Ponemon INSTITUTE

2014 State of Endpoint Risk

Sponsored by Lumension®

Independently conducted by Ponemon Institute LLC

Publication Date: December 2013

2014 State of Endpoint Risk

Ponemon Institute, December 2013

Part 1. Introduction

Just when many IT security practitioners were hoping to get their endpoint security risks under control, the exploding growth of mobility platforms and public cloud resources has turned these dreams into a security nightmare.

We surveyed 676 IT and IT security practitioners with involvement in endpoint security. Most of the participants in the study are involved in IT security, management and operations in their organizations.

According to these knowledgeable respondents, endpoint security risk is more difficult to manage than ever. The reason is the growing number of employees and other insiders using multiple mobile devices in the workplace followed by the increase in personal devices connected to the network and the growing popularity of public cloud services such as Dropbox.

Sponsored by Lumension Corporation, we are pleased to present the findings of the *2014 State of Endpoint Risk*. The study focuses on how organizations are addressing the IT endpoint risk and where the greatest vulnerabilities exist. In this report we will compare the findings to the study conducted in 2012.

Some of the most important findings from this study include the following:

- **Endpoint security risk is more difficult than ever to manage.** Seventy-one percent of respondents say the security threats created by vulnerabilities to the endpoint have become more difficult to stop or mitigate.
- **In the IT environment, mobility and third party applications are the greatest security risks**. Seventy-five percent of respondents say mobile devices such as smart phones represent the greatest risk of potential IT security risk within the IT environment.
- **The frequency of malware incidents increases.** Forty-four percent of respondents report a major increase in the number of malware incidents targeting their endpoints. General malware and web-borne malware attacks are the most frequent types of incidents or compromises to IT networks.
- **Mobile endpoints are vulnerable to malware attacks.** Sixty-eight percent of respondents say their mobile endpoints have been the target of malware in the last 12 months.
- **APTs are attacking endpoints.** Forty percent of respondents say their endpoints have been the entry point for an APT/targeted attack in the past 12 months.
- **Most organizations make endpoint security a priority but budgets lag behind**. In the past 24 months, more respondents say endpoint security is a priority in their organization's overall IT security strategy (65 percent of respondents). However, only 29 percent of respondents say spending has either significantly increased or increased for endpoint security during that time.
- **Malware incidents are straining IT security budgets**. Fifty percent of respondents say their organization's IT operating expenses are increasing and this is an increase from 46 percent of respondents in 2012. Sixty-seven percent say malware incidents contribute a very significant or significant increase in these expenses and this is up slightly from 64 percent in 2012.

▪ Part 2. Key Findings

In this section, we present an analysis of the major findings of the study. The complete audited results are presented in the appendix of this report. We organized the report according to the following topics:

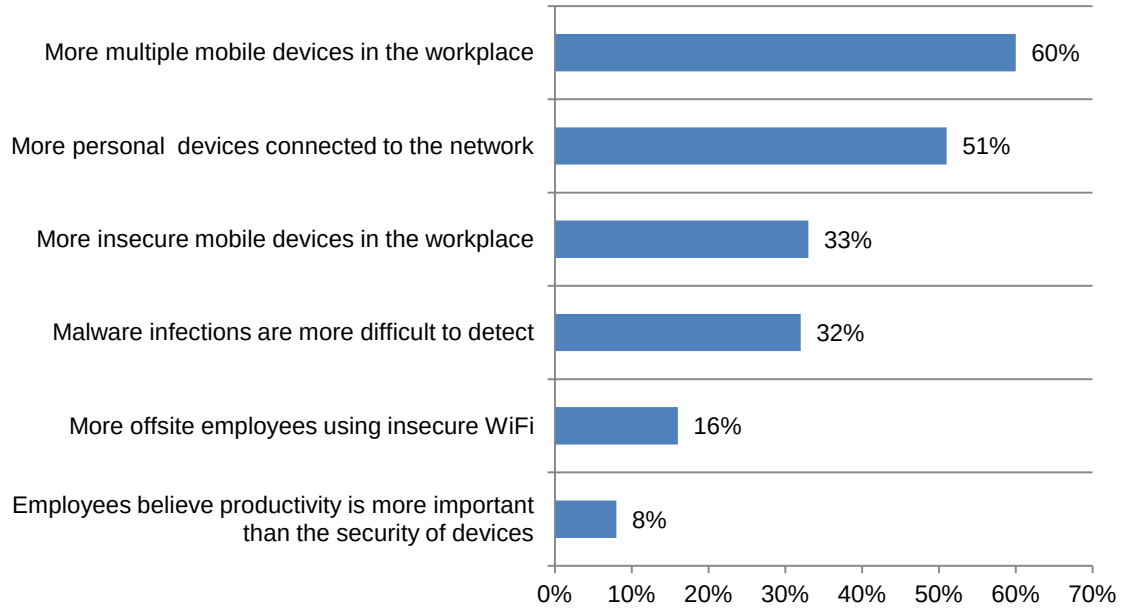
- The endpoint threat landscape
- Malware and APT attacks against the endpoint
- Budgets and spending to reduce endpoint risk

The endpoint threat landscape

Endpoint security risk is more difficult than ever to manage. Seventy-one percent of respondents say in the past 24 months the security threats created by vulnerabilities to the endpoint have become more difficult to stop or mitigate.

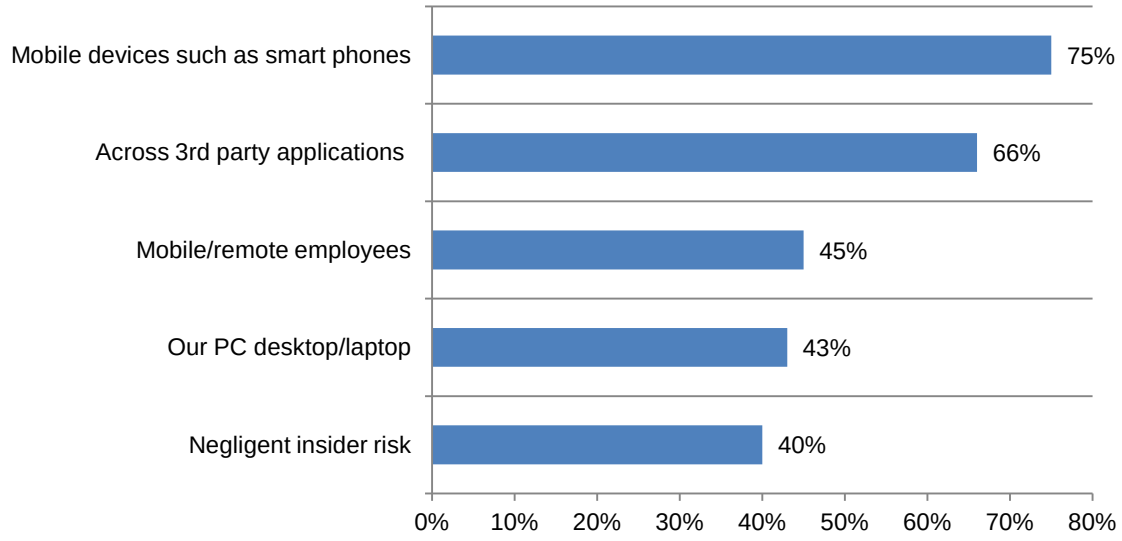
According to 60 percent of these respondents, the biggest threat is the growing number of employees and others using multiple mobile devices in the workplace followed by the increase in personal devices being connected to the network, as shown in Figure 1.

