2013 State of the Endpoint

Sponsored by Lumension

Independently conducted by Ponemon Institute LLC

Publication Date: December 2012

Ponemon Institute© Research Report

2013 State of the Endpoint

Ponemon Institute: December 2012

Part 1. Introduction

We are pleased to present the results of the *2013 State of the Endpoint* study sponsored by Lumension® and conducted by Ponemon Institute. Since 2010, we have tracked endpoint risk in organizations, the resources to address the risk and the technologies deployed to manage threats.

This study reveals that the state of endpoint risk is not improving. One of the top concerns is the proliferation of personally owned mobile devices in the workplace such as smart phones and iPads. In fact, 80 percent of those surveyed say laptops and other mobile data-bearing devices pose a significant security risk to their organization's networks or enterprise systems because they are not secure. Yet, only 13 percent say they use stricter security standards for employees' personal devices rather than for corporate-owned devices.

Malware attacks are increasing and are having a significant impact on IT operating expenses. Advanced persistent threats and hactivism pose the biggest headache to IT security pros. However, only 12 percent of those surveyed say current anti-virus/anti-malware technology is very effective in protecting their IT endpoints from today's malware risk and only 5 percent report a planned increase in the use of the technology. This comfort level with standalone anti-virus remains virtually unchanged since the 2010 study.

In this year's study, we surveyed 671 IT and IT security practitioners. Seventy-seven percent are employed in organizations with a headcount of more than 1,000. Sixty-four percent are at the supervisor level or higher.

Some of the most noteworthy findings include the following:

- Eighty percent of respondents believe laptops and other mobile data-bearing devices such as smart phones pose a significant security risk to their organization's networks or enterprise systems because they are not secure.

- Third-party application risk increases. Google Docs and Adobe, including Flash and Adobe Reader are the applications of greatest concern.

- Malware attacks are increasing. Fifty-eight percent of respondents say their organizations have more than 25 malware attempts or incidents each month and another 20 percent are unsure.

- The biggest headaches for IT pros are advanced persistent threats and hacktivism.

- Eighty-five percent of respondents are very concerned or increasingly concerned about Mac malware infections. This percentage remains unchanged from 2011.

- Higher IT operating expenses are blamed on malware.

- The lack of an enforceable centralized cloud security policy is putting unstructured confidential information at risk. Forty-five percent of respondents say their organization does not enforce employees' use of private clouds and 14 percent are unsure.

- Controlling access privileges is often non-existent in organizations represented in this study. Sixty percent do allow local admin privileges to part of their user environment or to the entire user environment.

Part 2. Key Findings

In this report, we organize the findings according to the following six topics:

- The endpoint threat landscape
- Mobility is an IT security headache
- The malware threat
- Barriers to achieving optimal endpoint security
- Current and future technologies
- Cloud computing and endpoint security

When feasible, we compare the findings for all three years the study was conducted.

1. The endpoint threat landscape

The greatest rise in IT security risk is occurring across mobile devices and third-party applications. According to respondents, the risks caused by mobile devices such as smart phones and removable media and vulnerabilities in third-party applications have gained significantly since 2010, as shown in Figure 1. In 2010, only 9 percent of respondents said mobile devices was a rising threat. This year 73 percent see it as one of the greatest risks within the IT environment. Other risks that have become more of a headache since 2010 are the use of cloud computing infrastructure and providers and the prevalence of mobile/remote employees.

Figure 1. IT security risks on the rise
Three choices permitted in 2010 and 5 choices permitted in 2011 and 2012

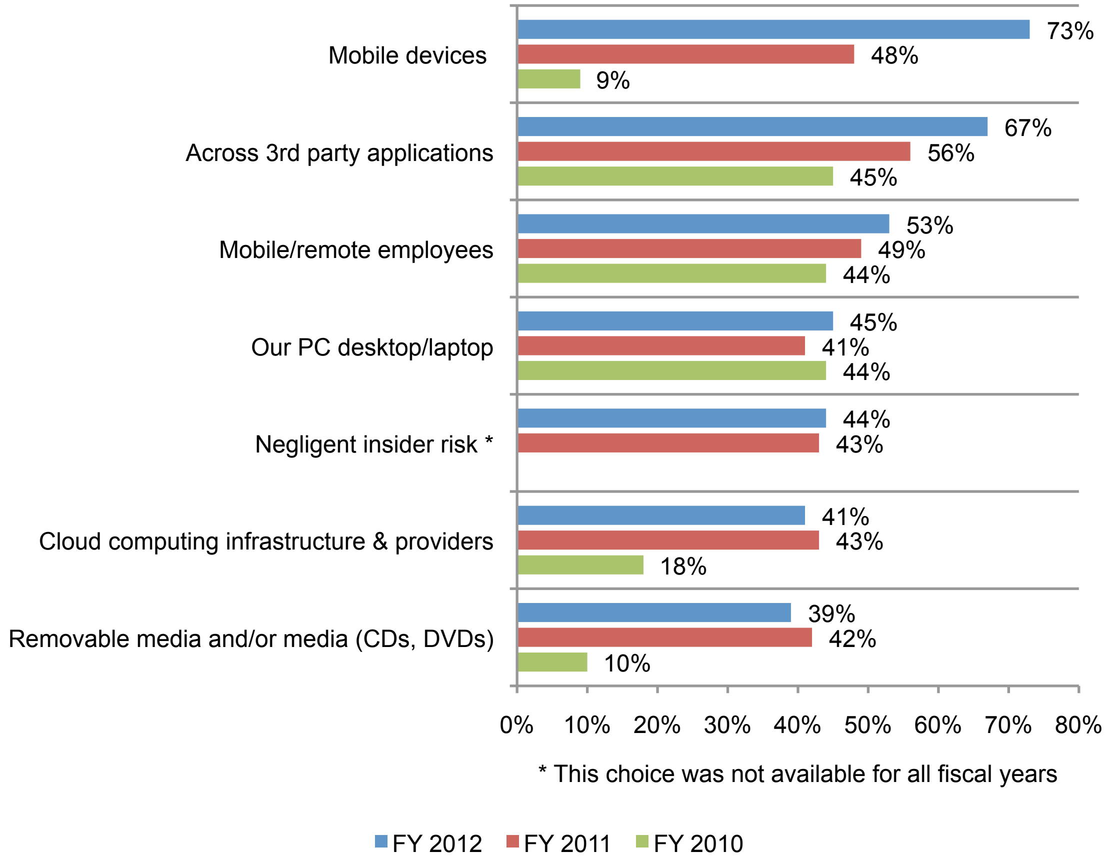
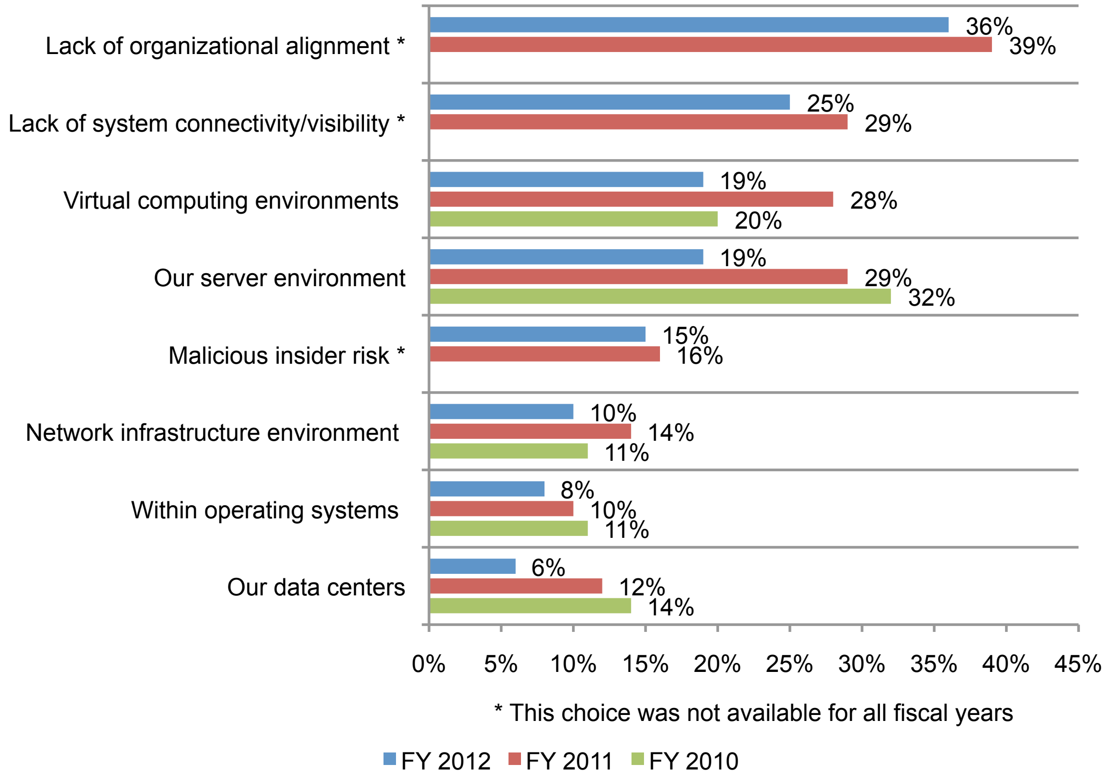


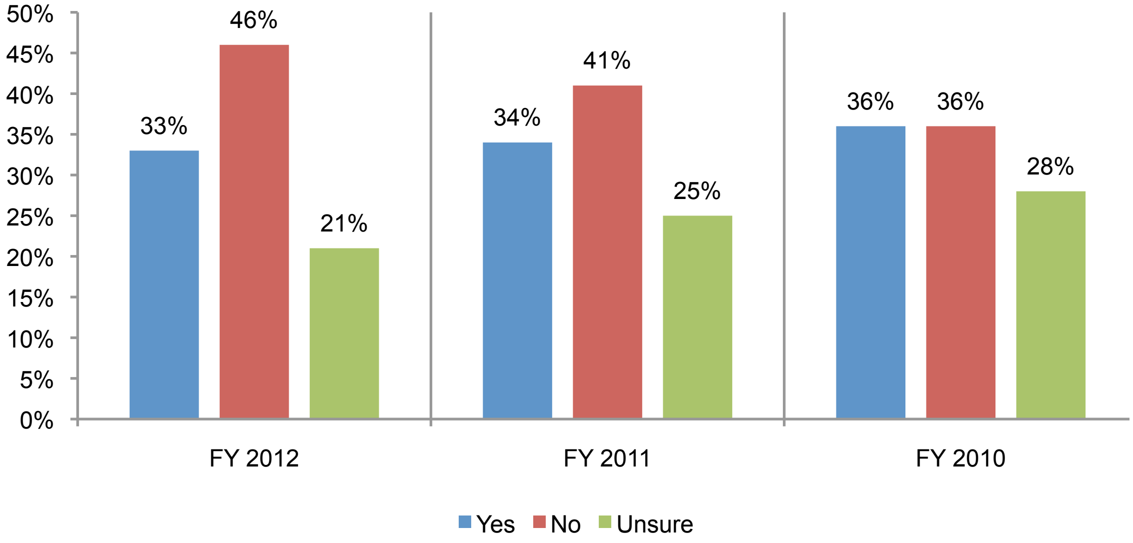
Figure 2 reveals that since 2010 certain worries about risks have declined. These are in the server environment, data centers and within operating systems. Other risks such as malicious insiders have stayed about the same.

