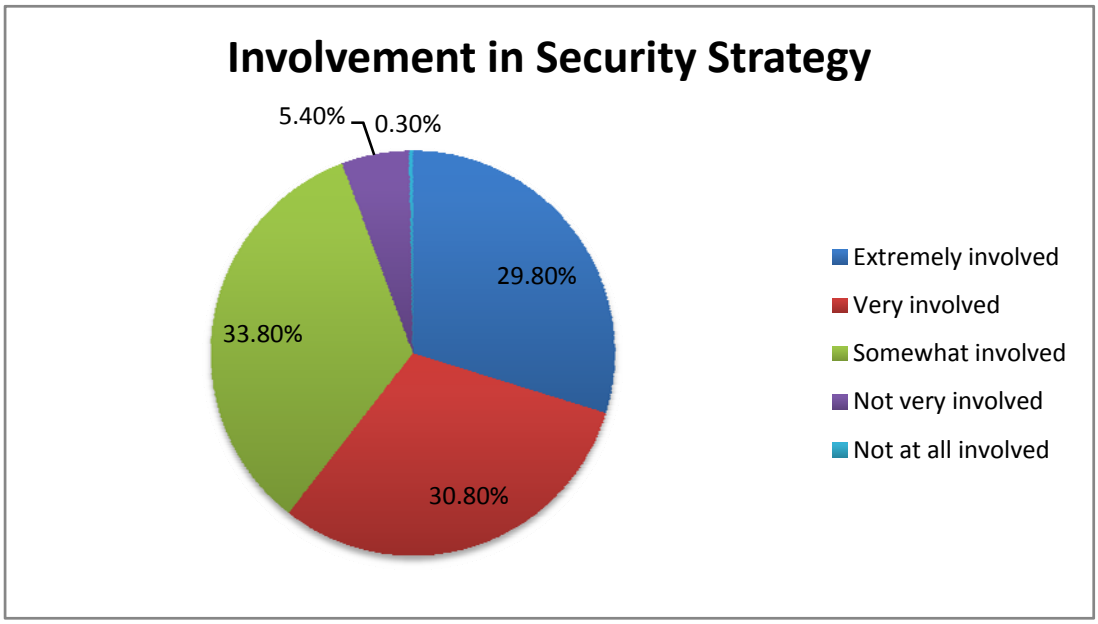

Figure 7–Participant Involvement in Security Strategy

Finally, most organizations responding were Fortune 500 large enterprises and multi-national organizations with more than 2000 employees:

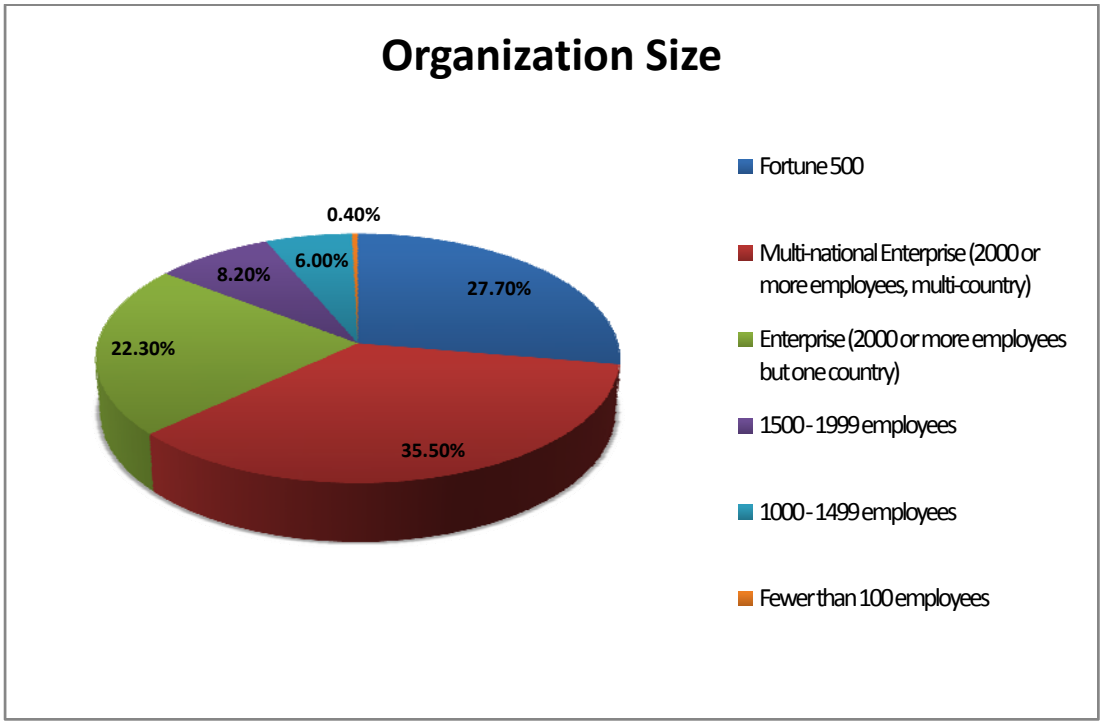

Figure 8 - Participant Organization Size

© 2011 IANS. All rights reserved. Commissioned by FireEye, Inc. For more information, write to ians@iansresearch.com.

About IANS

IANS is the leading provider of in-depth security insights delivered through its research, community, and consulting offerings. Fueled by interactions among IANS Faculty and end users, IANS provides actionable advice to information security, risk management, and compliance executives. IANS powers better and faster technical and managerial decisions through experience-driven advice.

IANS was founded in June 2001 as the Institute for Applied Network Security. Inspired by the Harvard Business School experience of interactive discussions driving collective insights, IANS adapted that format to fit the needs of information security professionals.

About FireEye

FireEye is the leading provider of next-generation threat protection focused on combating advanced malware, zero-day and targeted APT attacks. FireEye's solutions supplement security defenses such as traditional and next-generation firewalls, IPS, antivirus and Web gateways, which can't stop advanced malware. These technologies leave significant security holes in the majority of corporate networks. FireEye's Malware Protection Systems feature both inbound and outbound protection and a signature-less analysis engine that utilizes the most sophisticated virtual execution engine in the world to stop advanced threats that attack over Web and email. Our customers include enterprises and mid-sized companies across every industry as well as Federal agencies. Based in Milpitas, California, FireEye is backed by premier financial partners.

© 2012 IANS. All rights reserved. Commissioned by FireEye, Inc. For more information, write to ians@iansresearch.com.