Figure 1. What are the biggest threats to endpoint security?
Two responses permitted



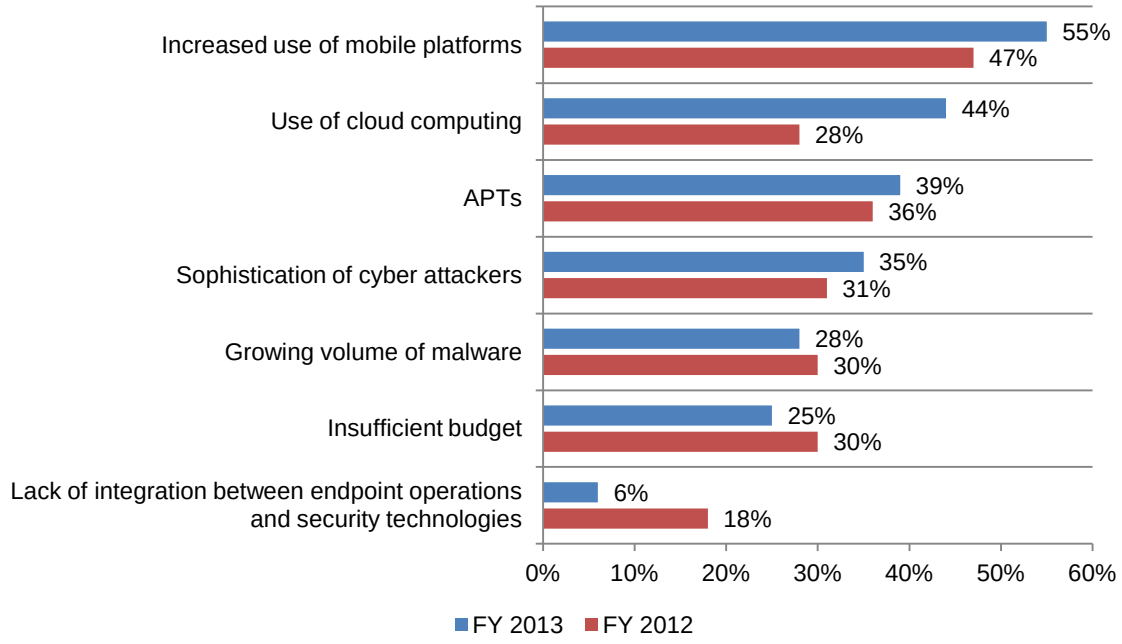
In the IT environment, mobility and third party applications are the greatest security risks. According to Figure 2, 75 percent of respondents say mobile devices such as smart phones represent the greatest risk of potential IT security risk within the IT environment. This is followed by the increase in the risk of third party applications.

Figure 2. Greatest IT Security Risks



The greatest risks to the organization are increased mobility and public cloud computing services. Figure 3 shows interesting trends from last year in what respondents think are the greatest security risks to the organization. Since the 2012 study was conducted, the percentage of respondents who identified the use of cloud computing resources as a major concern has increased from 28 percent to 44 percent. Fifty-five say the increased use of mobile platforms is a threat to the organization, up from 47 percent last year.

Figure 3. IT security risks of greatest concern to the organization
Three choices permitted

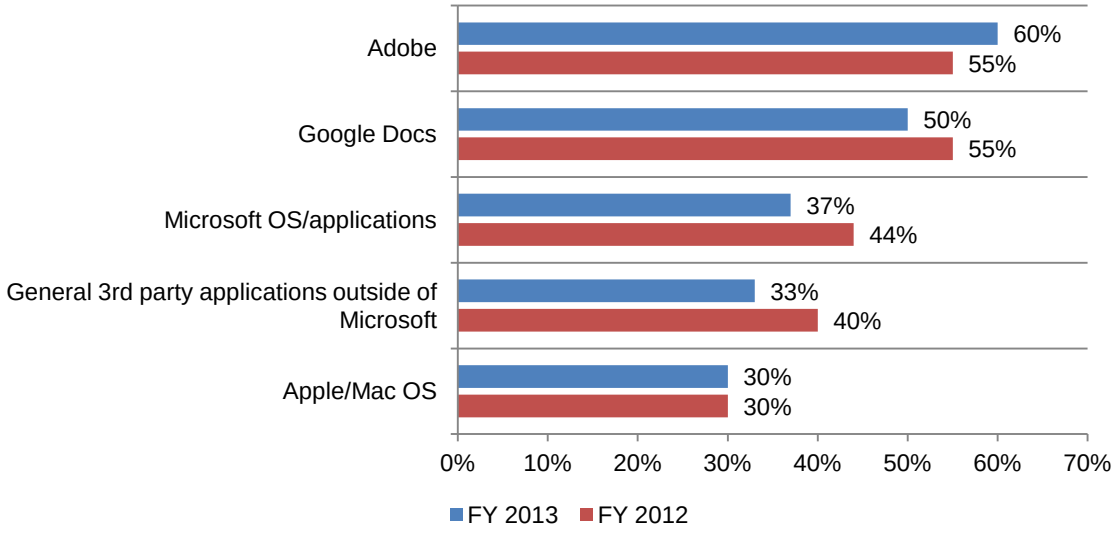


Dealing with the risks of third-party cloud services. According to respondents, the biggest increase in technologies that support employee productivity will be the use of third-party cloud computing resources. To manage this risk, 54 percent say their organization has a centralized cloud security policy, an increase from 40 percent in 2012. Fifty-five percent say their organizations enforce employees' use of private clouds, up from 41 percent in last year's study.

Certain applications increase an organization's IT risk. Applications considered to increase vulnerabilities and IT risk are similar to last year's study, as shown in Figure 4. These are: Adobe, Google Docs and Microsoft OS/applications. Of least concern are WinZip and Mozilla Firefox (not shown).

Seventy-four percent of respondents say their organizations are planning to pilot or expand their usage of application control/whitelisting technologies within the endpoint environment sometime within the next year.

Figure 4. Applications with the greatest IT risk
Top five choices

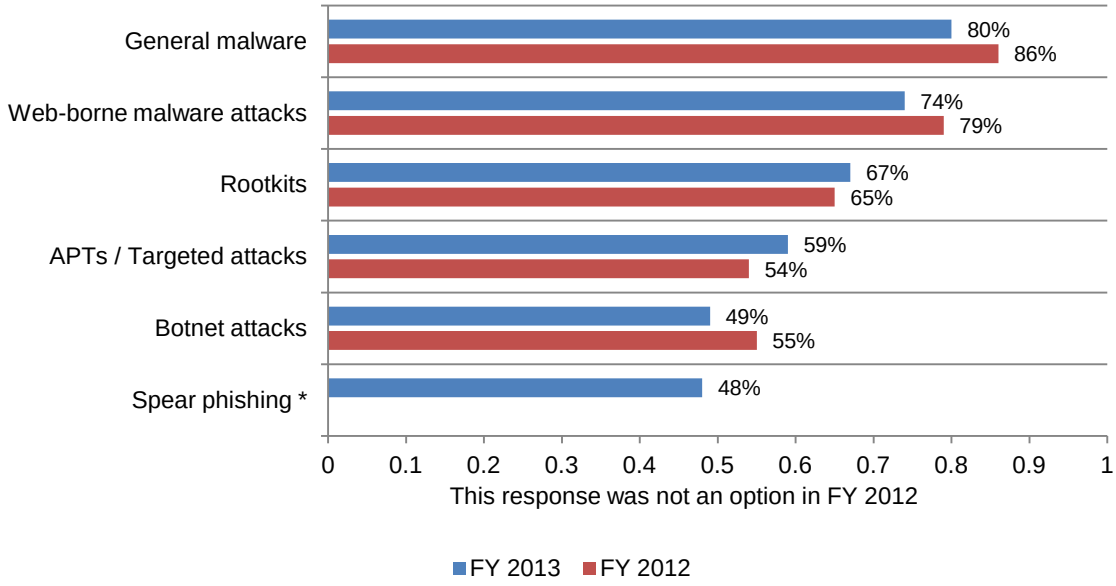


Malware and APT attacks against the endpoint are frequent

The frequency of malware incidents increases. Forty-four percent of respondents report a major increase in the number of malware incidents targeting their endpoints. This is greater than the 37 percent of respondents who reported a major increase in the 2012 study. On average, organizations report 50 malware attempts or incidents each month. This is up slightly from a monthly average of 47 such incidents.

