2015 State of the Endpoint Report: User-Centric Risk

Sponsored by Lumension

Independently conducted by Ponemon Institute LLC

Publication Date: January 2015

2015 State of Endpoint Report: User-Centric Risk

Ponemon Institute, January 2015

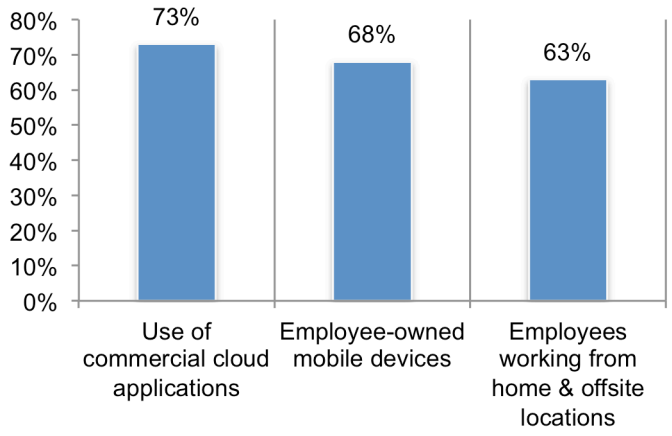
Part 1. Introduction

Ponemon Institute is pleased to present the results of the *2015 State of Endpoint Report: User-Centric Risk* study sponsored by Lumension. This annual study is conducted by Ponemon Institute to understand trends and changes in endpoint risk in organizations. An endpoint can include servers, desktops, laptops, smartphones, and even printers, ATMs and PoS devices.

The biggest problem identified in this year's research is the negligent or careless employee with multiple mobile devices using commercial cloud apps and working outside the office.

Figure 1. Reasons why IT believes endpoint risk has increased significantly

Strongly agree and agree response combined



We surveyed 703 US IT and IT security practitioners who are involved in endpoint security in their organizations. As shown in Figure 1, IT practitioners report use of commercial cloud applications (73 percent), BYOD (68 percent) and employees who operate from home offices and offsite locations (63 percent) have significantly increased endpoint risk. Sixty-eight percent of respondents say their IT department cannot keep up with employee demand for greater support and better mobile device connectivity.

Following are some of the most salient findings from the study:

Negligent employees are seen as the greatest source of endpoint risk. The primary reason for the difficulty in managing endpoint risk is negligent or careless employees who do not comply with security policies. This is followed by an increase in the number of personal devices connected to the network (BYOD), employees' use of commercial cloud applications in the workplace and the number of employees and others using multiple mobile devices in the workplace.

This year, mobile endpoints have been the target of malware. Seventy-one percent of respondents say in the past 24 months managing endpoint risk has become very difficult. In fact, 75 percent of respondents (an increase from 68 percent in last year's study) believe their mobile endpoints have been the target of malware over the past 12 months.

In recognition of the growing risk, endpoint security is becoming a more important priority. Sixty-eight percent of respondents say endpoint security is becoming a more important part of their organization's overall IT security strategy.

Web-borne malware attacks are frequent in an organization's IT networks. Eighty percent of respondents say web-borne malware attacks are seen frequently in their organization's IT

networks followed by advanced persistent threats (APT)/targeted attacks (65 percent) and rootkits (65 percent). The biggest increase is in zero day attacks, APTs and spear phishing.

Certain applications increase vulnerabilities and IT risk. Causing the most problems in managing endpoint risk are the following applications: Adobe (e.g. Acrobat, Flash Player, Reader) (62 percent of respondents), Oracle Java JRE (54 percent of respondents) and third-party cloud-based productivity apps (e.g. WinZip, VLC, VMware and VNC).

Mobile devices, such as smart phones, have seen the greatest rise in potential IT security risk in the IT environment. Eighty percent of respondents say smart phones are a concern followed by vulnerabilities in third party applications (69 percent), mobile remote employees (42 percent) and the negligent insider risk.

Governance and control processes are the biggest gaps in stopping attacks on endpoints. On average, 28 percent of attacks on an organization's endpoints cannot be realistically stopped with enabling technologies, processes and in-house expertise. Seventy percent of respondents agree that their organizations' endpoint security policies are difficult to enforce.

How will organizations deal with increased endpoint risk? The research also reveals these three predictions for 2015:

1. **Virtually all organizations will evolve toward a more "detect and respond" orientation from one that is focused on prevention.** In addition, according to 70 percent of respondents, their organizations are using or plan to use within the next two years the use of "big data" to enhance endpoint and database security.

2. **Threat intelligence increases in importance**. Sixty-four percent of respondents say they have added or plan to add a threat intelligence component to their companies' security stack.

3. **The endpoint becomes a security sensor**. In other words, where state or context data collected at the endpoint is used to determine if it has been or is being compromised.

Part 2. Key findings

In this section, we provide an analysis of the key findings. Several figures show comparable results captured since 2010. The completed audited findings are presented in the appendix of this report. We have organized the report according to the following themes:

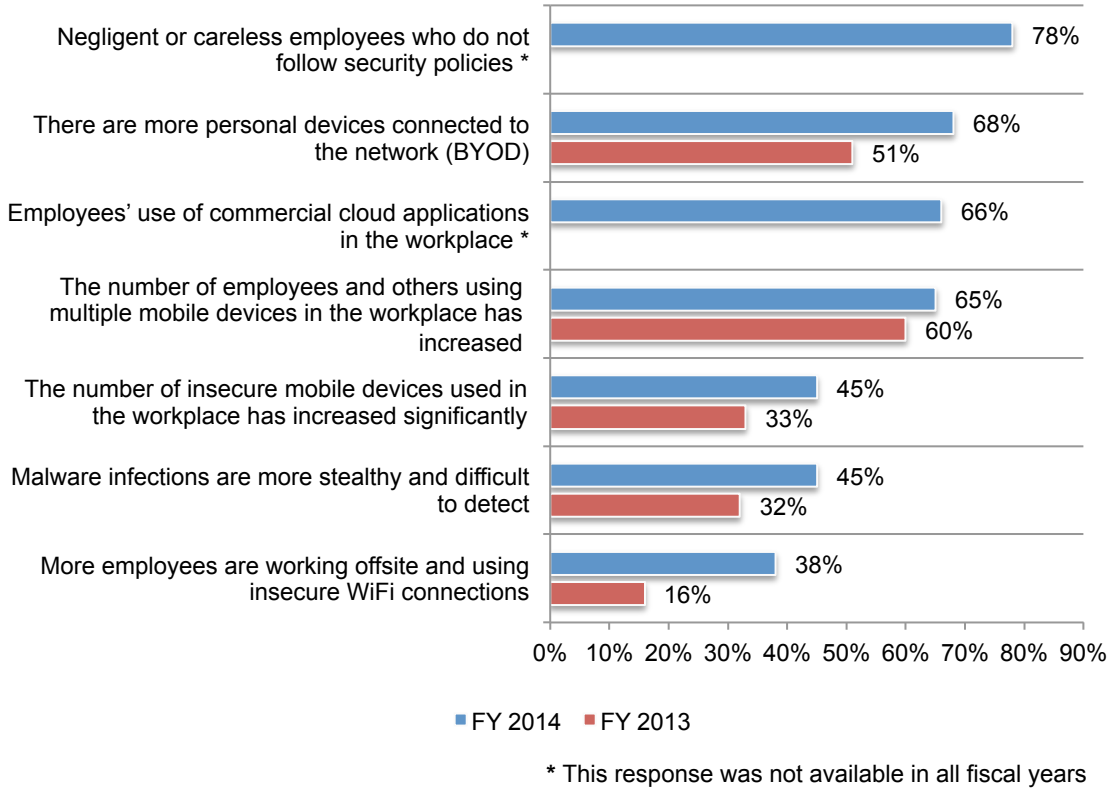
- The shift from endpoint risk to user centric risk
- Malware and other security compromises are getting worse
- How organizations are addressing endpoint risk
- Predictions for 2015

The shift from endpoint risk to user centric risk

Negligent employees (users) are seen as the greatest source of endpoint risk. Figure 1 reveals certain threats to endpoint security are increasing significantly. Since 2013, the percentage of respondents who say the threat of employees working offsite and using insecure WiFi increased from 16 percent to 38 percent (22 percent increase) and more personal devices connected to the network (BYOD) increased from 51 percent to 68 percent (17 percent increase).

For the first time, we asked if negligent employees who do not follow security policies are a threat to endpoint security. Seventy-eight percent of respondents agree, making it the number one threat.