Figure 2. IT security risks believed to be decreasing or staying the same
Three choices permitted in 2010 and 5 choices permitted in 2011 and 2012



Confidence in network security continues to decline. As shown in Figure 3, 46 percent of respondents do not believe their IT network is more secure now than it was a year ago. This is a 10 percent increase from 2010.

Figure 3. Is your IT network more secure now than it was a year ago?



The smart phone and iPad risk grows. Figure 4 reveals that when asked what IT security risks are of most concern, the top choice is the increased use of mobile platforms such as smart phones and iPads. This is consistent with the finding that one of the greatest threats to the IT environment is the increased use of mobile devices. The second concern is advanced persistent threats (APTs). This concern has increased from 24 percent of respondents in 2010 to 36 percent of respondents in this year's study.

Figure 4. IT security risks of most concern since 2010
More than three choices permitted in 2010 and 3 choices permitted in 2011 and 2012

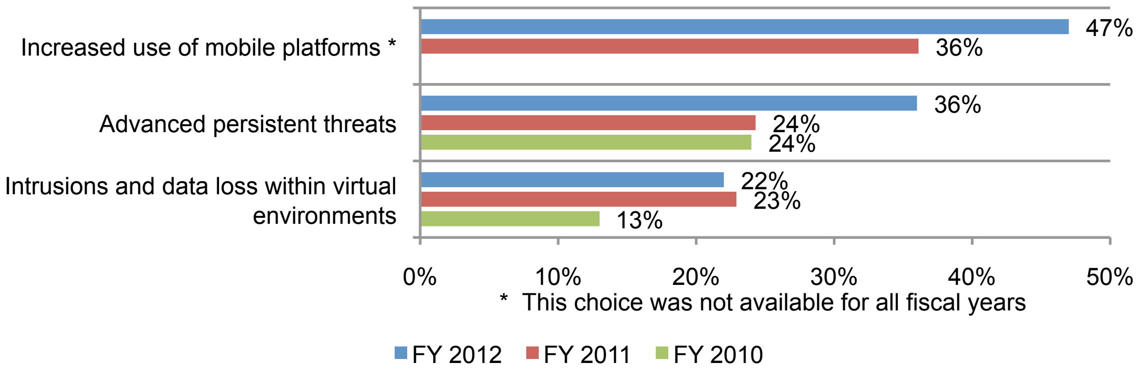
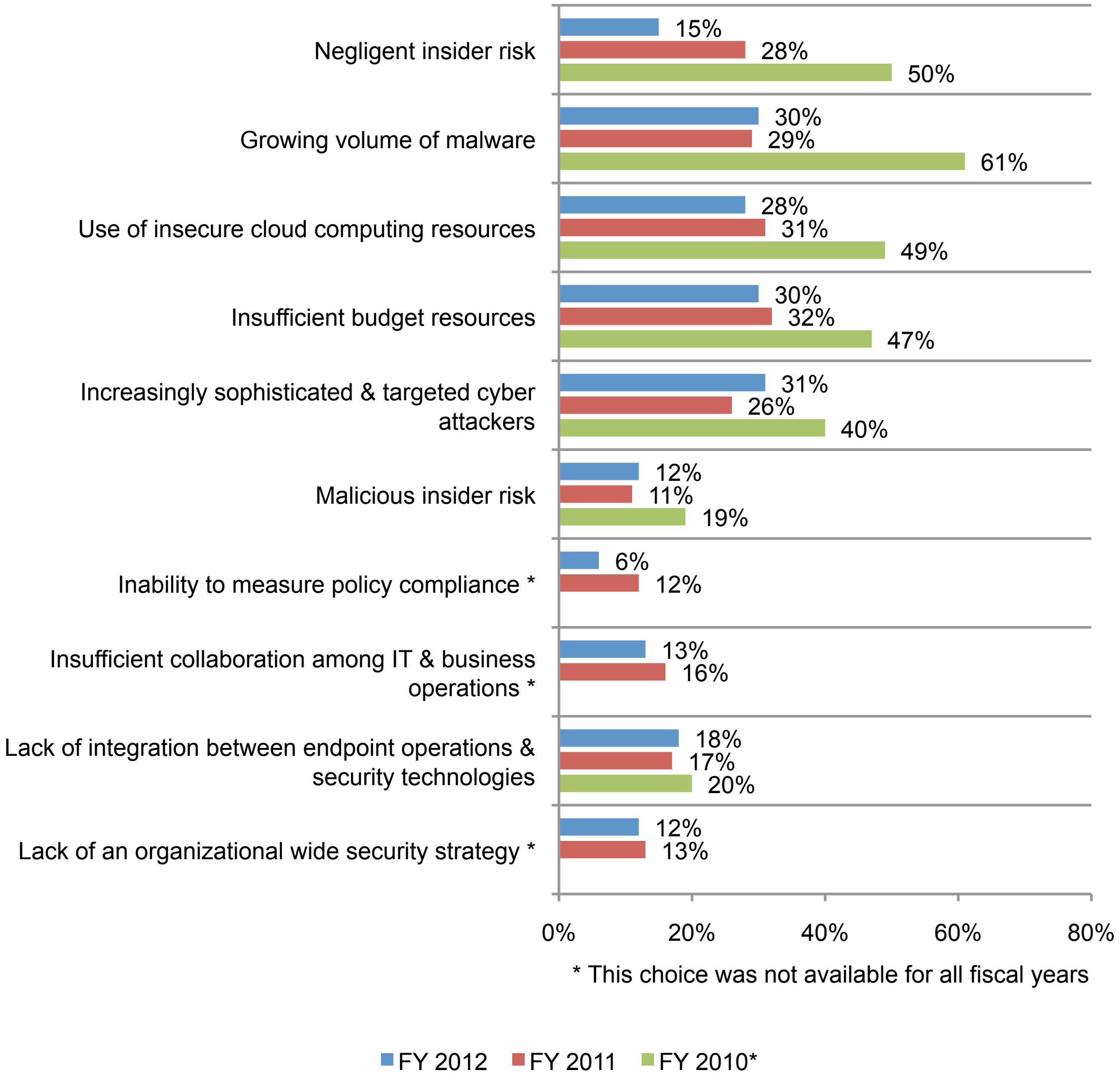


Figure 5 shows that concerns over certain risks have decreased since 2010. This may be attributed to the perception that they are not as pervasive or they are better able to reduce the threat.

For example, while respondents still worry about sophisticated and targeted cyber attackers this risk has declined. It is interesting to note that the negative insider risk has gone down significantly since 2010 as well as the growing volume of malware and use of insecure cloud computing resources.

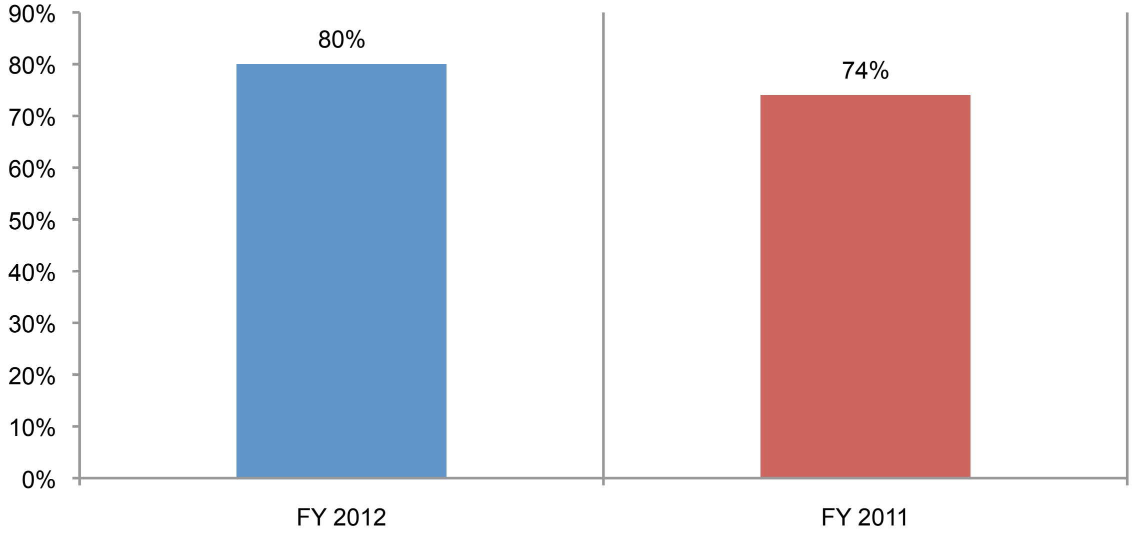
Figure 5. IT security risks that have declined or stayed the same
More than three choices permitted in 2010 and 3 choices permitted in 2011 and 2012