Figure 5 shows the most frequent types of incidents or compromises in the organization's IT networks. General malware and web-borne malware attacks are the most frequent types of incidents or compromises to IT networks. For the first time, we included spear phishing in the list of incidents or compromises and 48 percent of respondents say this type of compromise is occurring frequently.

Figure 5. The most frequent types of malware incidents
More than one response permitted

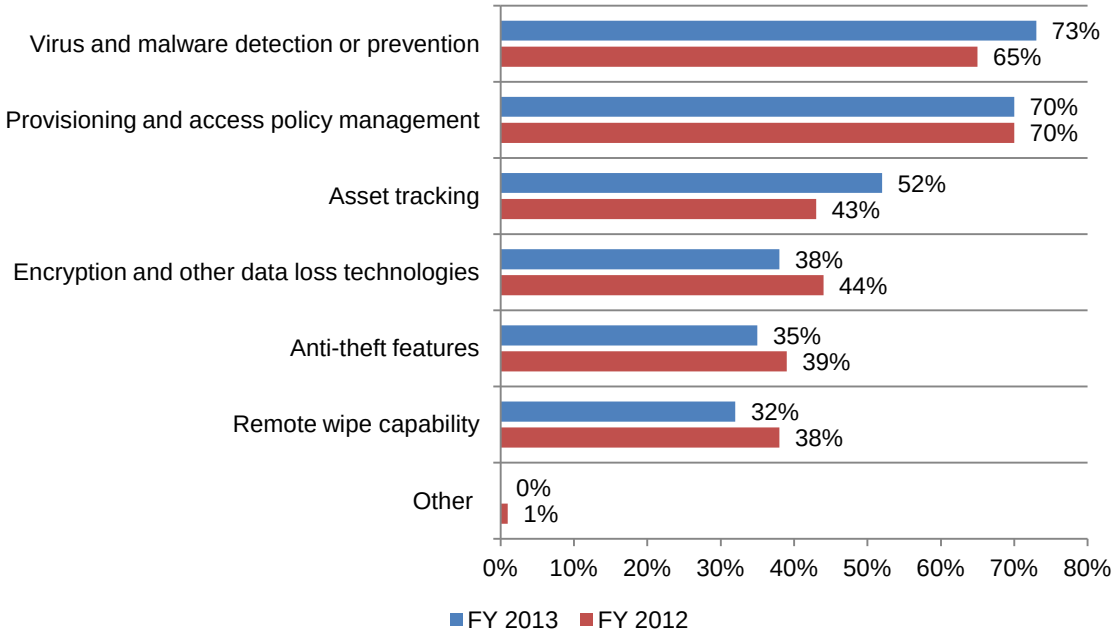


Mobile endpoints are vulnerable to malware attacks. Sixty-eight percent of respondents say their mobile endpoints have been the target of malware in the last 12 months.

The difficulty in minimizing the risk is the increasing use of mobile devices, smart phones and tablets. An average of 63 percent of an organization's employees are using mobile devices. Further, the average number of mobile devices that have to be actively managed in the workplace will increase from about 5,000 to 7,000 in the next three years.

As shown in Figure 6, the most important capabilities for mobile device management (MDM) are virus and malware detection or prevention, provisioning and access policy management and asset tracking. Since last year, there has been an increase in respondents who view virus and malware detection and asset tracking as important. Decreasing in importance is encryption and other data loss technologies and remote wipe capability.

Figure 6. What are the most important MDM features?
Three choices permitted

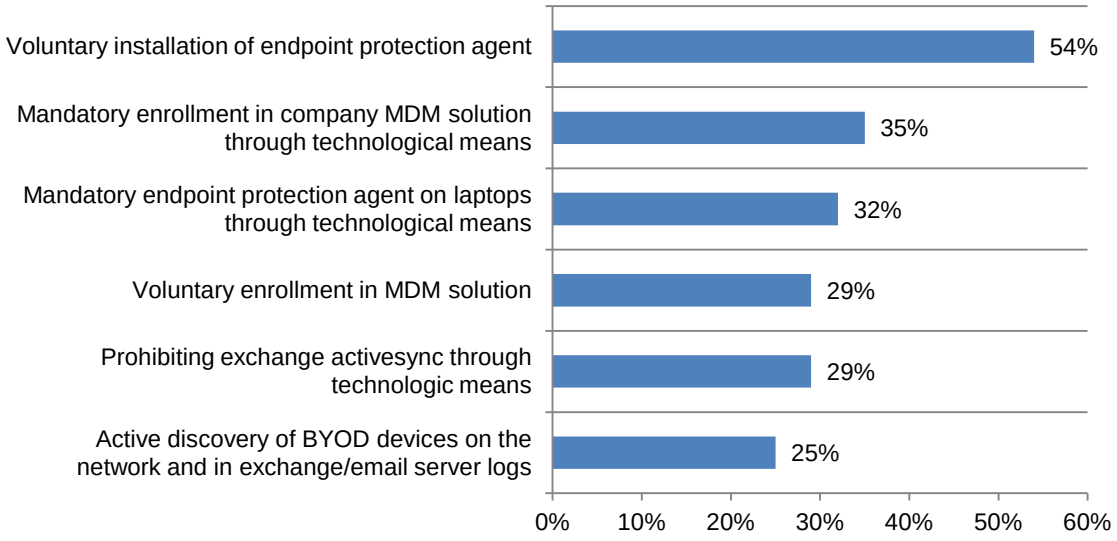


When asked what plans their organizations have to secure employee-owned devices, 43 percent say the plan is to use security technologies already in place for mobile corporate devices. Eleven percent of respondents say they have stricter security standards for BYOD than for corporate-owned devices.

Figure 7 reveals the steps being taken by the 54 percent of respondents who say their organizations have a BYOD security plan. The majority of respondents say they are relying on voluntarily installing the endpoint protection agent (54 percent).

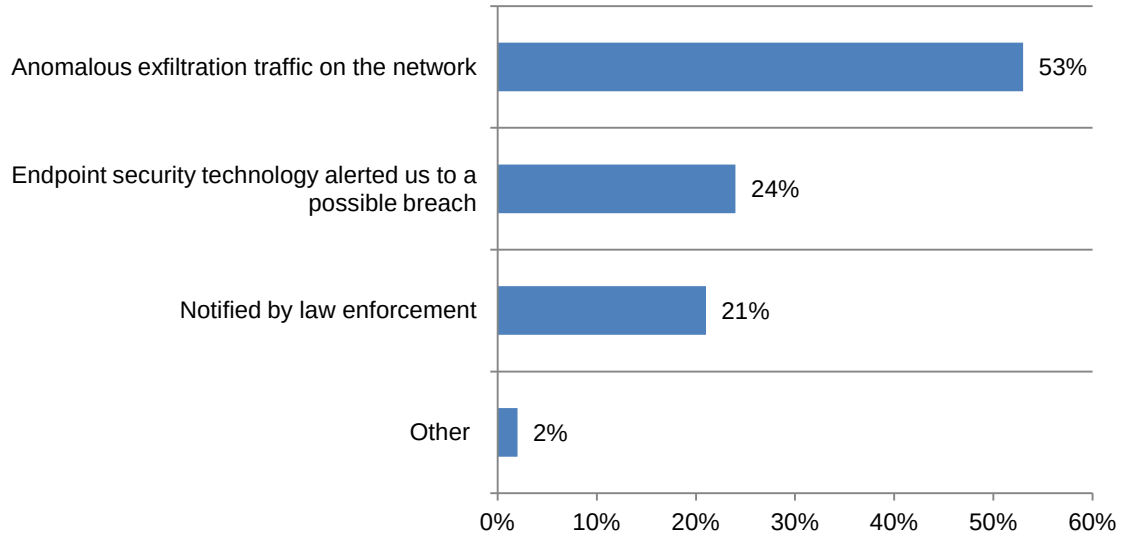
To a lesser extent other steps include: mandatory enrollment in company MDM solutions through technological means (35 percent) and mandatory endpoint protection agent on laptops through technological means (32 percent). Least used is the active discovery of BYOD devices on the network and in exchange/email server logs.