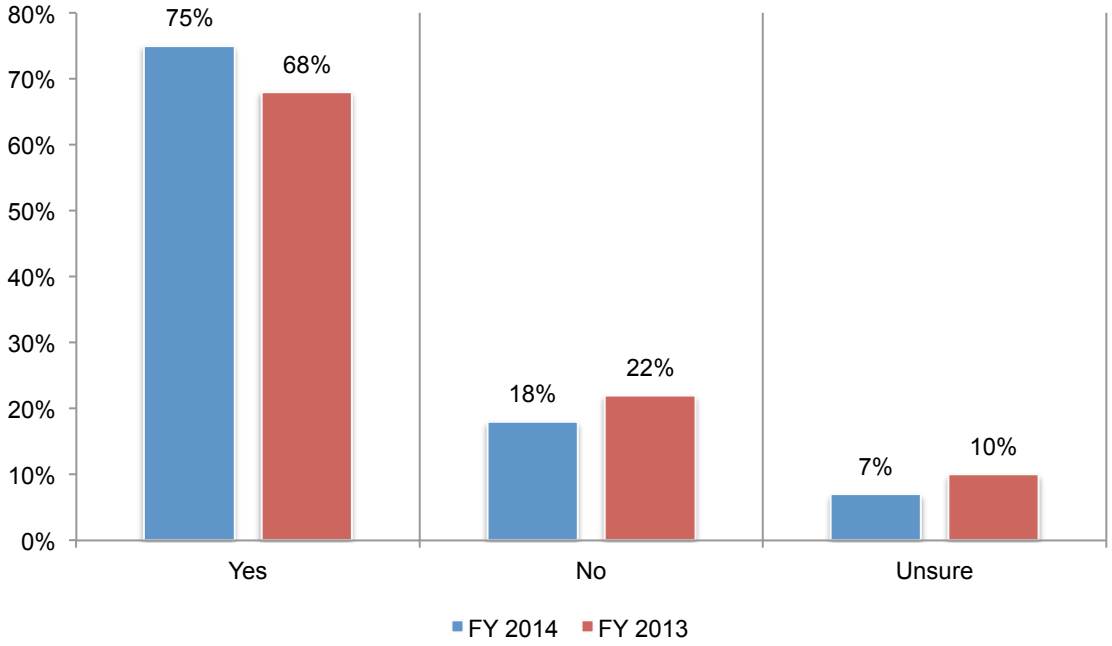
Figure 1. What are the biggest threats to endpoint security in your organization?
Five choices permitted



* This response was not available in all fiscal years

Malware targets mobile endpoints. Seventy-one percent of respondents say in the past 24 months managing endpoint risk has become very difficult. In fact, 75 percent of respondents (an increase from 68 percent in last year's study) believe their mobile endpoints have been the target of malware over the past 12 months, as shown in Figure 2.

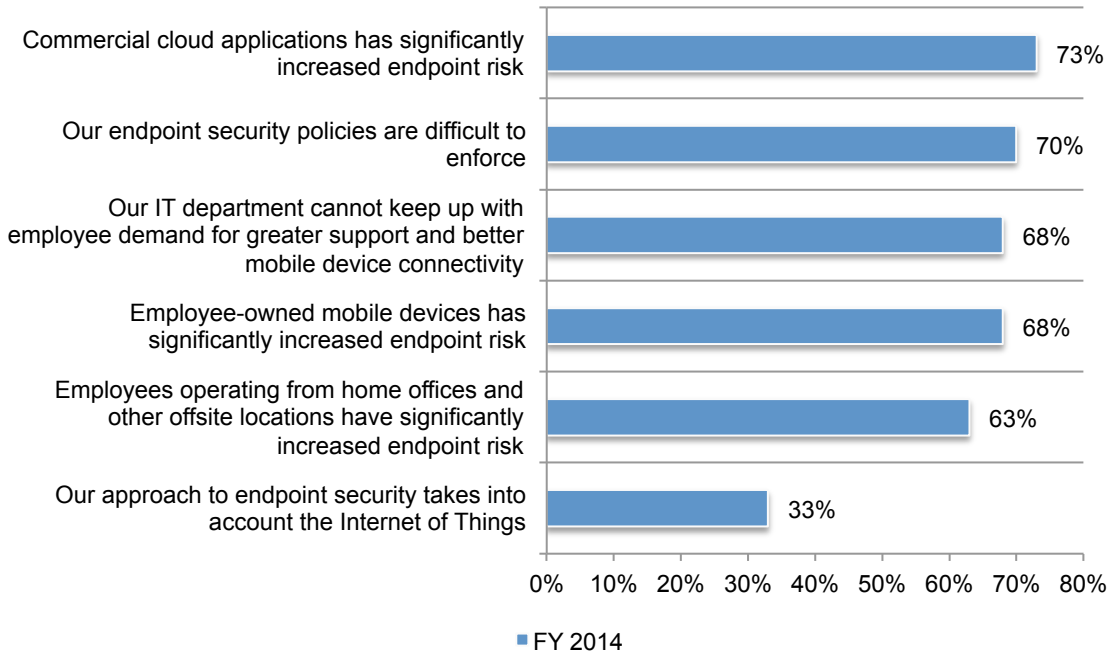
Figure 2. Mobile endpoints have been the target of malware over the past 12 months



Employees' use of mobile devices and commercial cloud increase endpoint risk significantly. Respondents report use of commercial cloud applications (73 percent), BYOD (68 percent), and employees who operate from home offices and offsite locations (63 percent) have significantly increased endpoint risk, as shown in Figure 3.

In fact, 68 percent of respondents say their IT department cannot keep up with employee demand for greater support and better mobile device connectivity and 70 percent say their endpoint security policies are difficult to enforce. Only 33 percent of respondents agree that their approach to endpoint security takes into account the Internet of Things (IoT), which means that most companies represented in this study are not addressing the potential endpoint risk created by IoT.

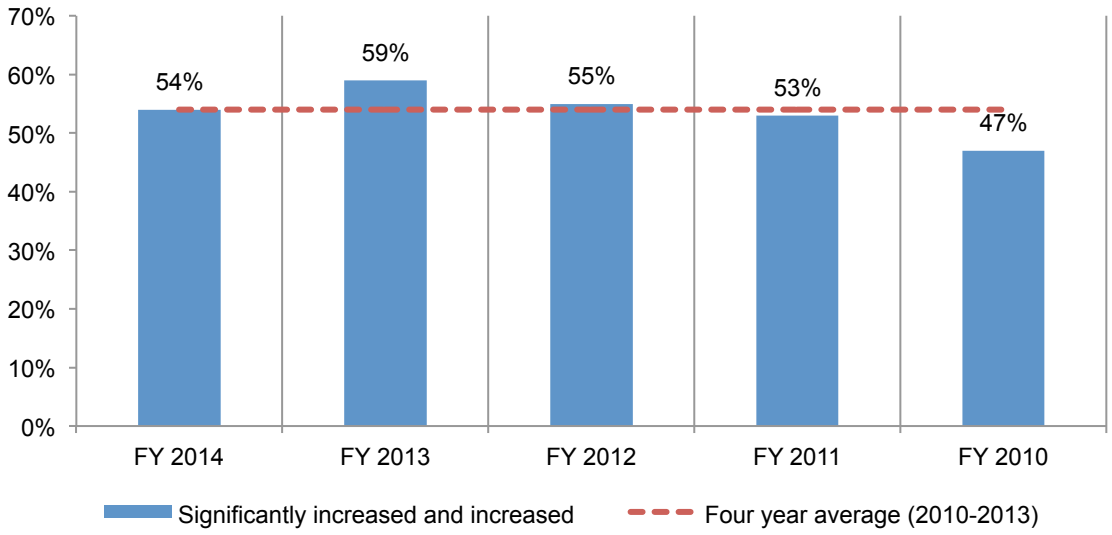
Figure 3. Factors contributing to endpoint security risk
Strongly agree and agree response combined



Malware and other security compromises are getting worse

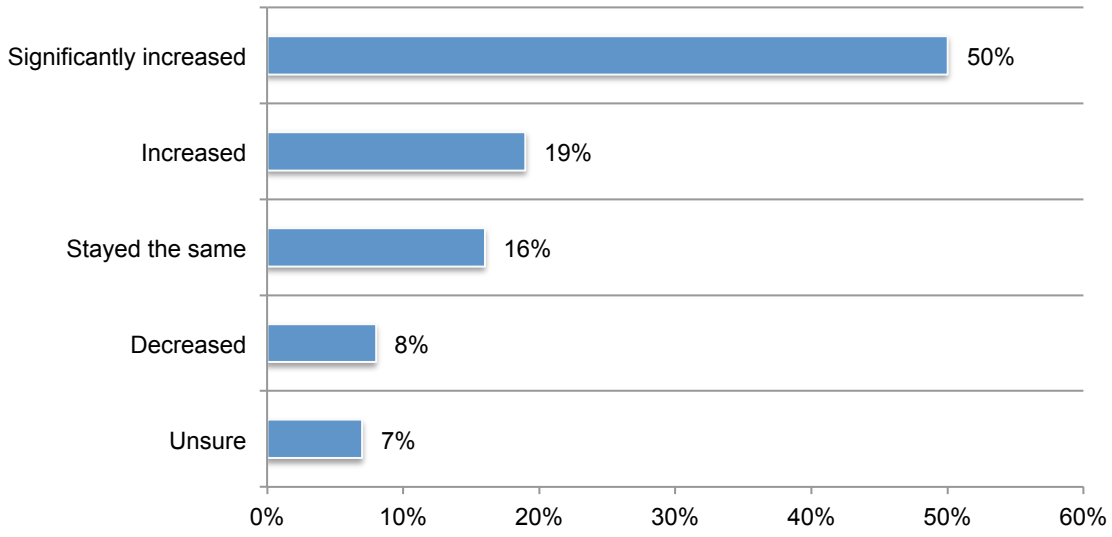
The rate of malware has steadily increased. With the exception of 2010, a majority of respondents report that the frequency of malware incidents continues to increase or significantly increase since we have been conducting this study. As noted in Figure 4, this trend increases for four years and then decreases in 2014. The average frequency of responses is 54 percent.