1. Mobility is an IT security headache

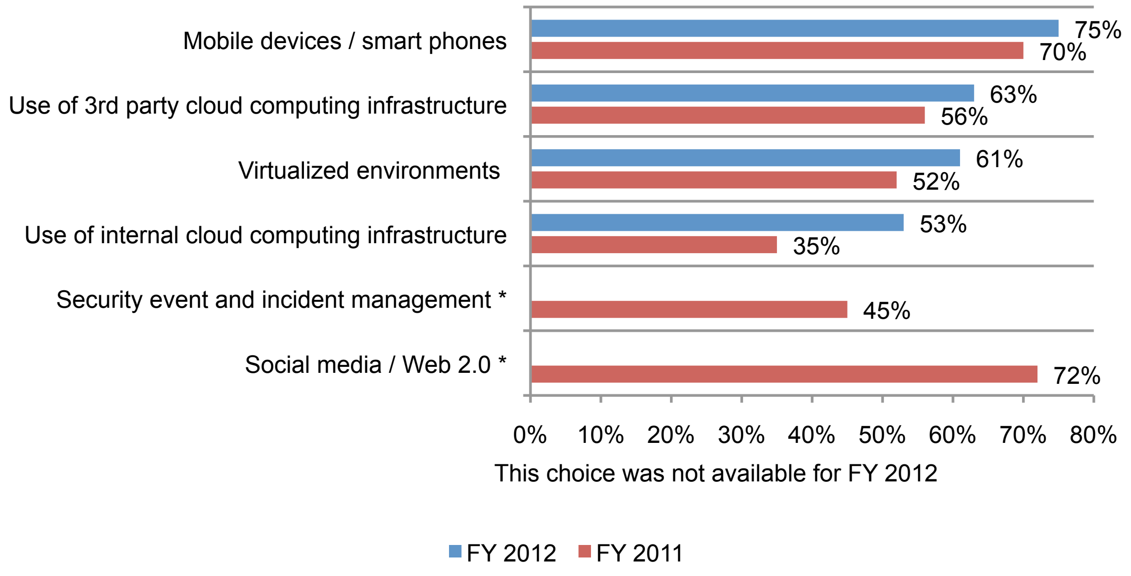
Mobility risks surge. Eighty percent believe laptops and other mobile data-bearing devices such as smart phones pose a significant security risk to their organization's networks or enterprise systems because they are not secure. As shown in Figure 6, this is an increase from 74 percent in 2011.

Figure 6. Mobile devices pose a significant security risk
Strongly agree and agree response combined



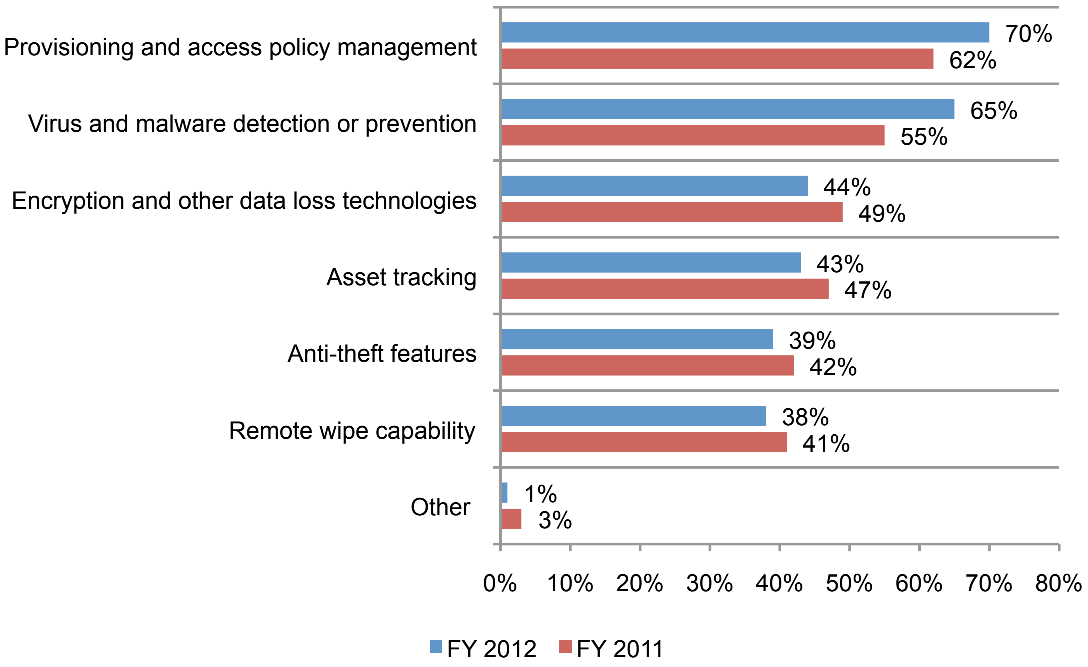
According to Figure 7, 75 percent say their organizations will have a substantial increase or increase in the use of mobile devices/smart phones. This is followed by increases in use of third party cloud computing infrastructures. When this was asked in 2011, the technology that was considered to increase the most was social media/Web 2.0.

Figure 7. Technologies expected to increase in the next 12 to 24 months
Substantial increase and increase response combined



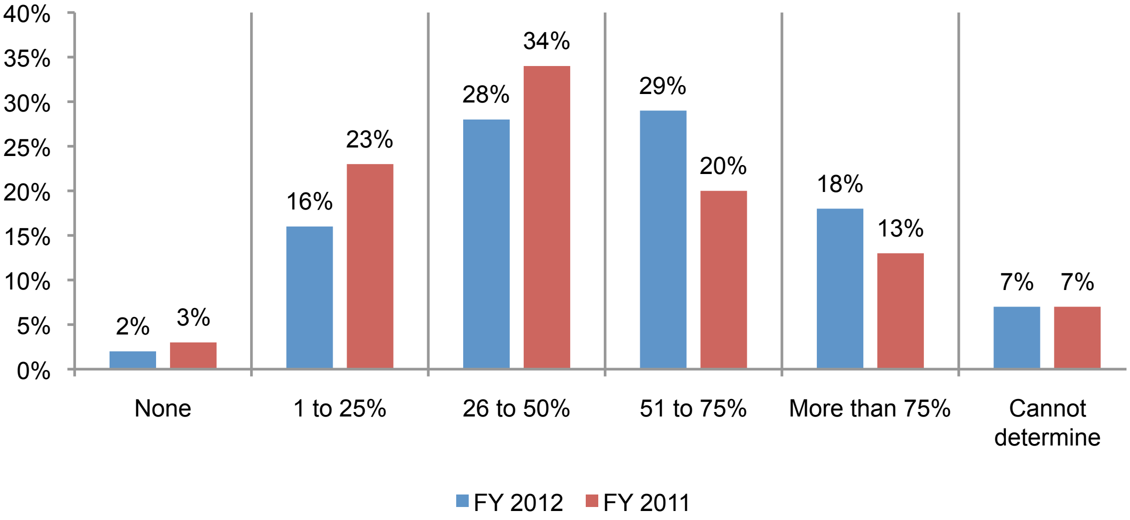
Thirty-seven percent report they will increase the use of mobile device technologies in 2013. Figure 8 shows that the three most important features for mobile device management are provisioning and access policy management, virus and malware detection or prevention and encryption and other data loss technologies.

Figure 8. Important mobile device management features
Three choices permitted



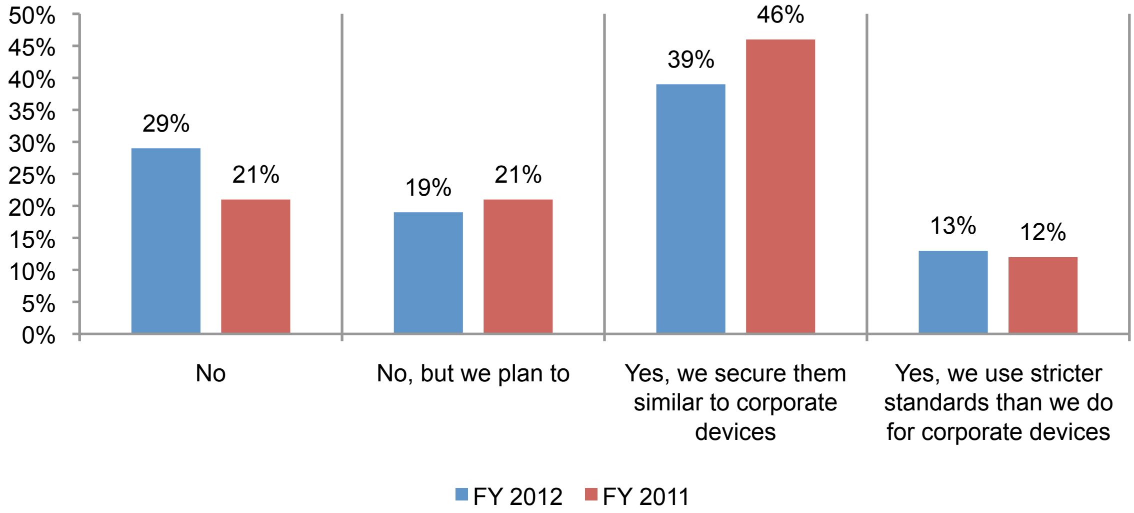
BYOD has increased significantly. According to Figure 9, 47 percent of respondents say that more than half of employees in their organizations are using their personal mobile devices in the workplace. This is an increase from 33 percent of respondents in 2011 who said more than half of respondents bring their own devices.