Figure 7. Steps to make BYOD more secure
More than one response permitted



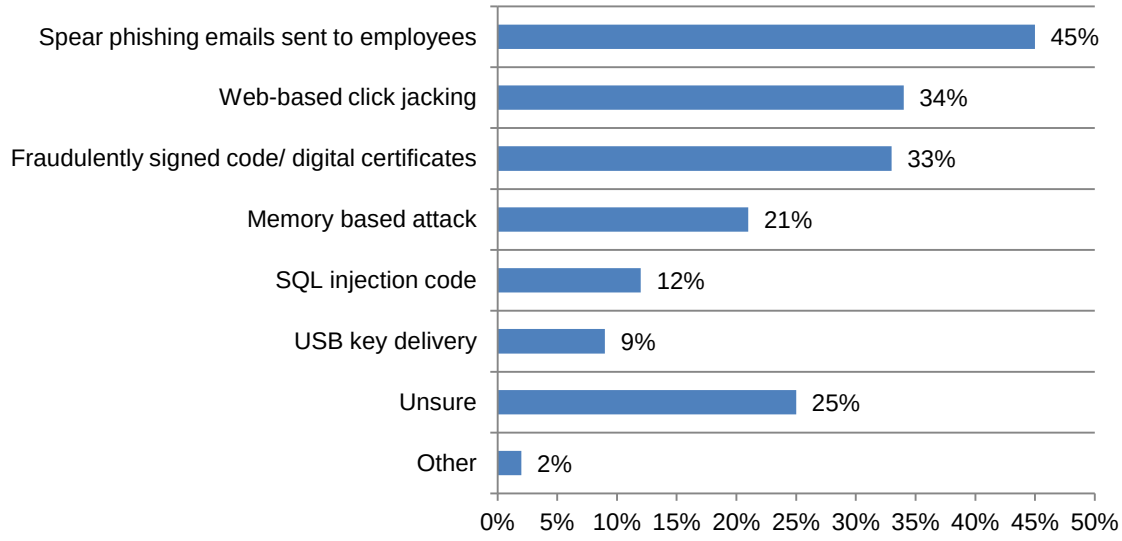
APTs are attacking endpoints. Forty percent of respondents say their endpoints have been the entry point for an APT/targeted attack in the past 12 months. Figure 8 reveals how respondents learned about the attack. The majority of respondents (53 percent) say they learned of the APT when they found anomalous exfiltration traffic on the network. Twenty-four percent say their endpoint security technology alerted them to a possible breach.

Figure 8. How did the organization learn about the APT attack?



As discussed, 48 percent of respondents say their organizations are experiencing more spear phishing incidents. Figure 9 shows that a similar percentage of respondents (45 percent) say spear phishing emails sent to employees are how the APT/targeted attack started. This is followed by APTs initiated by web-based click jacking (34 percent) and fraudulently signed code/digital certificates (33 percent).

Figure 9. How did the APT attack start?
More than one response permitted

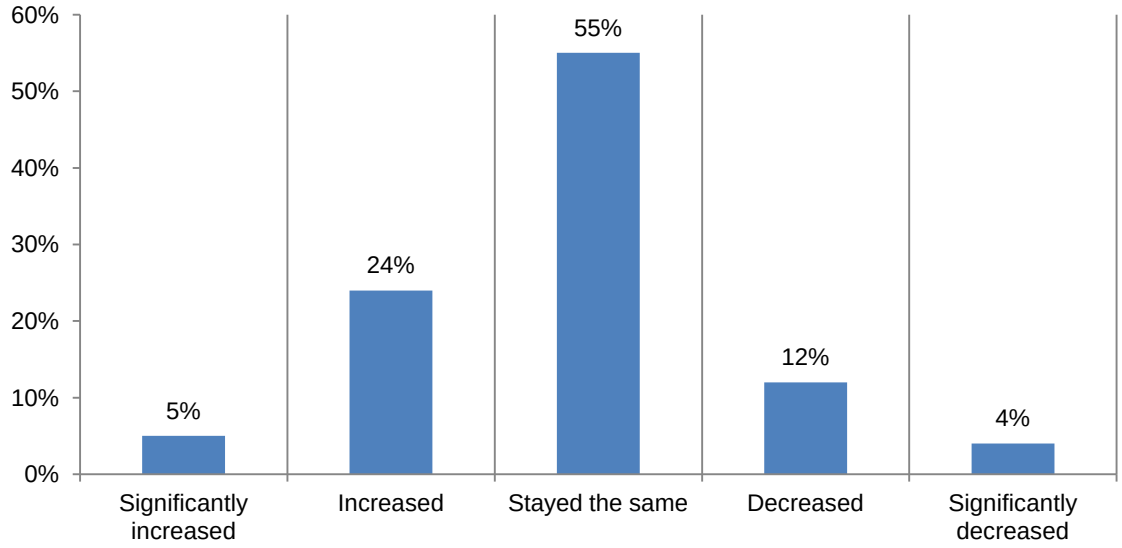


Investments in technology to manage endpoint risk

Most organizations make endpoint security a priority but budgets lag behind. In the past 24 months, more respondents say endpoint security is a priority in their organization's overall IT security strategy (65 percent of respondents).

However, only 29 percent of respondents say spending either significantly increased or increased for endpoint security in the last 24 months, as shown in Figure 10. Fifty-five percent of respondents say budgets stayed the same.

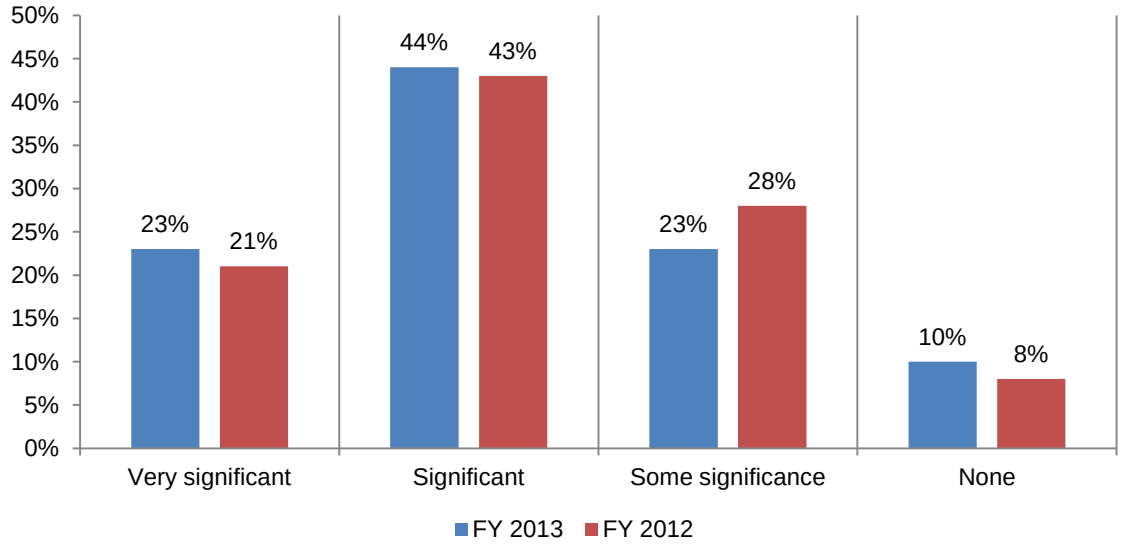
Figure 10. Will the budget for endpoint security change?