Figure 4. Changes in the frequency of malware incidents over five years
Significantly increased and increased response combined



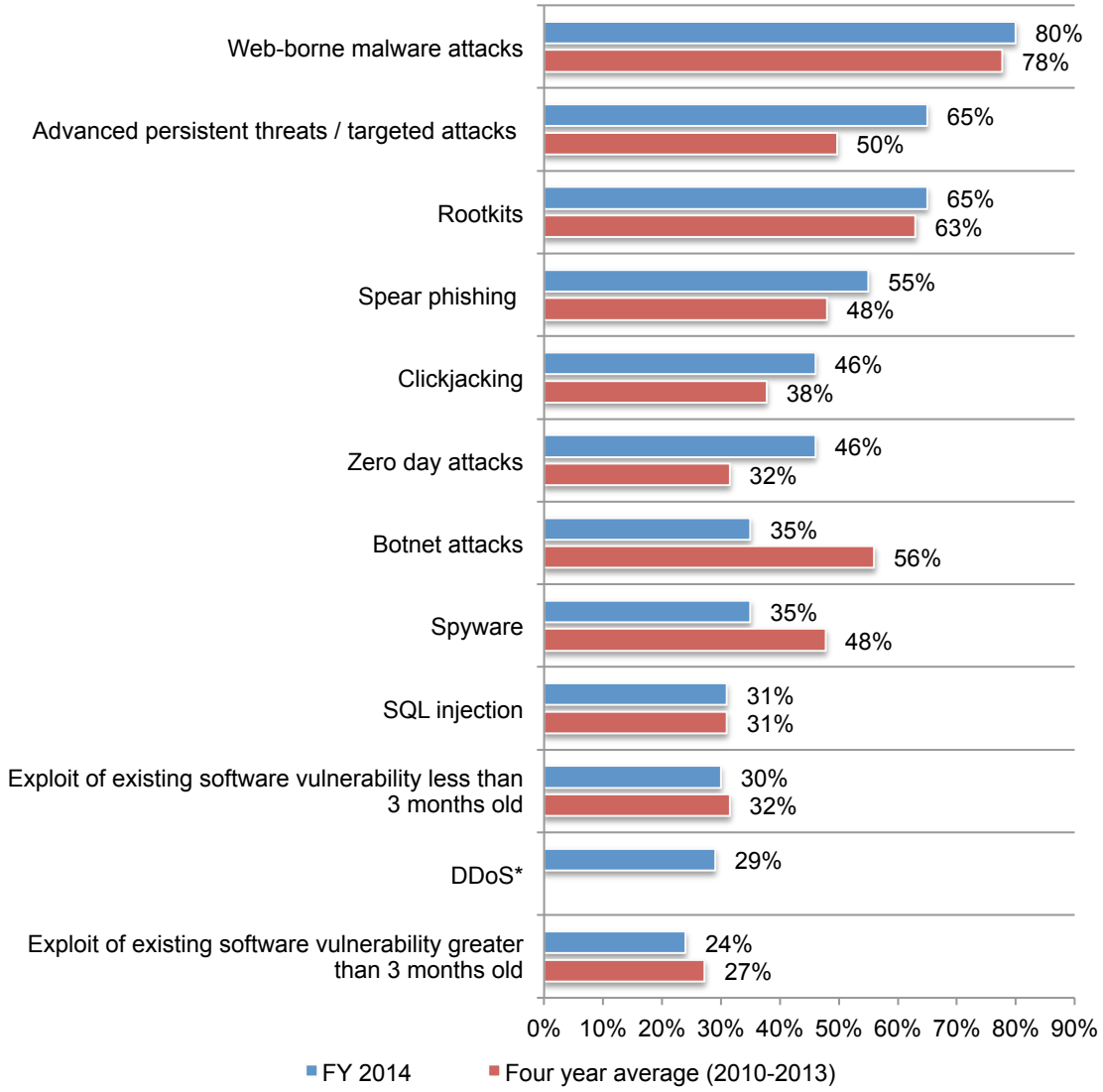
Malware incidents are increasing in severity. Figure 5 shows the change in the severity of malware experienced in 2014. As can be seen, half of respondents believe severity of malware infections have significantly increased over the past year. In sharp contrast, only 24 percent of respondents believe malware severity has decreased or stayed the same.

Figure 5. Change in the severity of malware incidents over the past year



Advanced persistent/targeted attacks increased dramatically. While web-borne malware attacks are still considered the most frequent, 65 percent of respondents say they are experiencing more APTs/targeted attacks, an increase from the four-year average of 50 percent of respondents, according to Figure 6. Other significant increases include zero day attacks (an increase from 32 percent to 46 percent) and spear phishing (an increase from 48 percent to 55 percent). Botnets and spyware have decreased in in this year's study.

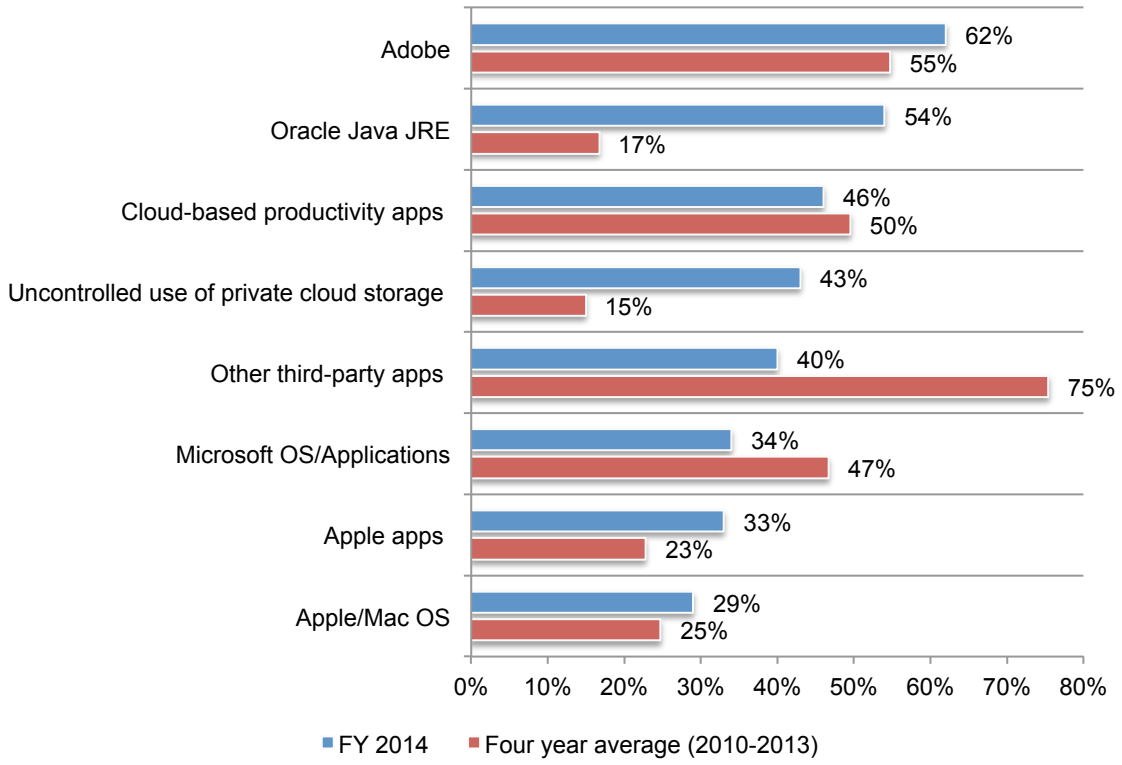
Figure 6. Trends in the most frequent attacks against an organization's IT networks
Most frequently cited incidents or compromises experienced by respondents
More than one response permitted



* This response was not available in all fiscal years

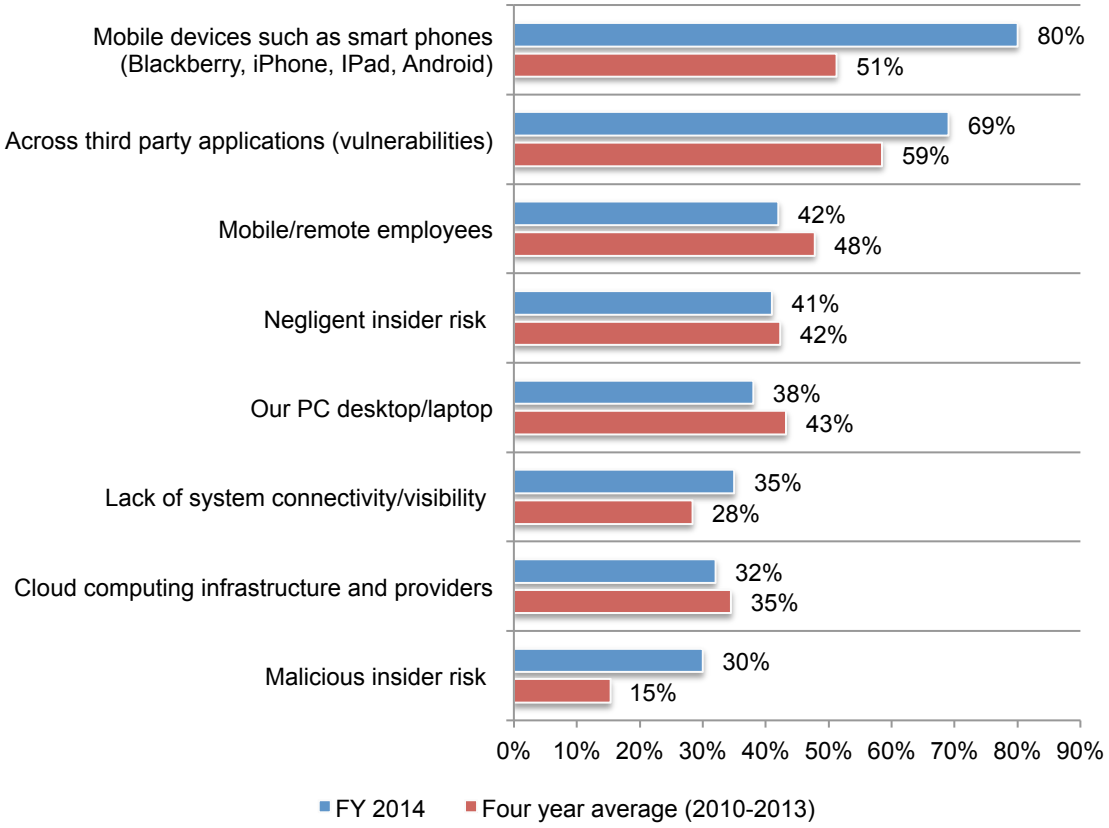
Applications increase endpoint risk. Applications causing the most problems in minimizing malware risks are Adobe (e.g. Acrobat, Flash Player, Reader) (62 percent of respondents), Oracle Java JRE (54 percent of respondents) and cloud-based productivity apps (e.g. WinZip, VLC, VMware and VNC). As shown in Figure 7, the risk of Oracle Java JRE and uncontrolled use of private cloud storage has increased significantly. In contrast, other third party apps and Microsoft OS/Applications have decreased in perceived malware risk.