Figure 9. Personal mobile device use in the workplace



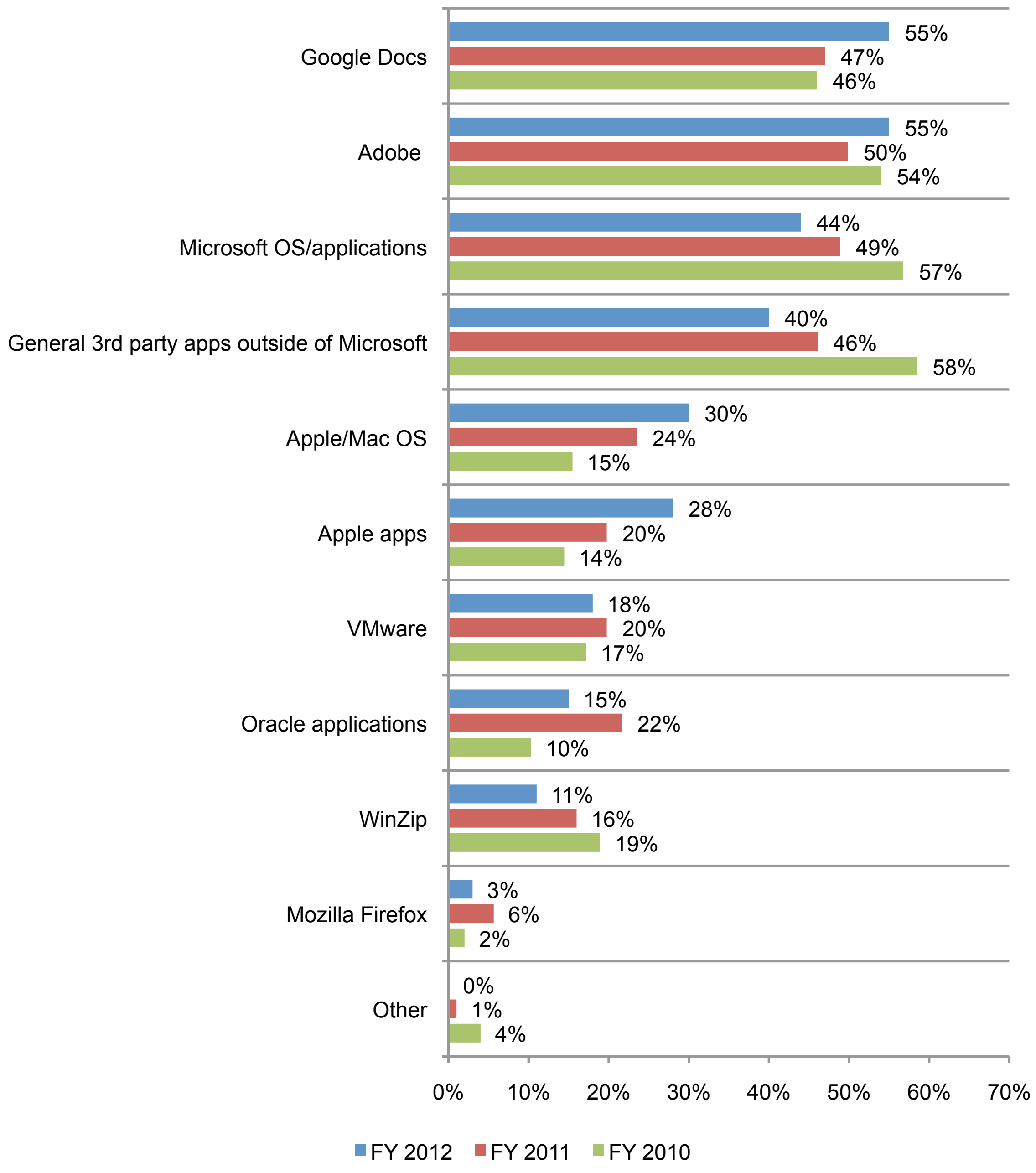
Further, only 13 percent say they use stricter standards for employee-owned mobile devices connected to their organization's networks than for corporate-owned devices, as shown in Figure 10. Twenty-nine percent of respondents say they do not take steps to secure employee-owned mobile devices, an increase from 21 percent in 2011.

Figure 10. Security policy for employee owned devices



Third-party application risk increases. Second to apprehension over mobile platforms is the potential for risk across third-party applications. According to Figure 11, Google Docs and Adobe, including Flash and Adobe Reader, are the applications of greatest concern to respondents. Worries about Apple/Mac OS have increased sharply since 2010. Applications that are less worrisome are general third-party applications as Oracle applications, WinZip and Mozilla Firefox.

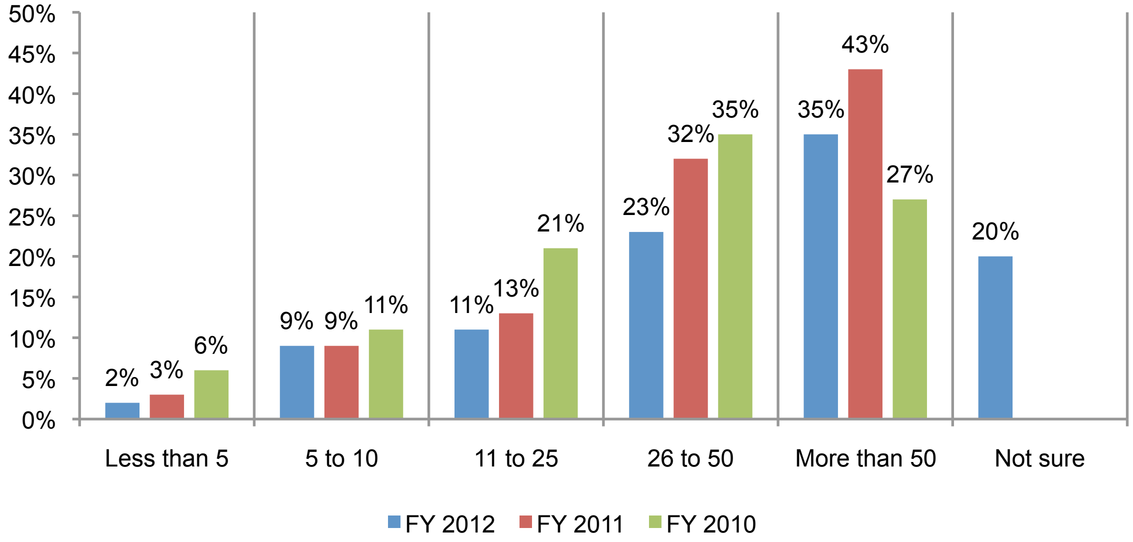
Figure 11. Most vulnerable third-party applications
Three choices permitted



2. The malware threat

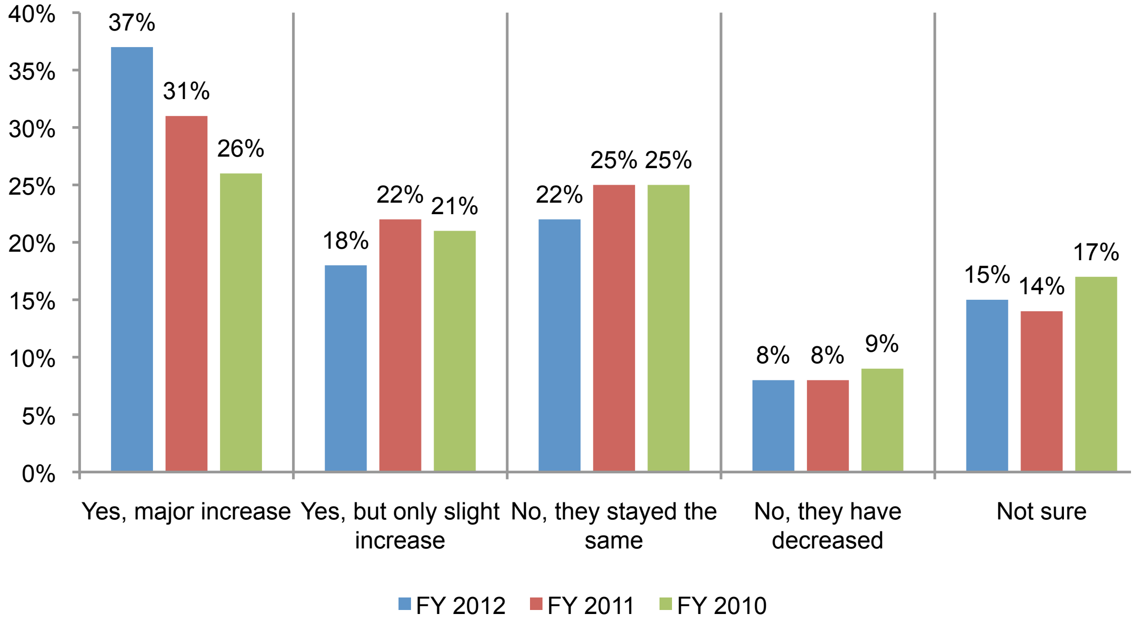
Malware attacks are increasing. According to Figure 12, 58 percent of respondents say their organizations have more than 25 malware attempts or incidents each month. However, 20 percent are not sure how many malware incidents are targeting their organizations**.**