What are the Budget predictions for 2014? Looking ahead, only 11 percent of respondents say the overall IT security budget for 2014 will significantly increase and 33 percent say the security budget will increase. Sixty percent of these respondents say on average their security budgets will increase between 5 to 20 percent.

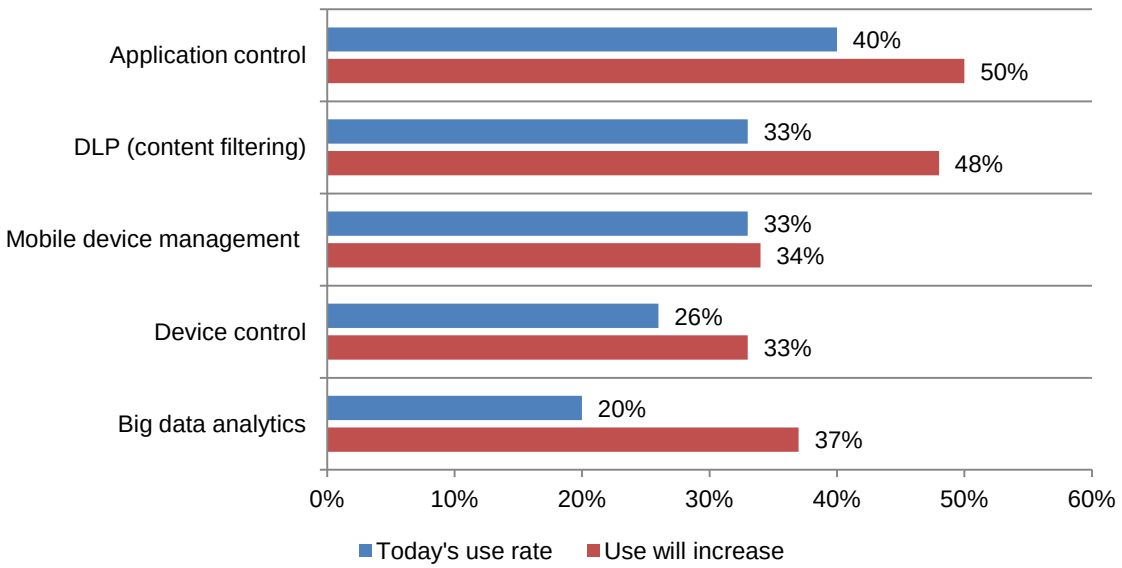
Malware incidents are straining IT security budgets. Fifty percent of respondents say their organization's IT operating expenses are increasing and this is an increase from 46 percent of respondents in 2012. As shown in Figure 11, 67 percent say malware incidents contribute a very significant or significant increase in these expenses and this is up slightly from 64 percent in 2012.

Figure 11. Do malware incidents increase IT security expenses?



How will companies spend their IT budget? Figure 12 reveals what technologies are mainly used today and where the biggest investments will occur. As shown, Application control/whitelisting (endpoint) will increase from 40 percent, data loss/lead prevention (content filtering) increases from 33 percent of respondents to 48 percent, active defense for identifying targeted attacks; mobile device management, and device control (removable media such as USB and CD/DVD) from 26 percent of respondents to 33 percent of respondents who say investments will increase.

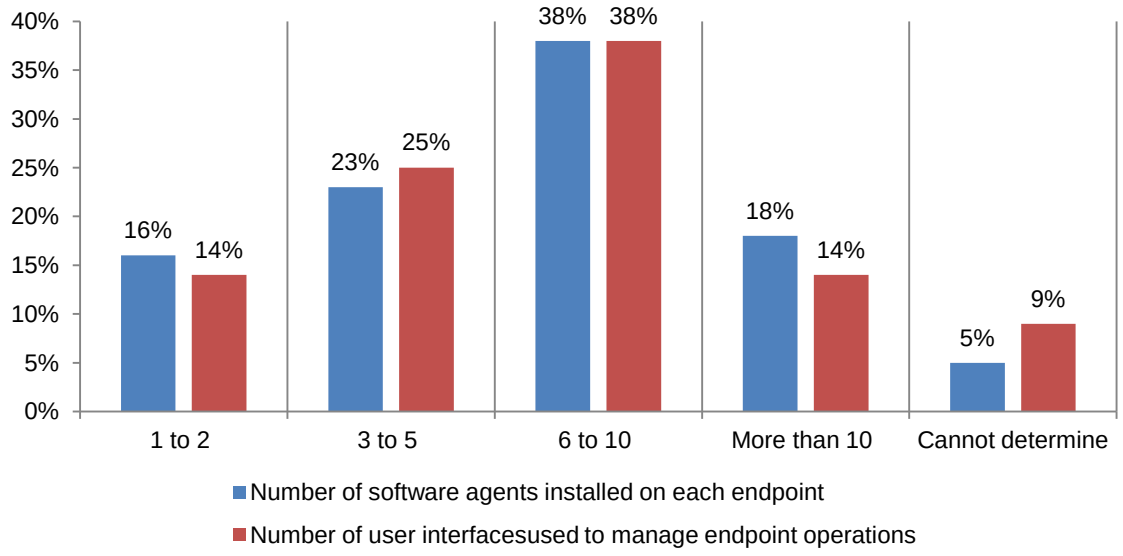
Figure 12. What technologies will organizations buy?
More than one response permitted



Use of integrated endpoint security suites will increase. Thirty-eight percent of respondents say their organization has such technology that includes vulnerability assessment, device control, anti-virus, anti-malware and others. Forty-nine percent say they will have this solution in the next 12 to 24 months.

As shown in Figure 13, an average of about 7 software agents are typically installed on each endpoint to perform management, security and/or other operations. On a typical day, on average 6 distinct software management user interfaces their organizations use to manage endpoint operations and security functions.

Figure 13. Software agents and software management user interfaces for endpoint risk management



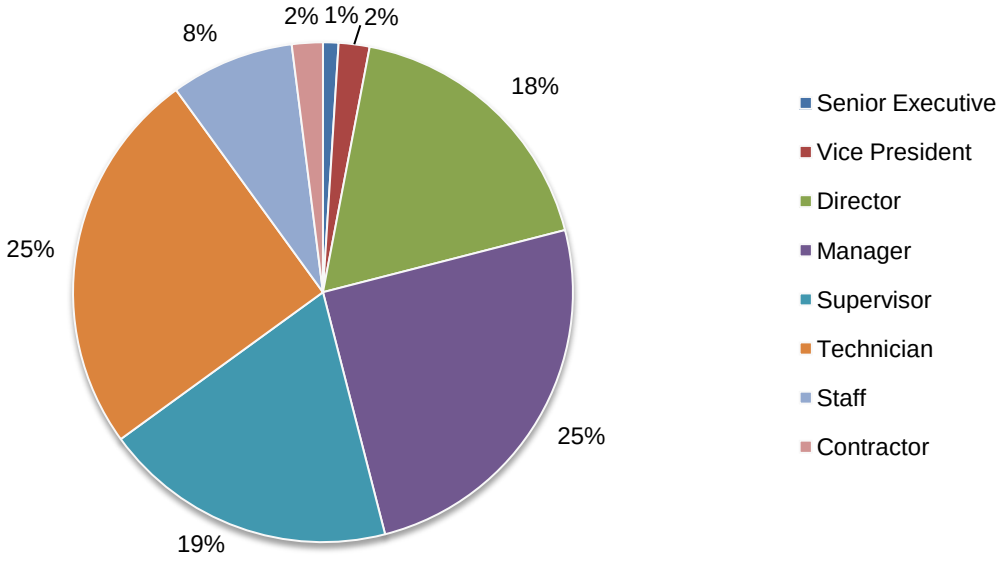
Part 4. Methods

A U.S. sampling frame of 19,001 IT practitioners who have knowledge in endpoint security were selected as participants to this survey. As shown in Table 1, 894 respondents completed the survey. Screening and failed reliability checks removed 218 surveys. The final sample was 676 surveys or a 3.6 percent response rate.