Figure 7. Trends in applications that increase IT risk
Applications that respondents believe are prone to malware infection
Five responses permitted



Mobile devices such as smart phones have seen the greatest rise in potential IT security risk in the IT environment. Figure 8 reveals that 80 percent of respondents say smart phones are a concern followed by vulnerabilities in commercial third party applications (69 percent), mobile remote employees (42 percent) and the negligent insider risk.

Figure 8. Trends in potential security risks within the IT environment
Areas and issues that cause significant IT security risks according to respondents
Five responses permitted



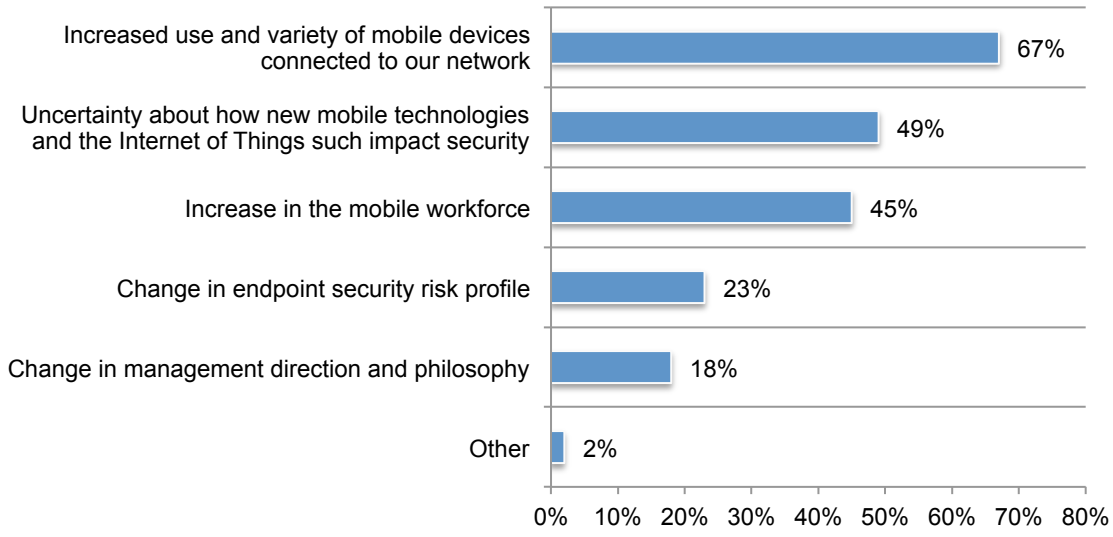
How organizations are addressing endpoint risk

Endpoint security is becoming a more important priority. Sixty-eight percent of respondents say endpoint security is becoming a more important part of their organization's overall IT security strategy.

The primary reasons are the increased use and variety of mobile devices connected to the network (67 percent of respondents) followed by uncertainty about how new mobile technologies and the Internet of Things affect security (49 percent of respondents) and an increase in the mobile workforce, as shown in Figure 9.

If endpoint security is less important, it is due to a change in management direction and philosophy and change in endpoint security risk profile. Almost half (49 percent) of respondents are concerned about the Internet of Things. As discussed previously 33 percent of respondents are concerned that their approach to endpoint security does not take into account the Internet of Things.

Figure 9. Why has endpoint security become more important over the past 24 months?
More than one response permitted

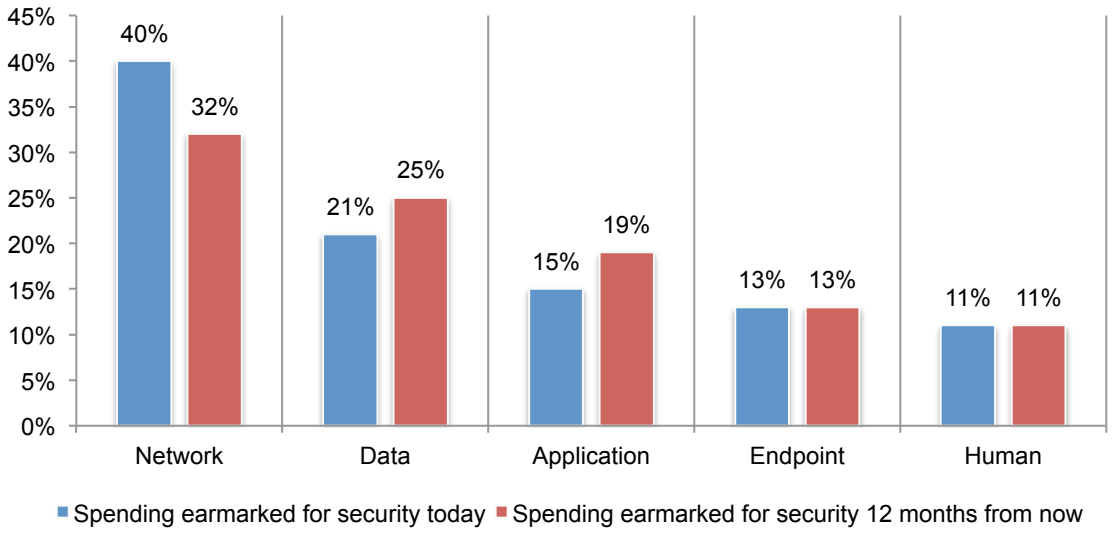


Growth in IT security remains constant. Forty-five percent of respondents say their organization's IT security budget will significantly increase (12 percent) or increase (33 percent). This is similar to last year when 43 percent of respondents believed their organizations would significantly increase (10 percent) and increase (33 percent).

While companies are making endpoint security a higher priority, Figure 10 reveals that the IT security budget allocation is expected to change next year. Network security is expected to decline from 40 percent to 32 percent. Data security and application security are expected to receive more funding. Despite the fact that employee negligence is recognized as a serious threat, only 11 percent of the budget is allocated to dealing with malicious or negligence insiders or third parties.

In another finding, only 34 percent of respondents say they have ample resources to minimize IT endpoint risk throughout their organization. This is consistent with prior studies.

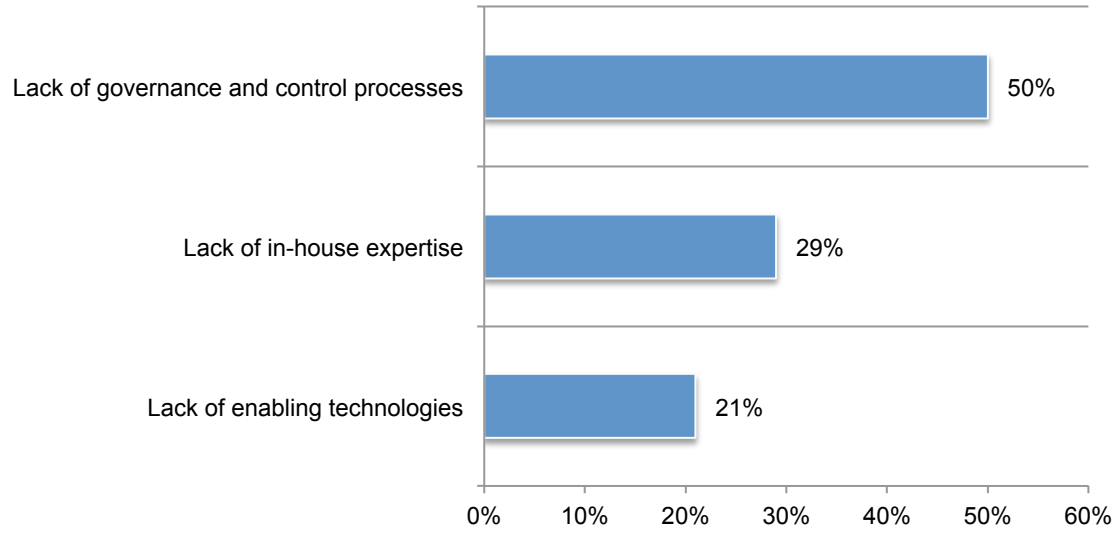
Figure 10. Spending earmarked for IT security risks



Governance and control processes are the biggest gaps in stopping attacks on endpoints. On average, respondents believe 72 percent of attacks on an organization's endpoints can be realistically stopped with enabling technologies, processes and in-house expertise.