Figure 12. Monthly malware attempts or incidents



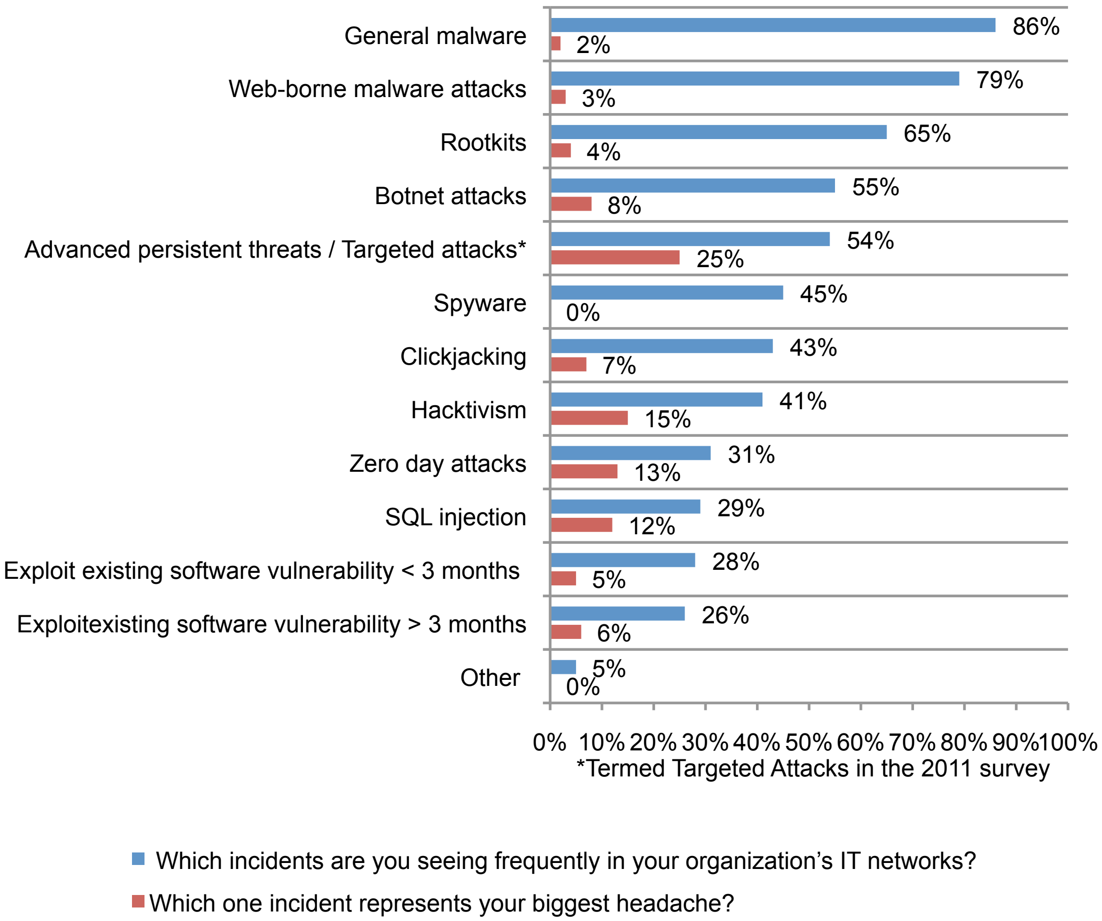
As shown in Figure 13, 37 percent say there has been a major increase in malware incidents in the last year. This is an increase from 26 percent in the 2010 study who said they saw a major increase.

Figure 13. Changes in malware incidents over the past year



In Figure 14 we show which incidents are the most annoying and the most occurring. While they may not be the most frequent incidents, respondents say the get the biggest headaches from APTs and hacktivism. The most frequent are general malware, web-borne malware attacks and rootkits.

Figure 14. Most frequent and annoying incidents
More than one choice permitted

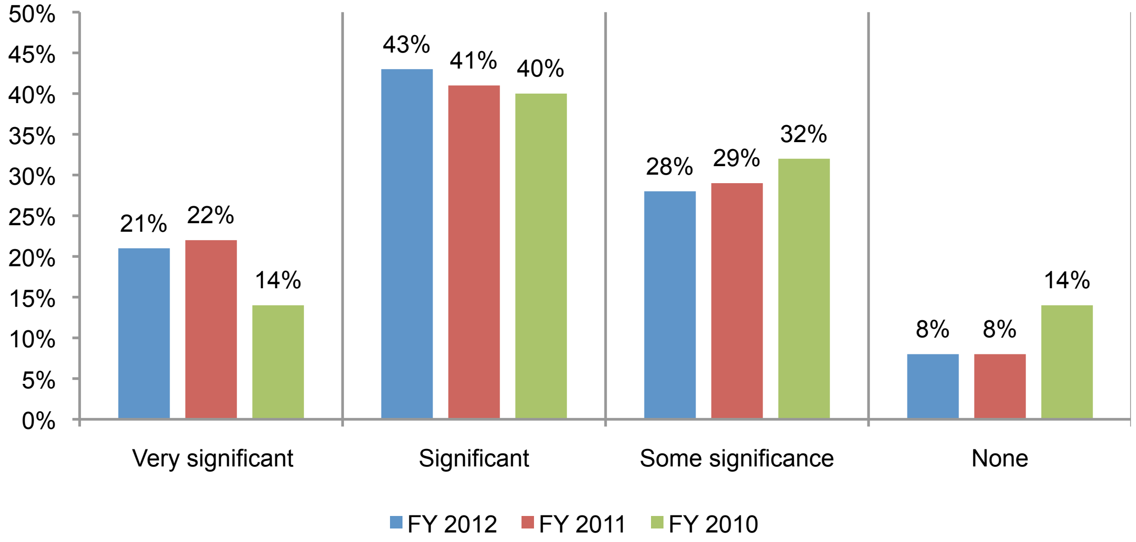


*Termed Targeted Attacks in the 2011 survey

When asked about Mac malware infections, 85 percent of respondents are very concerned or increasingly concerned about Mac malware infections. This perception is unchanged from 2011 when we first asked this question.

Malware is the cause of higher IT operating expenses. Forty-six percent say their organization's IT operating expenses are increasing. Of those, 64 percent say malware incidents are either a very significant or significant reason for the increase, as shown in Figure 15.

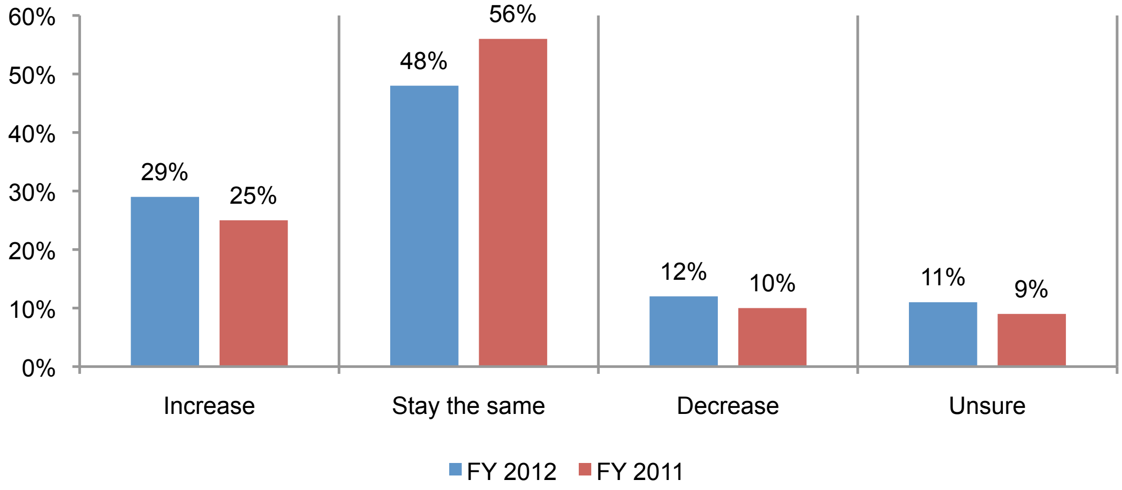
Figure 15. IT operating costs increase due to malware



3. Barriers to achieving optimal endpoint security

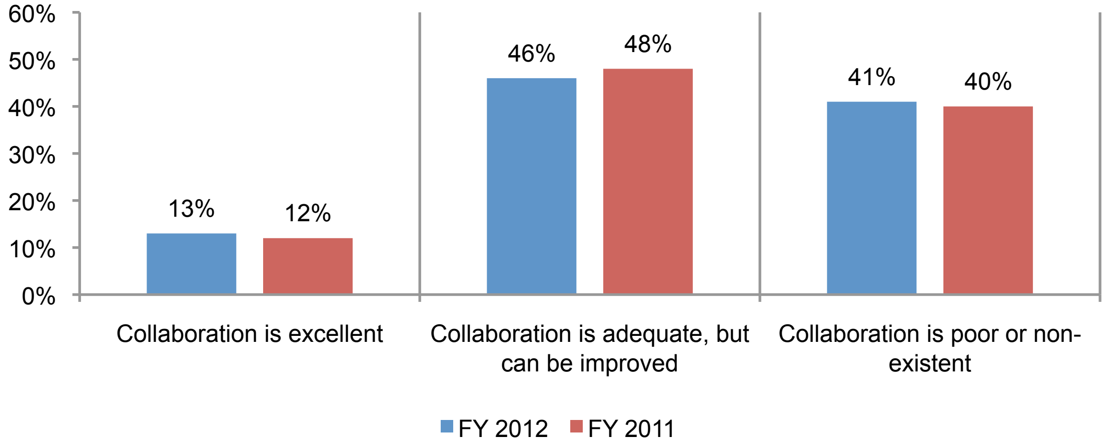
Resources are insufficient to address endpoint risk. Sixty-seven percent do not believe they have ample resources to minimize IT endpoint risk throughout their organization. This is an increase from 63 percent in 2010 who thought this was the situation in their organizations. Despite the popular perception they do not have enough resources, only a slightly higher percentage of respondents say their organization's IT security budget will increase compared to last year (29 percent vs. 25 percent) according to Figure 16. Forty-eight percent say the budget will stay the same.