Table 1. Sample response	Freq	Pct%
Total sampling frame	19,001	100.0%
Total returns	894	4.7%
Rejected and screened surveys	218	1.1%
Final sample	676	3.6%

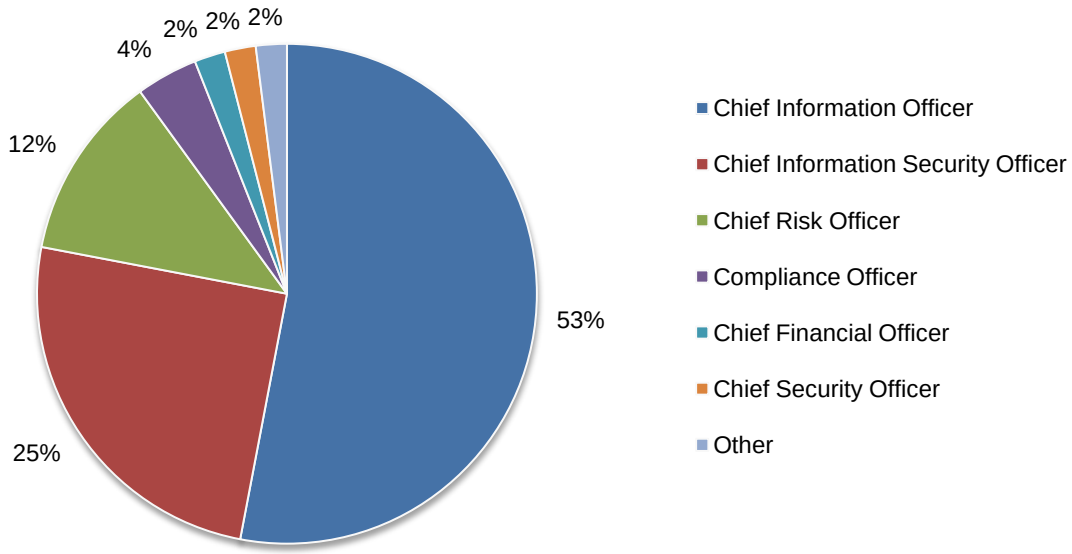
Pie Chart 1 reports the organizational level of respondents' current position. By design, 65 percent of respondents are at or above the supervisory levels.

Pie Chart 1. Organizational level that best describes your current position



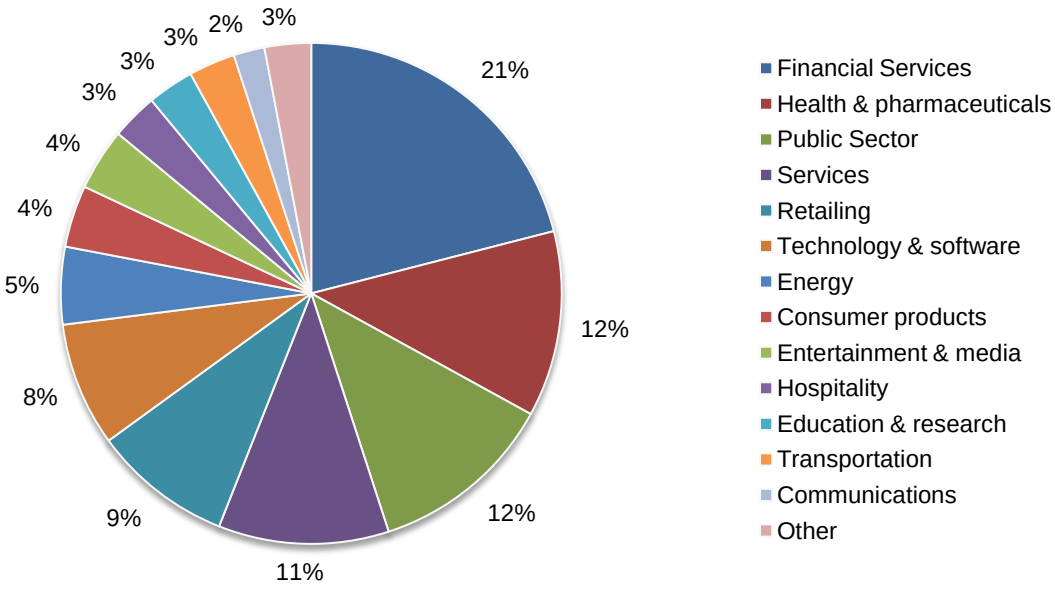
According to Pie Chart 2, 53 percent of respondents report directly to the Chief Information Officer and 25 percent report to the Chief Information Security Officer.

Pie Chart 2. Primary Person you or your IT security leader reports



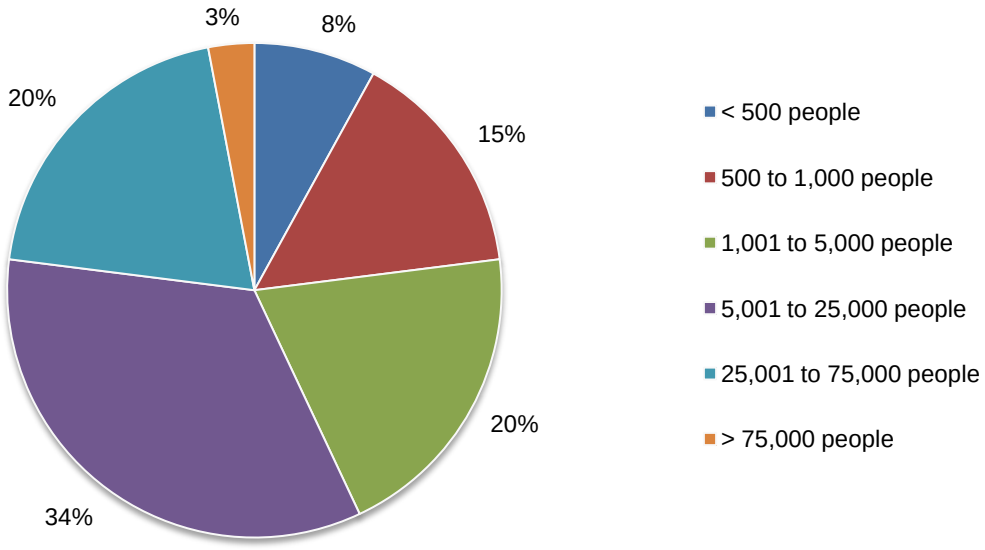
Pie Chart 3 reports the industry segments of respondents' organizations. This chart identifies financial services (21 percent) as the largest segment, followed by health & pharmaceuticals (12 percent) and public sector (12 percent).

Pie Chart 3. What industry best describes your organization's primary industry focus?



Pie Chart 4 reveals the worldwide headcount of the respondent's organization. Seventy-seven percent of respondents are from organizations with a global headcount greater than 1,000.

Pie Chart 4. Organization's worldwide headcount



Part 5. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

Appendix: Detailed Survey Results for FY 2013

The following tables provide the percentage frequency of responses to all survey questions contained in the present year's study. All survey responses were captured in October 2013.