According to Figure 11, the biggest gap in being able to mitigate these attacks is a lack of governance and control processes, which would include training and awareness programs for employees and enforcement of endpoint security policies. Seventy percent of respondents agree that their organizations' endpoint security policies are difficult to enforce.

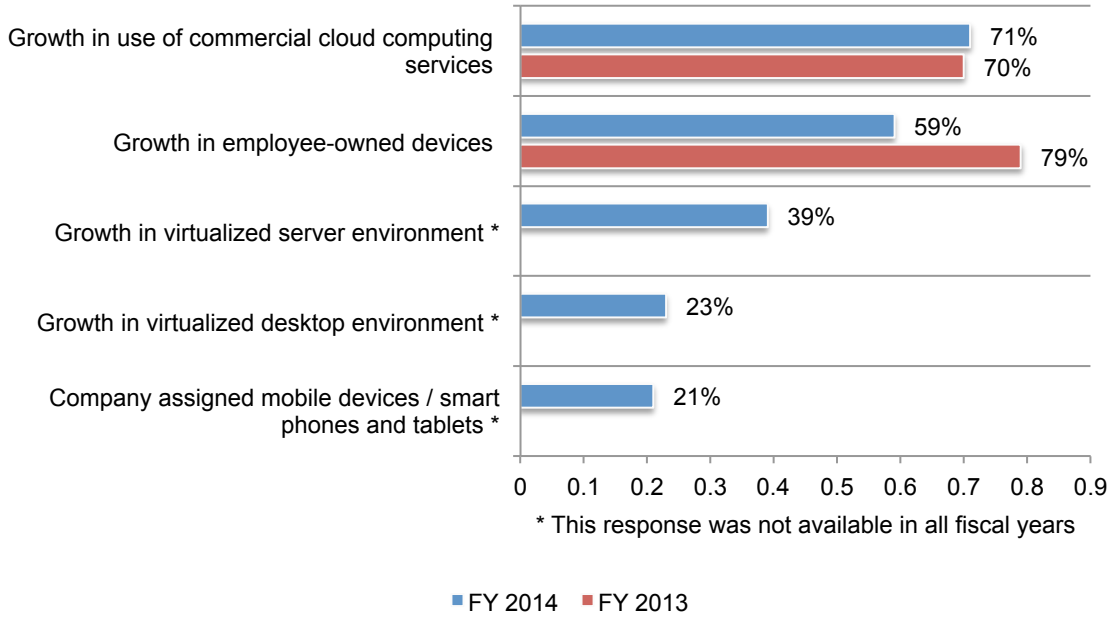
Figure 11. The one biggest gap in the ability to stop attacks to endpoints



Predictions for the forthcoming year

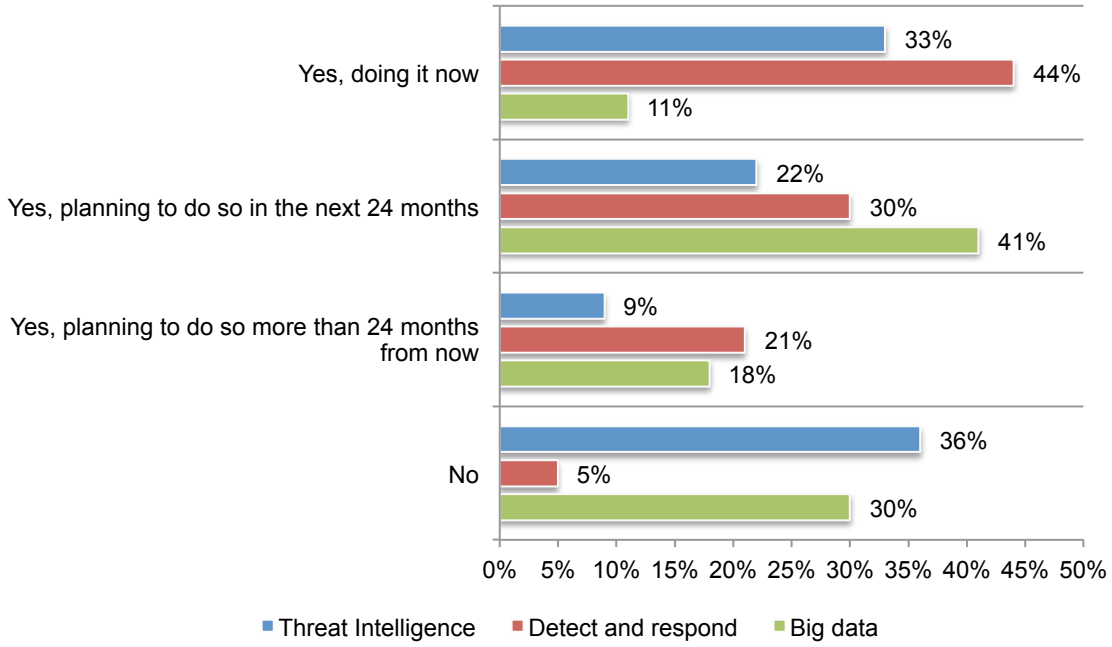
More risk ahead because of the continued growth in the use of commercial cloud applications. More employees and other insiders will continue to increase their use of commercial cloud computing services will gain in use (71 percent of respondents), as shown in Figure 12. However, growth in BYOD is expected to flatten. Last year, 79 percent of respondents believed there would be a substantial increase or increase in employee-owned devices in the workplace. This decreased to 59 percent of respondents in this year's study. Only 21 percent of respondents believe company assigned mobile devices will increase.

Figure 12. The change in technologies over the next 12 to 24 months
Substantial increase and increase response combined



What trends will organizations deploy to deal with endpoint risk? Virtually all organizations (95 percent of respondents) will evolve toward a more “detect and respond” orientation from one that is focused on prevention. Seventy percent of respondents say their organizations are using or planning to use in two years or more the use of “big data” to enhance endpoint security, as shown in Figure 13. Sixty-four percent of respondents say they have added or plan to add a threat intelligence component to its security stack.

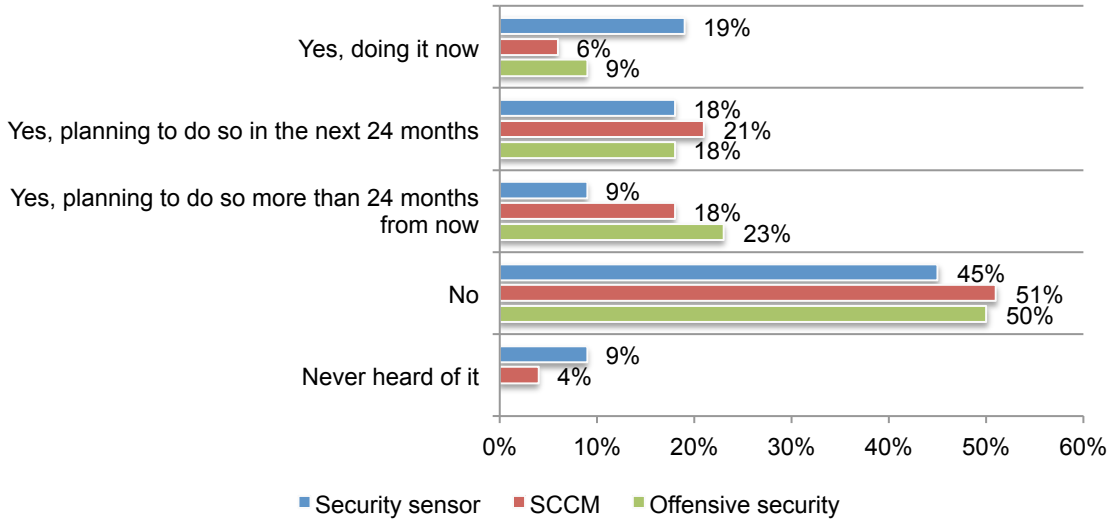
Figure 13. Use of threat intelligence, detect and respond and big data over the next 24 months or longer



Another popular trend is the notion of the endpoint as a security sensor. In other words, where state or context data collected at the endpoint is used to determine if it has been or is being compromised. Figure 14 reveals that 46 percent or respondents say this is something their organizations are doing it now or are planning to introduce (19 percent + 18 percent + 9 percent).

Of lesser importance is the need to develop an offensive security capability (i.e. discover who is behind an attack and then counterattack). Fifty percent of respondents are pursuing now or planning to pursue offensive security capability. Forty-five percent say their organizations are currently using or planning to use System Center Configuration Manager (SCCM).[1] In another finding, 43 percent of respondents say their organization has updated their security policies and tactical plans to keep pace with the emergence of destructive malware such as CryptoLocker and Shamoon.

Figure 14. Use of endpoint device as security sensor, SCCM and offensive security tactics over the next 24 months or more



[1] Officially called System Center Configuration Manager, or simply ConfigMgr, SCCM is a systems management software product by Microsoft for managing large groups of computers running Windows, Windows Embedded, Mac OS X, Linux or UNIX, as well as various mobile operating systems such as Windows Phone, Symbian, iOS and Android. SCCM provides remote control, patch management, software distribution, operating system deployment, network access protection and hardware and software inventory.