Figure 16. IT security budget changes from last year



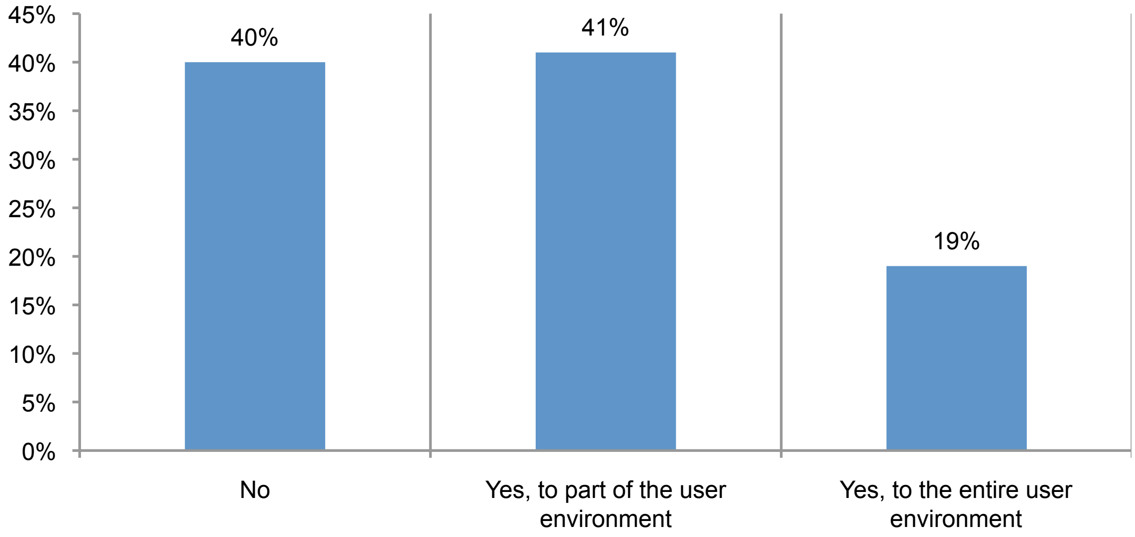
A lack of collaboration continues. As shown in Figure 17, another barrier that continues to prevent organizations from achieving optimum endpoint security is the poor or non-existent collaboration between IT operations and IT security to support planning, communications and information sharing. This has not changed since the 2011 study.

Figure 17. Collaboration between IT operations and IT security



Controlling access privileges is often non-existent. Protecting user access to sensitive information is critical to safeguarding sensitive and confidential information. According to Figure 18, 40 percent say they do not allow or permit local admin privileges to all or part of their user environment. However, 60 percent do allow such admin privileges to part of the user environment (41 percent) or to the entire user environment (19 percent).

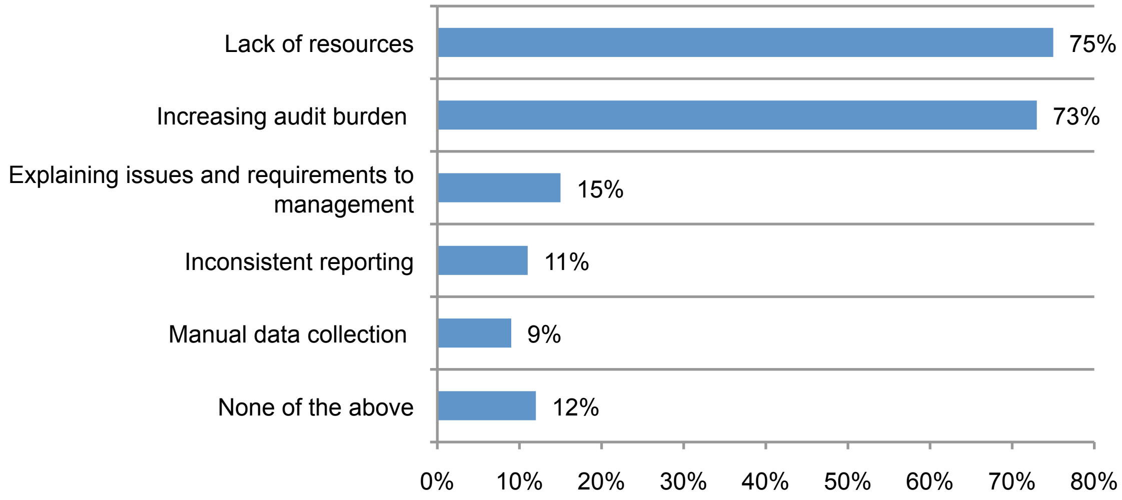
Figure 18. Admin privileges allowed



More than 51 percent of respondents say their organizations do not have any plans to change procedures to improve access governance. However, 45 percent say they are waiting for Windows 8 improvements.

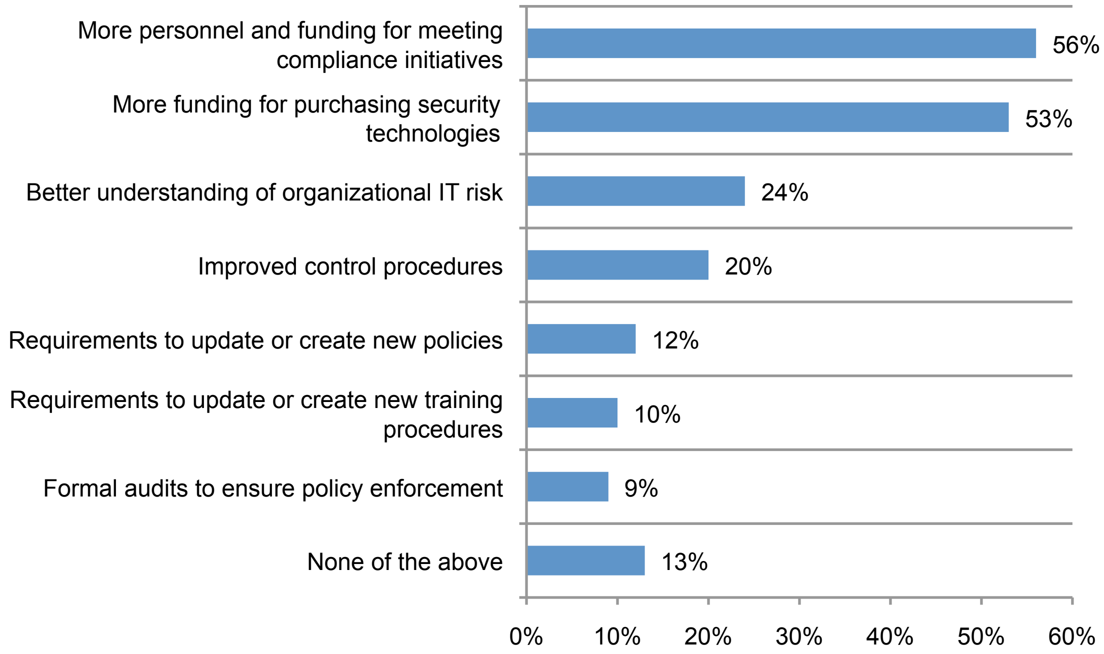
Compliance creates burdens for organizations. According to Figure 19, the greatest challenge to meeting federal compliance regulations is the lack of resources such as skilled personnel, bandwidth and budget. This is followed by 73 percent who say it is an increased audit burden because of the amount of time required and the paperwork frequency of audit cycles.

Figure 19. Greatest challenges in meeting federal compliance regulations
Two choices permitted



Least difficult is manual data collection such as compliance by spreadsheet. In recognition of these challenges, organizations represented in this study are getting more personnel and funding for meeting compliance initiatives and investing in security technologies (Figure 20).

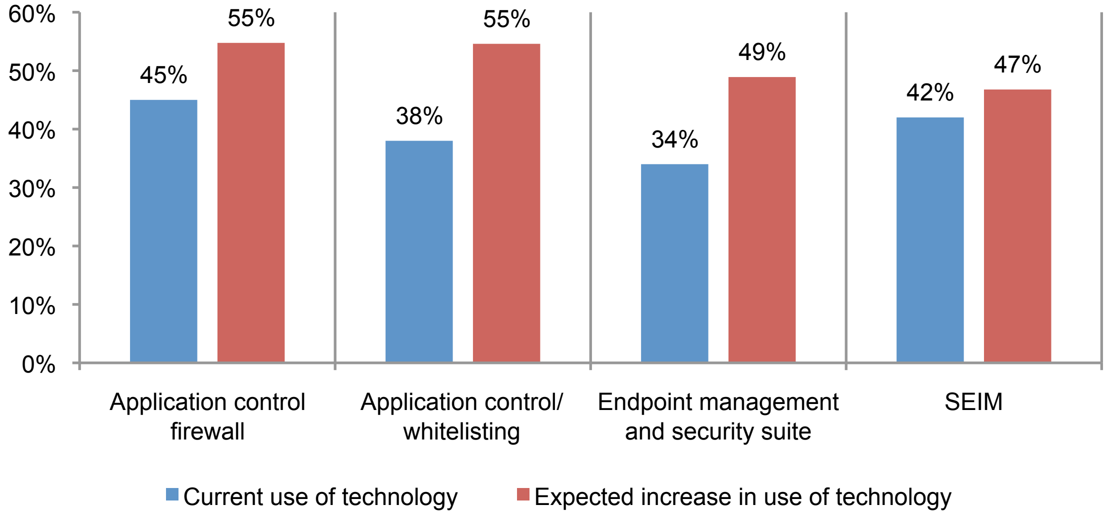
Figure 20. Impact of external compliance requirements on IT security function
Two choices permitted