Sample response	PCT%
Total sampling frame	19,001
Total returns	894
Rejected and screened surveys	218
Final sample	676
Response rate	3.6%

Part 1. Screening

S1. What best describes **your level of involvement** in endpoint security within your organization?	PCT%
None (stop)	0%
Low (stop)	0%
Moderate	11%
Significant	55%
Very significant	34%
Total	100%

S2. What best describes the number of employees (end users) who have access to your organization's network?	PCT%
Less than 50 (stop)	0%
51 to 100	0%
101 to 500	10%
501 to 1,000	21%
More than 1,000	69%
Total	100%

S3. What best describes your role within your organization's IT department?	PCT%
IT management	24%
IT operations	23%
Data administration	10%
IT compliance	10%
IT security	29%
Applications development	5%
I'm not involved in my organization's IT function (stop)	0%
Total	100%

S4. Please check all the activities that you see as part of your job or role.	PCT%
Managing budgets	55%
Evaluating vendors	40%
Setting priorities	32%
Securing systems	56%
Ensuring compliance	31%
None of the above (stop)	0%

Part 2: Attributions		
Please rate your opinion for the following two (2) statements using the scale provided below each item.	Strongly agree	Agree
Q1a. We have ample resources to minimize IT endpoint risk throughout our organization.	16%	16%
Q1b. Laptops and other mobile data-bearing devices such as smart phones are secure and do not present a significant security risk to our organization's networks or enterprise systems.	8%	13%

Part 3: Endpoint Risk

Q2a. In the past 24 months, has it become more difficult to reduce endpoint risk?	PCT%
Yes	71%
No	29%

Q2b. If yes, what is the single biggest threat to endpoint security in your organization? (Please select two top choices)	PCT%
Malware infections are more stealthy and difficult to detect	32%
The number of employees and others using multiple mobile devices in the workplace has increased	60%
The number of insecure mobile devices used in the workplace has increased significantly	33%
There are more personal devices connected to the network (BYOD)	51%
More employees are working offsite and using insecure WiFi connections	16%
Employees are more concerned about being productive than making sure their devices are secure	8%
Other	0%
Total	200%

Q3a. In the past 24 months, has endpoint security become a more important priority of your organization's overall IT security strategy?	PCT%
Yes	65%
No	35%
Total	100%

Q3b. If yes, over the past 24 months how has the budget for endpoint security changed?	PCT%
Significantly increased	5%
Increased	24%
Stayed the same	55%
Decreased	12%
Significantly decreased	4%
Total	100%

Q4a. How will your organization's IT security budget for 2014 compare to 2013?	PCT%
Significantly increase	10%
Increase	33%
Stay the same	43%
Decrease	11%
Significantly decrease	3%
Total	100%

Q4b. If the IT security budget for 2014 is increasing, what is the projected percentage increase?	PCT%
< 5%	22%
5 to 10%	35%
11 to 20%	25%
21 to 30%	11%
31 to 40%	5%
41 to 50%	2%
> 50%	0%
Total	100%

Q5. On average, how many malware attempts or incidents does your IT organization deal with monthly?	PCT%
Less than 5	0%
5 to 10	7%
11 to 25	13%
26 to 50	21%
More than 50	41%
Not sure	18%
Total	100%
Extrapolated value	50.5

Q6. Has the frequency of malware incidents changed over the last year within your organization?	PCT%
Yes, major increase	44%
Yes, but only slight increase	15%
No, the frequency stayed the same	19%
No, there has been a slight decrease	8%
No, there has been a major decrease	2%
No, they have decreased	
Not sure how the frequency has changed	12%
Total	100%

Q7. Which of these types of incidents or compromises are you seeing **frequently** in your organization's IT networks? Please check all that apply.	PCT%
Zero day attacks	36%
Exploit of existing software vulnerability less than 3 months old	35%
Exploit of existing software vulnerability greater than 3 months old	26%
SQL injection	28%
Spyware	40%
Botnet attacks	49%
Clickjacking	46%
Rootkits	67%
General malware	80%
Web-borne malware attacks	74%
Advanced persistent threats (APT) / Targeted attacks*	59%
Spear phishing	48%
Hacktivism	
Other (please specify)	4%
Total	592%
*Termed Targeted Attacks in the 2011 survey	

Q8. Where are you seeing the greatest rise of potential IT security risk within your IT environment? Please choose only your top five choices.	PCT%
Our server environment	17%
Our data centers	7%
Within operating systems (vulnerabilities)	8%
Across 3rd party applications (vulnerabilities)	66%
Our PC desktop/laptop	43%
Mobile devices such as smart phones (Blackberry, iPhone, IPad, Android)	75%
Removable media (USB sticks) and/or media (CDs, DVDs)	35%
Network infrastructure environment (gateway to endpoint)	12%
Malicious insider risk	15%
Negligent insider risk	40%
Negligent third party risk (partner, vendors, customers, etc.)	33%
Cloud computing infrastructure and providers	36%
Virtual computing environments (servers, endpoints)	9%
Mobile/remote employees	45%
Lack of system connectivity/visibility	31%
Lack of organizational alignment	28%
Total	500%
*Top 3 choices in the 2010 survey	

Q9a. Have your endpoints been the entry point for an APT/ targeted attack in the last 12 months?	PCT%
Yes	40%
No	35%
Unsure	25%
Total	100%

Q9b. If yes, how did you learn you were victim of APT/ targeted attacks?	PCT%
Our endpoint security technology alerted us to a possible breach	24%
We were notified by law enforcement	21%
We found anomalous exfiltration traffic on the network	53%
Other (please specify)	2%
Total	100%

Q9c. If yes, how did the APT/ targeted attack start? Please select more than one if your company experienced multiple targeted attacks.	PCT%
Spear phishing emails sent to employees	45%
USB key delivery	9%
Fraudulently signed code/ digital certificates	33%
Web-based click jacking	34%
SQL injection code	12%
Memory based attack	21%
Other	2%
Unsure	25%
Total	181%

Q10. In the coming year, which of the following IT security risks are of most concern to your organization? Please select only your top three choices.*	PCT%
Use of cloud computing resources (i.e. Dropbox)	44%
Advanced persistent threats / targeted attacks	39%
Malicious insider risk	12%
Negligent insider risk	14%
Insufficient budget resources	25%
Increased use of mobile platforms (smart phones, iPads, etc.)	55%
Growing volume of malware	28%
Increasingly sophisticated and targeted cyber attackers	35%
Lack of an organizational wide security strategy	9%
Insufficient collaboration among IT and business operations	11%
Lack of integration between endpoint operations and security technologies	6%
Inability to measure policy compliance	5%
Intrusions and data loss within virtual environments	17%
Other (please specify)	0%
Total	300%
*Three responses permitted in 2012	

Part 4. Endpoint Productivity		
Q11. Please estimate how the use of each one of the following technologies will change in your organization over the next 12 to 24 months. Please use the following five-point scale for each technology listed below.1= substantial increase, 2 = increase, 3 = no change, 4 = decrease, 5 = substantial decrease. **Please leave blank if your organization does not use or plan to use each technology listed below.**	Substantial increase	Increase
Mobile devices / smart phones and tablets	44%	35%
Virtualized environments (servers & desktops)	14%	31%
Use of 3rd party (non-company) cloud computing infrastructure	38%	32%
Use of internal cloud computing infrastructure	23%	23%

Q12. What percent of your organization's employees use mobile devices in the workplace?	PCT%
None	0%
1 to 25%	5%
26 to 50%	18%
51 to 75%	40%
More than 75%	29%
Cannot determine	8%
Total	100%
Extrapolated value	63%