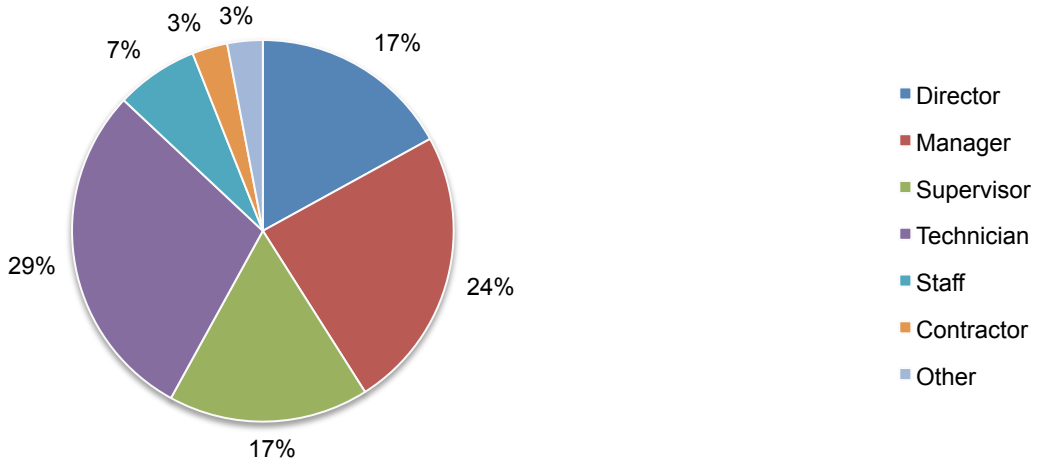
Part 3. Methods

A sampling frame composed of 18,664 IT and IT security practitioners located in the United States and are involved in endpoint security were selected for participation in this survey. As shown in the Table 1, 902 respondents completed the survey. Screening removed 199 surveys. The final sample was 703 surveys (or a 3.8 percent response rate).

Table 1. Sample response	Freq	Pct%
Total sampling frame	18,664	100.0%
Total returns	902	4.8%
Rejected and screened surveys	199	1.1%
Final sample	703	3.8%

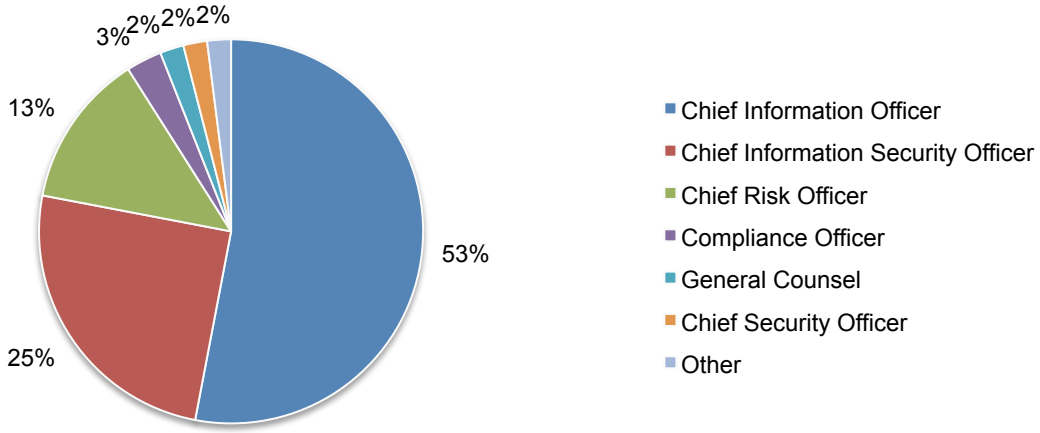
Pie chart 1 reports the current position or organizational level of respondents. By design, 58 percent of respondents reported their current position is at or above the supervisory level.

Pie Chart 1. Current position or organizational level



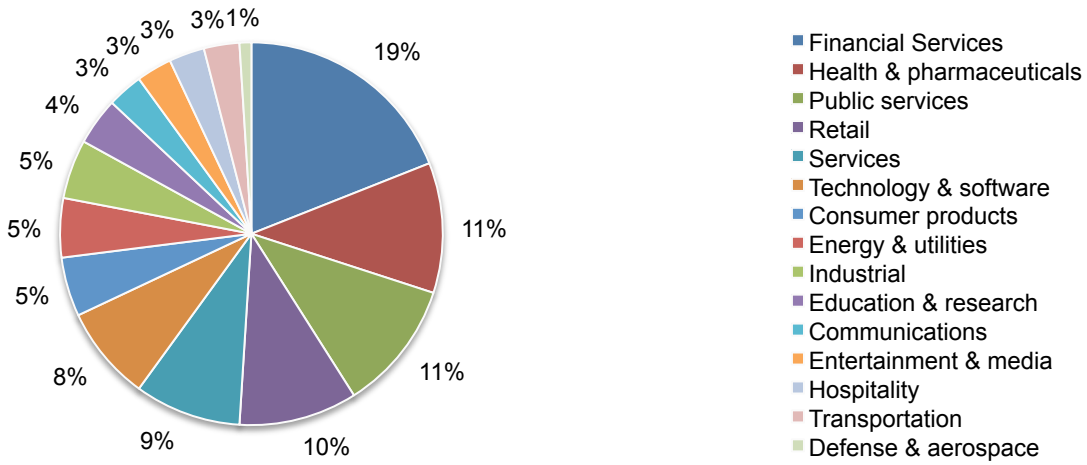
According to Pie Chart 2, more than half of the respondents (53 percent) report to the chief information officer. Another 25 percent responded they report to the chief information security officer.

Pie Chart 2. Primary Person respondent or IT security leader reports to



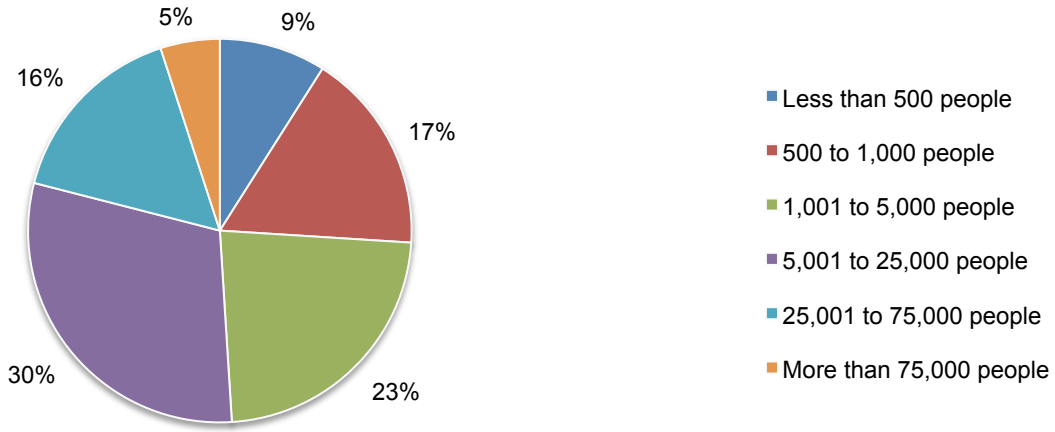
Pie Chart 3 reports the primary industry classification of respondents' organizations. This chart identifies financial services (19 percent) as the largest segment, followed by health and pharmaceuticals (11 percent) and public sector (11 percent).

Pie Chart 3. Primary industry classification



According to Pie Chart 4, 74 percent of the respondents are from organizations with a global headcount of over 1,000 employees.

Pie Chart 4. Worldwide headcount of the organization



Part 4. 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

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in November 2014

Survey response	FY 2014	FY 2013	FY 2012	FY 2011	FY 2010
Total sampling frame	18,664	19,001	17,744	18,988	11,890
Rejected and screened surveys	199	218	252	223	218
Final sample	703	676	671	688	564
Response rate	3.8%	3.6%	3.8%	3.6%	4.7%

Part 1. Screening					
S1. What best describes your level of involvement in endpoint security within your organization?	FY 2014	FY 2013	FY 2012	FY 2011	FY 2010
None (stop)	0%	0%	0%	0%	0%
Low (stop)	0%	0%	0%	0%	0%
Moderate	10%	11%	9%	10%	11%
Significant	54%	55%	54%	50%	56%
Very significant	36%	34%	33%	33%	28%
Total	100%	100%	100%	100%	100%

S2. How many network-connected mobile devices does your organization support?	FY 2014	FY 2013	FY 2012	FY 2011	FY 2010
Less than 100 (stop)	0%	0%	1%	1%	1%
100 or more connected devices	100%	100%	96%	95%	96%
Total	100%	100%	97%	96%	97%

S3. What best describes your role within your organization's IT department?	FY 2014	FY 2013	FY 2012	FY 2011	FY 2010
IT management	26%	24%	24%	21%	24%
IT operations	21%	23%	23%	23%	23%
Data administration	9%	10%	11%	13%	11%
IT compliance	8%	10%	9%	9%	9%
IT security	32%	29%	27%	29%	27%
Applications development	4%	5%	5%	5%	5%
I'm not involved in my organization's IT function (stop)	0%	0%	0%	0%	0%
Total	100%	100%	100%	100%	100%

Part 2: Attributions			
Q1. We have ample resources to minimize IT endpoint risk throughout our organization.	FY 2014	FY 2013	FY 2012
Strongly agree	15%	16%	14%
Agree	19%	16%	19%
Unsure	21%	28%	33%
Disagree	34%	30%	26%
Strongly disagree	11%	10%	8%
Total	100%	100%	100%

Q2. The use of employee-owned mobile devices (a.k.a. BYOD) has **significantly** increased endpoint risk throughout or organization.	**FY 2014**
Strongly agree	38%
Agree	30%
Unsure	17%
Disagree	10%
Strongly disagree	5%
Total	100%

Q3. The use of commercial cloud applications (such as Dropbox, Box.net, GoogleDocs, etc.) has **significantly** increased endpoint risk throughout or organization.	**FY 2014**
Strongly agree	41%
Agree	32%
Unsure	14%
Disagree	8%
Strongly disagree	5%
Total	100%