4. Current and future technologies

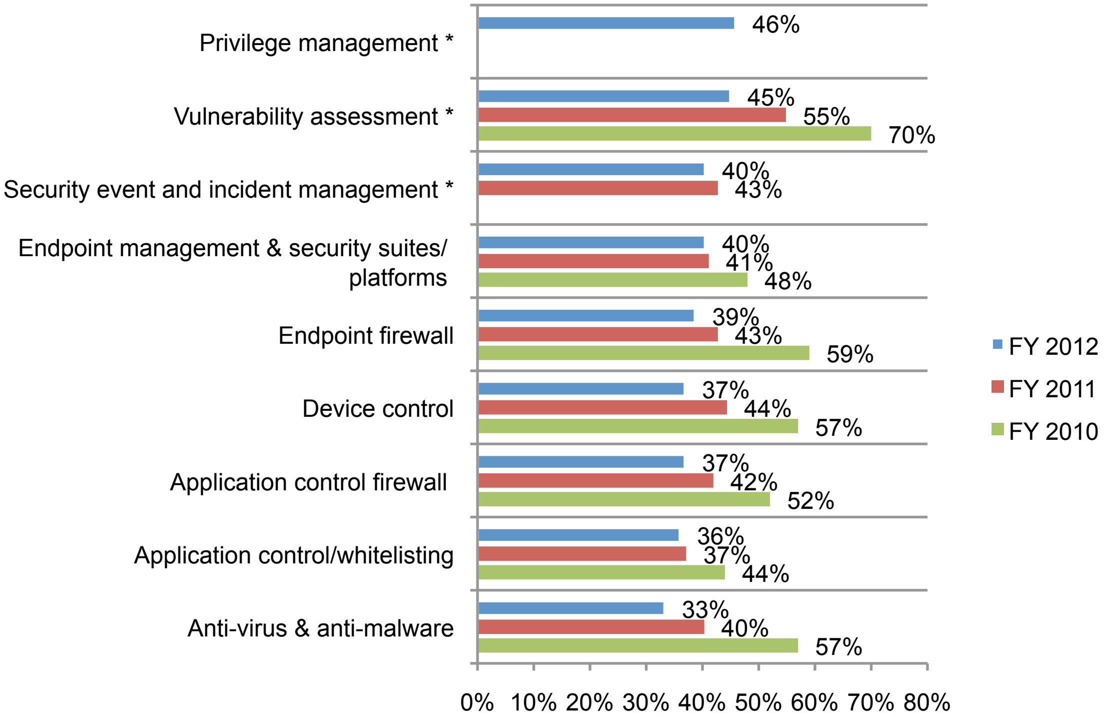
Certain technologies will be more widely deployed. As shown in Figure 21, 55 percent say they will increase investments in application control firewalls and application control/whitelisting (endpoint). Increased spending will also occur for endpoint management and security suite followed by SEIM. Thirty-seven percent plan to increase their investment in mobile device management. Expected to increase, but at a lower rate, are endpoint firewalls, intrusion detection systems and vulnerability assessment.

Figure 21. Technologies in use or to be invested in over the next 12 months
More than one choice permitted



Privilege management and vulnerability assessment are the approaches considered most valuable to meeting their organization's IT risk mitigation requirements. This is followed by SEIM, endpoint management & security suites/platforms (includes multiple integrated technologies) and endpoint firewalls, according to Figure 22.

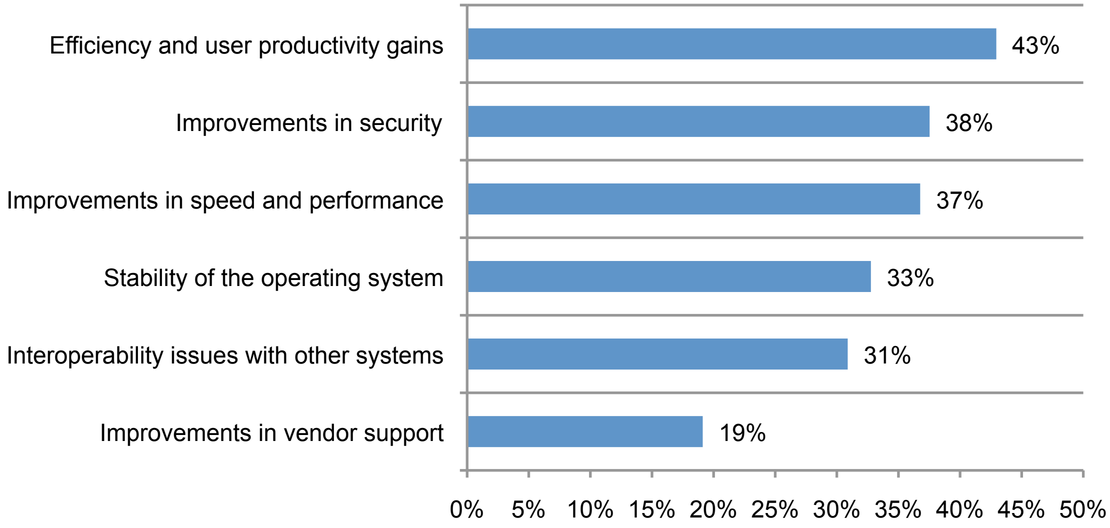
Figure 22. Most effective tools for reducing IT risk
Fiscal years 2012 and 2011 limited to 5 choices



* This choice not available for all fiscal years

Windows 8 migration expected in most organizations. Sixty-nine percent of organizations represented in this study are certain (38 percent) or likely (31 percent) to migrate to Windows 8. According to Figure 23, the two most important reasons for migrating to Windows 8 is efficiency and user productivity gains followed by improvements in security, speed and performance.

Figure 23. Reasons for migrating to Windows 8
Two choices permitted

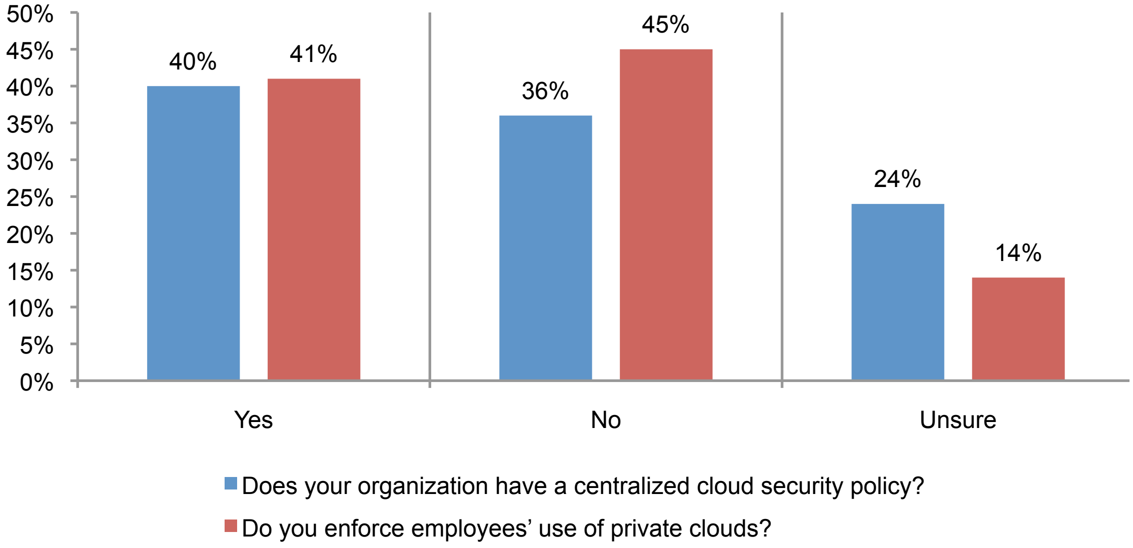


5. Cloud computing and endpoint security

The lack of an enforceable centralized cloud security policy is putting unstructured confidential information at risk. While 40 percent say they have a centralized cloud security policy, 36 percent say they do not have such a policy and 24 percent are unsure.

As revealed in another Ponemon Institute study[1], there are enormous security threats and risks associated with inadequate safeguards over the plethora of confidential business information contained in documents, spreadsheets, presentations and email attachments that end up in a private cloud such as DropBox. According to 45 percent of respondents, their organizations do not enforce employees' use of private clouds and 14 percent are unsure, as shown in Figure 24. As a result, organizations do not know what and how much company data exists in the cloud and if it is appropriately safeguarded.

Figure 24. The existence and enforcement of cloud security policies



[1] *2012 Confidential Documents at Risk Study*, conducted by Ponemon Institute and sponsored by WatchDox, July 2012

Part 3. Conclusion & Recommendations

The changing security terrain is keeping the state of endpoint security from improving. As shown in this study, personally owned mobile devices in the workplace, an increase in the mobile workforce, third party applications, employees use of private clouds and advanced persistent threats are shown to be major challenges to endpoint security. Based on the findings, the following are recommendations:

- Create acceptable use policies for personally owned devices in the workplace.

- Conduct risk assessments and consider the use of an integrated endpoint security suite that includes vulnerability assessment, device control, anti-virus and anti-malware.

- Establish governance practices for privileged users at the device level to define acceptable use of mobile, BYOD and corporate-owned asset as well as limit the installation of third-party applications. Consider the implementation of application whitelisting and privilege management software to control acceptable third-party application installation and enforce change control processes.

- Ensure that policies and procedures clearly state the importance of protecting sensitive and confidential information stored in the cloud. The policy should outline what information is considered sensitive and proprietary.

- To better address the difficulties in managing the endpoint risk, collaboration between IT operations and IT security should be improved to achieve a better allocation of resources and the creation of strategies to address risks associated with hacktivism, BYOD, third-party applications and cloud computing.

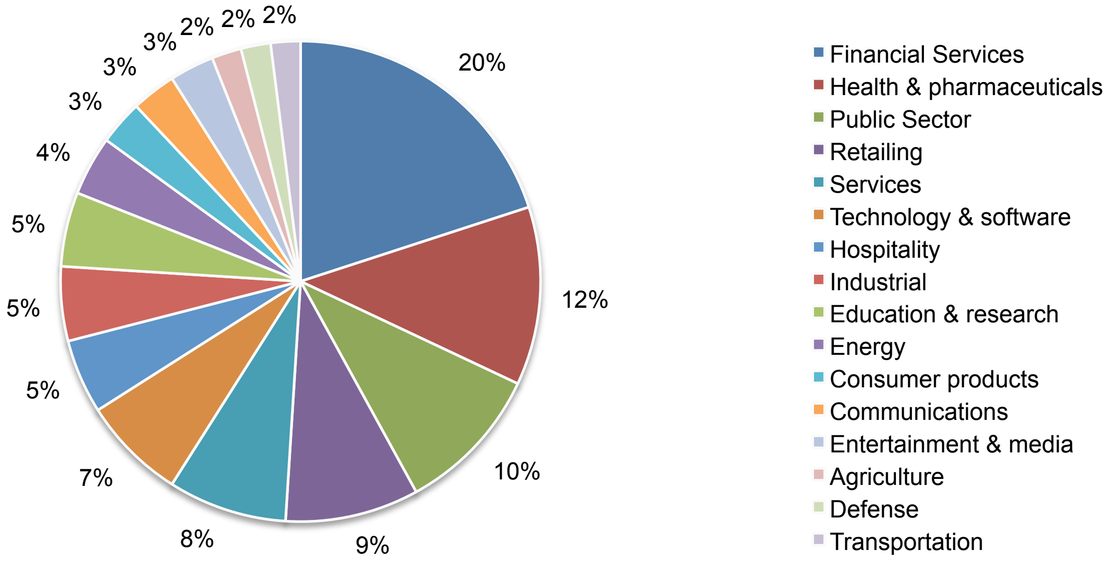
Part 5. Methods

A random sampling frame of 17,744 IT and IT security practitioners located in all regions of the United States were selected as participants to this survey. As shown in Table 1, 923 respondents completed the survey. Screening removed 178 surveys and an additional 74 surveys that failed reliability checks were removed. The final sample was 671 surveys (or a 3.8 percent response rate).