Q13. How many mobile devices does your organization actively manage?	PCT%
None	4%
< 50	5%
50 to 100	2%
101 to 250	6%
251 to 750	8%
751 to 1,500	11%
1,501 to 5,000	20%
> 5,000	35%
Unsure	9%
Total	100%
Extrapolated value	4,755

Q14. And in the next 3 years, how many mobile devices do you anticipate will be actively managed by your organization?	PCT%
None	0%
< 50	2%
50 to 100	2%
101 to 250	3%
251 to 750	7%
751 to 1,500	9%
1,501 to 5,000	14%
> 5,000	54%
Unsure	9%
Total	100%
Extrapolated value	6,592

Q15. Have your mobile endpoints been the target of malware in the last 12 months?	PCT%
Yes	68%
No	22%
Unsure	10%
Total	100%

Q16a. If employee-owned mobile devices are connected to your organization's networks, does the organization have an effort in place to secure them?	PCT%
No, and we have no immediate plans to manage employee owned devices	28%
No, but we plan to begin managing them soon	18%
Yes, we secure them in a manner similar to that already in place for corporate devices	43%
Yes, we use stricter security standards for employee-owned mobile devices than we do for corporate-owned devices	11%
Total	100%

Q16b. If yes, what elements are included in your mobile device management (MDM) policy for employee-owned devices? Please check all that apply.	PCT%
Mandatory enrollment in company MDM solution through technological means	35%
Mandatory endpoint protection agent on laptops through technological means	32%
Prohibiting exchange activesync through technologic means	29%
Active discovery of BYOD devices on the network and in exchange/email server logs	25%
Voluntary enrollment in MDM solution	29%
Voluntary installation of endpoint protection agent	54%
Total	204%

Q17. Which of the following technologies does your organization use or plan to invest in over the next 12 months? In addition, please estimate how each technology's use will change over this time period.	Today's use rate	Use will increase
Anti-virus	100%	0%
Application control firewall (gateway) (NGFW)	44%	4%
Application control/whitelisting (endpoint)	40%	50%
Data loss/leak prevention (content filtering)	33%	48%
Device control (removable media i.e., USB, CD/DVD)	26%	33%
Endpoint firewall	65%	25%
Intrusion detection	62%	8%
Network access control (NAC)	51%	11%
Patch & remediation management	52%	20%
Vulnerability assessment (vulnerability scanning)	45%	27%
Active defense (big data and predictive analytics) for identifying targeted atacks	20%	37%
Whole disk encryption	32%	13%
Endpoint management and security suite (integrated technologies like AV, patch, etc.)	37%	30%
Mobile device management	33%	34%
Security Event and Incident Management (SEIM)	39%	12%
Identity verification (for detecting behavior anomalies when attempting access)	33%	15%

Q18. Please identify the percentage of your organization's IT environment that is committed to the following operating system platforms. Use all 100 points in the table below to allocate your response.	Points
Windows o/s	53
Mac o/s	17
Linux	15
Unix	13
Other	2
Total points	100

Q19. [For those using the Apple Mac], How concerned are you about Mac malware infections?	PCT%
Very concerned	45%
Increasingly concerned	45%
Not at all concerned	9%
Not applicable	1%
Total	100%

Q20a. Are your organization's IT operating expenses increasing?	PCT%
Yes	50%
No	37%
Unsure	13%
Total	100%

Q20b. If yes, to what extent are malware incidents contributing to an increase in expenses?	PCT%
Very significant	23%
Significant	44%
Some significance	23%
None	10%
Total	100%

Part 5. Endpoint Resources

Q21a. Does your organization have a centralized cloud security policy?	PCT%
Yes	54%
No	34%
Unsure	12%
Total	100%

Q21b. If yes, do you enforce employees' use of private clouds (i.e., use of DropBox)?	PCT%
Yes	55%
No	37%
Unsure	8%
Total	100%

Q22. In regards to mobile device management, what are the three most important capabilities for meeting your organization's needs?	PCT%
Provisioning and access policy management	70%
Virus and malware detection or prevention	73%
Asset tracking	52%
Encryption and other data loss technologies	38%
Anti-theft features	35%
Remote wipe capability	32%
Other (please specify)	0%
Total	300%

Q23. When it comes to IT security, which applications are of greatest concern to your organization in terms of increasing vulnerabilities and IT risk? Please choose only your top three choices.	PCT%
Microsoft OS/applications	37%
Apple/Mac OS	30%
Apple apps (QuickTime, iTunes, etc.)	29%
Adobe (Flash, Adobe Reader, etc.)	60%
WinZip	8%
Oracle applications	20%
VMware	15%
Google Docs	50%
Mozilla Firefox	3%
General 3rd party applications outside of Microsoft	33%
Use of private cloud applications (such Dropbox)	15%
Other (please specify)	0%
Total	300%

Q24. Is your organization planning to pilot or expand its usage of application control/whitelisting technologies within the endpoint environment sometime within the next 12 months?	PCT%
Yes, with certainty	35%
Yes, likely to do so	39%
No	18%
Unsure	8%
Total	100%

Q25. Does your organization have an integrated endpoint security suite (vulnerability assessment, device control, anti-virus, anti-malware or others)?	PCT%
Yes	38%
No, but our organization expects to have an endpoint security suite within the next 12-24 months	49%
No	13%
Total	100%

Q26. Approximately how many **software agents** does your organization typically have installed on each endpoint to perform management, security and/or other operations? Please provide your best estimate.	PCT%
1 to 2	16%
3 to 5	23%
6 to 10	38%
More than 10	18%
Cannot determine	5%
Total	100%
Extrapolated value	6.69

Q27. On a typical day, how many different or distinct software management **user interfaces** does your organization use to manage endpoint operations & security functions? Please provide your best estimate.	PCT%	FY 2012
1 to 2	14%	19%
3 to 5	25%	25%
6 to 10	38%	35%
More than 10	14%	11%
Cannot determine	9%	10%
Total	100%	100%
Extrapolated value	6.24	6.01

Part 6: Organizational Characteristics & Demographics

D1. What organizational level best describes your current position?	PCT%	FY 2012
Senior Executive	1%	0%
Vice President	2%	2%
Director	18%	19%
Manager	25%	26%
Supervisor	19%	19%
Technician	25%	23%
Staff	8%	7%
Contractor	2%	3%
Other	0%	1%
Total	100%	100%

D2. Check the **Primary Person** you or your IT security leader reports to within the organization.	PCT%	FY 2012
CEO/Executive Committee	0%	0%
Chief Financial Officer (CFO)	2%	1%
General Counsel	1%	3%
Chief Information Officer (CIO)	53%	54%
Chief Information Security Officer (CISO)	25%	23%
Compliance Officer	4%	6%
Human Resources VP	0%	0%
Chief Security Officer (CSO)	2%	4%
Chief Risk Officer	12%	9%
Other	1%	0%
Total	100%	100%

D6. What industry best describes your organization's **primary** industry focus?	**PCT%**
Consumer products	4%
Communications	2%
Agriculture	1%
Defense	1%
Energy	5%
Entertainment & media	4%
Financial Services	21%
Health & pharmaceuticals	12%
Hospitality	3%
Industrial	1%
Public Sector	12%
Education & research	3%
Retailing	9%
Services	11%
Technology & software	8%
Transportation	3%
Total	100%

D4. Where are your employees located? Check all that apply.	**PCT%**
United States	100%
Canada	63%
Europe	72%
Middle East	28%
Asia-Pacific	55%
Latin America (including Mexico)	36%
Africa	6%

D5. What is the worldwide headcount of your organization?	**PCT%**
Less than 500 people	8%
500 to 1,000 people	15%
1,001 to 5,000 people	20%
5,001 to 25,000 people	34%
25,001 to 75,000 people	20%
More than 75,000 people	3%
Total	100%

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO),** we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.