Q4. Employees operating from home offices and other offsite locations (a.k.a. mobile workforce) have **significantly** increased endpoint risk throughout or organization.	**FY 2014**
Strongly agree	35%
Agree	28%
Unsure	17%
Disagree	15%
Strongly disagree	5%
Total	100%

Q5. Our IT department cannot keep up with employee demand for greater support and better mobile device connectivity.	**FY 2014**
Strongly agree	36%
Agree	32%
Unsure	13%
Disagree	12%
Strongly disagree	7%
Total	100%

Q6. Our approach to endpoint security takes into account the Internet of Things.	**FY 2014**
Strongly agree	15%
Agree	18%
Unsure	33%
Disagree	23%
Strongly disagree	11%
Total	100%

Q7. Our endpoint security policies are difficult to enforce.	FY 2014
Strongly agree	39%
Agree	31%
Unsure	15%
Disagree	10%
Strongly disagree	5%
Total	100%

Part 3: General questions		
Q8a. In the past 24 months, has it become more difficult to manage endpoint risk?	FY 2014	FY 2013
Yes	69%	71%
No	31%	29%
Total	100%	100%

Q8b. If yes, what are the **top five** (5) biggest threats to endpoint security in your organization?	FY 2014	FY 2013
Malware infections are more stealthy and difficult to detect	45%	32%
The number of employees and others using multiple mobile devices in the workplace has increased	65%	60%
The number of insecure mobile devices used in the workplace has increased significantly	45%	33%
There are more personal devices connected to the network (BYOD)	68%	51%
Employees' use of commercial cloud applications in the workplace *	66%	
More employees are working offsite and using insecure WiFi connections	38%	16%
Emergence of new mobile technologies such as Google Glasses, Apple Watch and others *	5%	
Emergence of the Internet of Things (IoT)*	13%	
Negligent or careless employees who do not follow security policies *	78%	
Other	1%	0%
Total	424%	192%

* This response not available in all FY's, two choices permitted in FY2013

Q10a. In the past 24 months, has endpoint security become a more important priority of your organization's overall IT security strategy?	FY 2014	FY 2013
Yes	68%	65%
No	32%	35%
Total	100%	100%

Q10b. If yes, why has endpoint security become more important over the past 24 months?	FY 2014
Change in endpoint security risk profile	23%
Change in management direction and philosophy	18%
Increased use and variety of mobile devices connected to our network	67%
Uncertainty about how new mobile technologies and the Internet of Things such impact security	49%
Increase in the mobile workforce	45%
Other	2%
Total	204%

Q10c. If no, why has endpoint security become less important over the past 24 months?	FY 2014
Change in endpoint security risk profile	42%
Change in management direction and philosophy	46%
Increased reliance on network and perimeter security controls	28%
Shift in IT and/or security priorities	39%
Lack of effective tools/solutions	26%
Diminished resources	19%
Other	1%
Total	201%

Q11. Which of the following statements best describes your endpoint security strategy?	FY 2014
Our endpoint strategy focuses more on securing the data and less on the device.	55%
Our endpoint strategy focuses more on securing the device and less on the data.	15%
Our endpoint strategy focuses equally on securing the device and data.	30%
Total	100%

Q12. Does your organization's approach to endpoint security include the tagging, securing and management of data that resides on the device?	FY 2014
Yes	44%
No	56%
Total	100%

Q13. Does your organization's approach to endpoint security include the tagging, securing and management of data that is accessed by the device, but resides on a public cloud?	FY 2014
Yes	26%
No	74%
Total	100%

Q14a. How will your organization's IT security budget for 2015 compare to 2014?	FY 2014	FY 2013
Significantly increased	12%	10%
Increased	33%	33%
Stayed the same	40%	43%
Decreased	10%	11%
Significantly decreased	2%	3%
Unsure*	3%	0%
Total	100%	100%

This response not available in all FY's

Q14b. If the IT security budget for 2015 is increased, what is the approximate percentage increase?	FY 2014	FY 2013
5 percent or less	20%	22%
5 to 10 percent	33%	35%
11 to 20 percent	28%	25%
21 to 30 percent	10%	11%
31 to 40 percent	6%	5%
More than 50 percent	3%	2%
Total	100%	100%

Q15a. Following are 5 areas of IT security risks. Please allocate the amount of spending earmarked for each risk listed in the table below. Use all 100 points in the table to allocate your response **today**.	FY 2014
Network	40
Application	15
Data	21
Endpoint	13
Human	11
Total points	100

Q15b. Following are 5 areas of IT security risks. Please allocate the amount of spending earmarked for each risk listed in the table below. Use all 100 points in the table to allocate your response **12 months from now**.	FY 2014
Network	32
Application	19
Data	25
Endpoint	13
Human	11
Total points	100

Q16. How has the **frequency** of malware incidents changed over the past year within your organization?	FY 2014	FY 2013	FY 2012	FY 2011	FY 2010
Significantly increased	39%	44%	37%	31%	26%
Increased	15%	15%	18%	22%	21%
Stayed the same	26%	19%	22%	25%	25%
No, there has been a slight decrease*		8%			
Decreased	9%		8%	8%	9%
Significantly decreased	1%	2%			
Unsure	10%	12%	15%	14%	17%
Total	100%	100%	100%	100%	98%

This response not available in all FY's

Q17. How has the **severity** of malware incidents changed over the past year within your organization?	FY 2014
Significantly increased	50%
Increased	19%
Stayed the same	16%
Slight decrease*	4%
Decreased*	4%
Significantly decreased*	0%
Unsure	7%
Total	100%

This response not available in all FY's

Q18. With your current enabling technologies, processes and in-house expertise, what percentage of attacks to your organization's endpoints can be realistically stopped?	FY 2014
0 to 10%	2%
11 to 20%	0%
21 to 30%	2%
31 to 40%	6%
41 to 50%	5%
51 to 60%	13%
61 to 70%	15%
71 to 80%	13%
81 to 90%	13%
91 to 100%	31%
Total	100%
Extrapolated value	72%

Q19. Where is the **one biggest gap** in your organization's ability to stop attacks to endpoints?	FY 2014
Lack of in-house expertise	29%
Lack of enabling technologies	21%
Lack of governance and control processes	50%
Total	100%

Q20. Which of these types of incidents or compromises are you seeing **frequently** in your organization's IT networks? Please check all that apply.	FY 2014	FY 2013	FY 2012	FY 2011	FY 2010
Zero day attacks	46%	36%	31%	29%	30%
Exploit of existing software vulnerability less than 3 months old	30%	35%	28%	33%	30%
Exploit of existing software vulnerability greater than 3 months old	24%	26%	26%	31%	26%
SQL injection	31%	28%	29%	32%	35%
Spyware	35%	40%	45%	49%	57%
Botnet attacks	35%	49%	55%	56%	64%
Clickjacking	46%	46%	43%	37%	25%
Rootkits	65%	67%	65%	63%	57%
General malware*		80%	86%	89%	92%
DDoS*	29%				
Web-borne malware attacks	80%	74%	79%	83%	75%
Advanced persistent threats (APT) / targeted attacks	65%	59%	54%	36%	
Spear phishing	55%	48%			
Hacktivism*			41%	33%	
Other (please specify)	3%	4%	5%	6%	13%
Total	544%	592%	587%	577%	504%

*This response not available in all FY's

Q21. Do you believe mobile endpoints have been the target of malware over the past 12 months?	FY 2014	FY 2013
Yes	75%	68%
No	18%	22%
Unsure	7%	10%
Total	100%	100%

Q22. Where are you seeing the greatest rise of potential IT security risk within your IT environment? Please choose only your **top five** choices.	FY 2014	FY 2013	FY 2012	FY 2011	FY 2010*
Our server environment	17%	17%	19%	29%	32%
Our data centers	6%	7%	6%	12%	14%
Within operating systems (vulnerabilities)	9%	8%	8%	10%	11%
Across third party applications (vulnerabilities)	69%	66%	67%	56%	45%
Our PC desktop/laptop	38%	43%	45%	41%	44%
Mobile devices such as smart phones (Blackberry, iPhone, IPad, Android)	80%	75%	73%	48%	9%
Removable media (USB sticks) and/or media (CDs, DVDs)	29%	35%	39%	42%	10%
Network infrastructure environment (gateway to endpoint)	12%	12%	10%	14%	11%
Malicious insider risk	30%	15%	15%	16%	
Negligent insider risk	41%	40%	44%	43%	
Negligent third party risk (partner, vendors, customers, etc.)	28%	33%			
Cloud computing infrastructure and providers	32%	36%	41%	43%	18%
Virtual computing environments (servers, endpoints)	10%	9%	19%	28%	20%
Mobile/remote employees	42%	45%	53%	49%	44%
Lack of system connectivity/visibility	35%	31%	25%	29%	
Lack of organizational alignment	22%	28%	36%	39%	
Total	500%	500%	500%	499%	299%

*Top 3 choices in the 2010 survey

Q23. Please estimate how the use of each one of the following technologies will change in your organization over the next 12 to 24 months.	
Q23a. Company assigned mobile devices / smart phones and tablets	FY 2014
Substantial increase	10%
Increase	11%
No change	26%
Decrease	35%
Substantial decrease	15%
Not used	3%
Total	100%

Q23b. Employee-owned mobile devices / smart phones and tablets*	FY 2014	FY 2013	FY 2012
Substantial increase	33%	44%	40%
Increase	26%	35%	35%
No change	15%	3%	3%
Decrease	9%	4%	5%
Substantial decrease	5%	3%	3%
Not used	12%	11%	14%
Total	100%	100%	100%

* Q11from 2013 survey did not specify employee-owned

Q23c. Virtualized server environment*	FY 2014
Substantial increase	12%
Increase	27%
No change	20%
Decrease	13%
Substantial decrease	8%
Not used	20%
Total	100%

*Virtualized environments (servers & desktops) combined in previous FY's

Q23d. Virtualized desktop environment*	FY 2014
Substantial increase	8%
Increase	15%
No change	22%
Decrease	5%
Substantial decrease	1%
Not used	49%
Total	100%

*Virtualized environments (servers & desktops) combined in previous FY's

Q23e. Employee use of commercial cloud computing services *	FY 2014	FY 2013	FY 2012
Substantial increase	38%	38%	32%
Increase	33%	32%	31%
No change	23%	18%	20%
Decrease	6%	7%	6%
Substantial decrease	0%	2%	5%
Not used	0%	3%	6%
Total	100%	100%	100%

* FY 2013 wording slightly different - Use of 3rd party (non-company) cloud computing

Q24. 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 five (5)** choices.	FY 2014	FY 2013	FY 2012	FY 2011	FY 2010
Microsoft OS/Applications	34%	37%	44%	49%	57%
Apple/Mac OS	29%	30%	30%	24%	15%
Apple apps (Air, QuickTime, iTunes, etc.)	33%	29%	28%	20%	14%
Adobe (Acrobat, Flash Player Reader etc.)	62%	60%	55%	50%	54%
Oracle Java JRE	54%	20%	15%	22%	10%
Browsers (e.g., Chrome, Firefox, Safari, IE Opera, etc.)*	16%	3%	3%	6%	2%
Cloud-based productivity apps (e.g., Google Docs, Office 365, Evernote, etc.)	46%	50%	55%	47%	46%
Other third-party apps (e.g., WinZip, VLC, VMware, VNC, etc.)	40%	56%	69%	82%	95%
Uncontrolled use of private cloud storage (e.g., Box, Dropbox, iCloud, etc.)	43%	15%			
Uncontrolled use of removal storage devices or media (e.g., USB flash drives, CDs/DVDs, etc.)	18%				
Other (please specify)	2%	0%	0%	1%	4%
Total	377%	300%	299%	299%	298%

* Q23 from the FY2013 survey listed Firefox as a single option

Q25. Does your organization have an integrated endpoint security suite (vulnerability assessment, device control, anti-virus, anti-malware, patch management or other capabilities)?	FY 2014	FY 2013	FY 2012	FY 2011
Yes	42%	38%	35%	33%
No, but our organization expects to have an endpoint security suite within the next 12-24 months	47%	49%	48%	46%
No	11%	13%	17%	21%
Total	100%	100%	100%	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.	FY 2014	FY 2013	FY 2012	FY 2011	FY 2010
1 to 2	14%	16%	19%	18%	
3 to 5	19%	23%	21%	23%	
6 to 10	41%	38%	41%	39%	
More than 10	21%	18%	13%	10%	
Cannot determine	5%	5%	6%	10%	
Total	100%	100%	100%	100%	
Extrapolated value	7.03	6.69	6.35	6.12	

Q27. On a typical day, how many different or distinct software management **user interfaces or consoles** does your organization use to manage endpoint operations and security functions? Please provide your best estimate.	FY 2014	FY 2013	FY 2012	FY 2011	FY 2010
1 to 2	12%	14%	19%	23%	
3 to 5	23%	25%	25%	29%	
6 to 10	43%	38%	35%	30%	
More than 10	17%	14%	11%	9%	
Cannot determine	5%	9%	10%	9%	
Total	100%	100%	100%	100%	
Extrapolated value	6.81	6.52	6.01	5.48	

Part 4. Predictions & Trends

Q28. The notion of the endpoint as a security sensor – that is, where state or context data collected at the endpoint is used to determine if it has been or is being compromised – is gaining in popularity. Is this something your organization is doing or planning to do?	**FY 2014**
Yes, doing it now	19%
Yes, planning to do so in the next 24 months	18%
Yes, planning to do so more than 24 months from now	9%
No	45%
Never heard of it	9%
Total	100%

Q29. Has your organization added or plan to add, a threat intelligence component to its security stack?	**FY 2014**
Yes, doing it now	33%
Yes, planning to do so in the next 24 months	22%
Yes, planning to do so more than 24 months from now	9%
No	36%
Total	100%

Q30. Traditional endpoint defense has focused on prevention, but there is a growing movement towards a so-called "detect and respond" orientation. Is your organization moving towards this paradigm?	**FY 2014**
Yes, doing it now	44%
Yes, planning to do so in the next 24 months	30%
Yes, planning to do so more than 24 months from now	21%
No	5%
Never heard of it	0%
Total	100%

Q31. Is your organization currently using or planning to use SCCM as its main systems management tool?	**FY 2014**
Yes, using it now	6%
Yes, planning to use in the next 24 months	21%
Yes, planning to use more than 24 months from now	18%
No	51%
Never heard of it	4%
Total	100%

Q32. A growing trend in cyber attacks has been the unleashing of so-called "destructive malware" (such as Cryptolocker, Shamoon, etc.). Has your organization's tactical plans and policies kept up with this development?	FY 2014
Yes	43%
No	53%
Unsure	4%
Total	100%

Q33. A growing trend has been the use of co-called "big data" as a tool to enhance endpoint and database security. Is your organization using or planning to use big data as part of its cyber defense?	FY 2014
Yes, using it now	11%
Yes, planning to use in the next 24 months	41%
Yes, planning to use more than 24 months from now	18%
No	30%
Total	100%

Q34. The cyber security community has been discussing the need to develop an offensive security capability (i.e., discover who is behind an attack and then counterattack). Is this something your organization is or will be pursuing?	FY 2014
Yes, pursuing now	9%
Yes, planning to pursue in the next 24 months	18%
Yes, planning to pursue more than 24 months from now	23%
No	50%
Total	100%

Part 5. Organizational Characteristics & Demographics					
D1. What organizational level best describes your current position?	FY 2014	FY 2013	FY 2012	FY 2011	FY 2010
Senior Executive	1%	1%	0%	1%	2%
Vice President	1%	2%	2%	1%	1%
Director	17%	18%	19%	22%	23%
Manager	24%	25%	26%	23%	25%
Supervisor	17%	19%	19%	18%	19%
Technician	29%	25%	23%	20%	16%
Staff	7%	8%	7%	10%	9%
Contractor	3%	2%	3%	4%	3%
Other	1%	0%	1%	1%	2%
Total	100%	100%	100%	100%	100%

D2. Check the **Primary Person** you or your IT security leader reports to within the organization.	FY 2014	FY 2013	FY 2012	FY 2011	FY 2010
CEO/Executive Committee	1%	0%	0%	0%	1%
Chief Financial Officer (CFO)	1%	2%	1%	1%	2%
General Counsel	2%	1%	3%	2%	2%
Chief Information Officer (CIO)	53%	53%	54%	53%	50%
Chief Information Security Officer (CISO)	25%	25%	23%	23%	21%
Compliance Officer	3%	4%	6%	8%	9%
Human Resources VP	0%	0%	0%	0%	2%
Chief Security Officer (CSO)	2%	2%	4%	5%	6%
Chief Risk Officer (CRO)	13%	12%	9%	8%	5%
Other	0%	1%	0%	0%	2%
Total	100%	100%	100%	100%	100%

D3. What industry best describes your organization's **primary** industry focus?	FY 2014	FY 2013	FY 2012	FY 2011	FY 2010
Agriculture & food services	0%	1%	2%	1%	2%
Communications	3%	2%	3%	5%	4%
Consumer products	5%	4%	3%	2%	3%
Defense & aerospace	1%	1%	2%	3%	3%
Education & research	4%	3%	5%	6%	5%
Energy & utilities	5%	5%	4%	3%	2%
Entertainment & media	3%	4%	3%	4%	3%
Financial Services	19%	21%	20%	18%	19%
Health & pharmaceuticals	11%	12%	12%	10%	11%
Hospitality	3%	3%	5%	4%	4%
Industrial	5%	1%	5%	4%	5%
Public services	11%	12%	10%	12%	13%
Retail	10%	9%	9%	8%	7%
Services	9%	11%	8%	9%	8%
Technology & software	8%	8%	7%	8%	6%
Transportation	3%	3%	2%	3%	5%
Total	100%	100%	100%	100%	100%

D4. Where are your employees located? Check all that apply.	FY 2014	FY 2013	FY 2012	FY 2011	FY 2010
United States	100%	100%	100%	100%	100%
Canada	65%	63%	65%	69%	63%
Europe	70%	72%	71%	70%	68%
Middle East	31%	28%	26%	23%	19%
Asia-Pacific	54%	55%	50%	45%	41%
Latin America (including Mexico)	39%	36%	32%	31%	29%
Africa	5%	6%	5%	7%	8%

D5. What is the worldwide headcount of your organization?	FY 2014	FY 2013	FY 2012	FY 2011	FY 2010
Less than 500 people	9%	8%	7%	5%	6%
500 to 1,000 people	17%	15%	16%	16%	13%
1,001 to 5,000 people	23%	20%	21%	22%	19%
5,001 to 25,000 people	30%	34%	33%	31%	32%
25,001 to 75,000 people	16%	20%	19%	21%	21%
More than 75,000 people	5%	3%	4%	5%	9%
Total	100%	100%	100%	100%	100%
Extrapolated value	17,340	18,125	18,268	19,750	22,832

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.