Table 1. Sample response	FY 2012	FY 2011	FY 2010
Total sampling frame	17,744	18,988	11,890
Total returns	923	911	782
Rejected surveys	74	80	65
Screened surveys	178	143	153
Final sample	671	688	564
Response Rate	3.8%	3.6%	4.7%

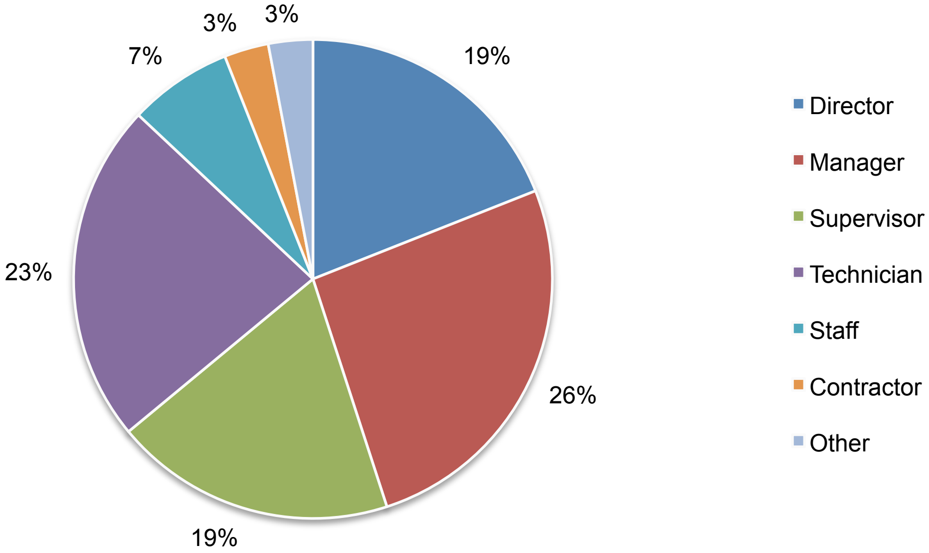
Pie Chart 1 reports the respondents' primary industry focus. Twenty percent of respondents are in financial services and 12 percent are in health and pharmaceutical. Another ten percent are in the public sector.

Pie Chart 1. Distribution of respondents according to primary industry classification



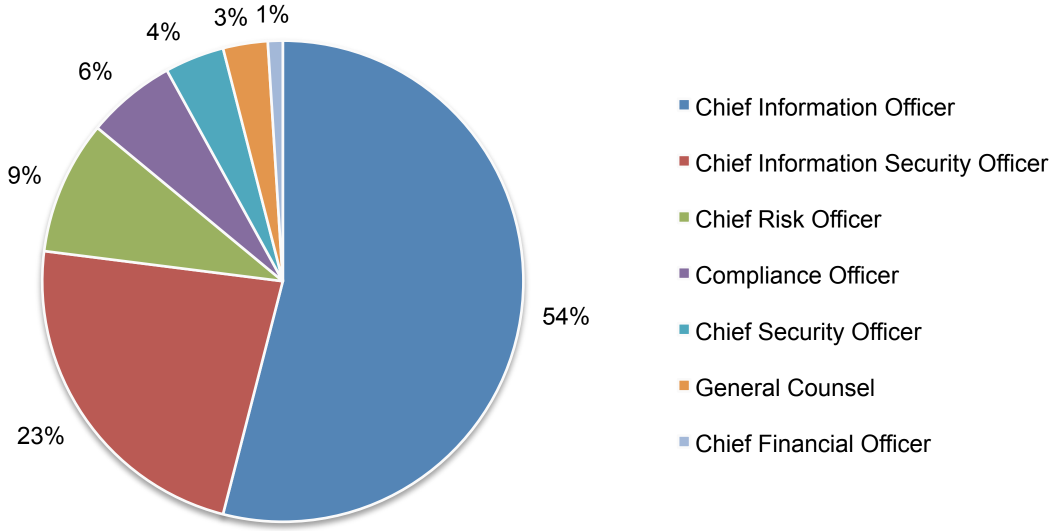
Pie Chart 2 reports the respondent's organizational level within participating organizations. The majority (64 percent) of respondents are at or above the supervisory levels.

Pie Chart 2. What organizational level best describes your current position?



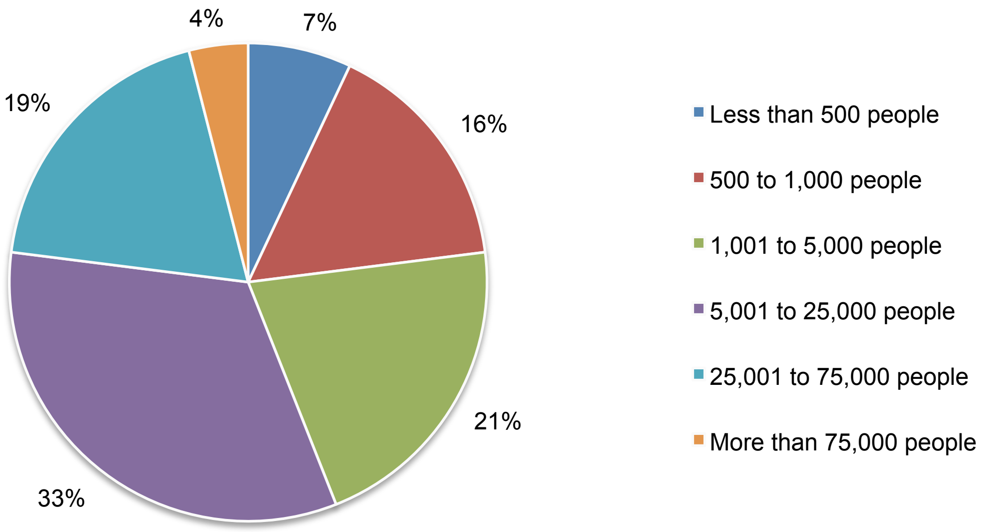
According to Pie Chart 3, 54 percent of respondents report directly to the Chief Information Officer and 23 percent report to the Chief Information Security Officer.

Pie Chart 3. The primary person you or the IT security leader reports to within the organization



As shown in Pie Chart 4, 77 percent of respondents are from organizations with a worldwide headcount greater than 1,000.

Pie Chart 4. Worldwide headcount



Part 6. 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 September 2012.

Sample response	**FY 2012**	**FY 2011**	**FY 2010**
Total sampling frame	17,744	18,988	11,890
Total returns	923	911	782
Total rejections	74	80	65
Screened surveys	178	143	153
Final sample	671	688	564
Response rate	3.8%	3.6%	4.7%

Part 1. Screening			
S1. What best describes your level of involvement in endpoint security within your organization?	**FY 2012**	**FY 2011**	**FY 2010**
None (stop)	24	33	27
Low (stop)	14	21	13
Moderate	76	85	77
Significant	456	417	398
Very significant	279	275	202
Total	849	831	717

S2. What best describes the number of employees (end users) who have access to your organization's network?	**FY 2012**	**FY 2011**	**FY 2010**
Less than 50 (stop)	26	30	19
51 to 100	10	11	6
101 to 500	60	62	53
501 to 1,000	142	135	118
More than 1,000	573	560	481
Total	811	798	677

S3. What best describes your role within your organization's IT department?	**FY 2012**	**FY 2011**	**FY 2010**
IT management	175	156	135
IT operations	163	150	146
Data administration	73	69	81
IT compliance	70	61	57
IT security	206	177	183
Applications development	35	32	35
I'm not involved in my organization's IT function (stop)	53	123	21
Total	775	768	658

S4. Please check all the activities that you see as part of your job or role.	**FY 2012**	**FY 2011**	**FY 2010**
Managing budgets	401	398	319
Evaluating vendors	254	237	228
Setting priorities	223	235	201
Securing systems	359	305	260
Ensuring compliance	174	178	159
None of the above (stop)	61	80	73

Part 2: Attributions	FY 2012	
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.	14%	19%
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.	9%	11%

Part 2: Attributions	FY 2011	
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.	15%	20%
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.	11%	15%

Part 2: Attributions	FY 2010	
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.	17%	20%
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.		

Q2. What one statement best describes how IT operations and IT security work together to support organizational planning, communications, and information sharing?	FY 2012	FY 2011
Collaboration is excellent	13%	12%
Collaboration is adequate, but can be improved	46%	48%
Collaboration is poor or non-existent	41%	40%
Total	100%	100%

Part 3: Endpoint Risk

Q3. Is your IT network more secure now than it was a year ago?	FY 2012	FY 2011	FY 2010
Yes	33%	34%	36%
No	46%	41%	36%
Unsure	21%	25%	28%
Total	100%	100%	100%

Q4. On average, how many malware attempts or incidents does your IT organization deal with monthly?	FY 2012	FY 2011	FY 2010
Less than 5	2%	3%	6%
5 to 10	9%	9%	11%
11 to 25	11%	13%	21%
26 to 50	23%	32%	35%
More than 50	35%	43%	27%
Not sure	20%		
Total	100%	100%	100%

Q5. Has the frequency of malware incidents changed over the last year within your organization?	FY 2012	FY 2011	FY 2010
Yes, major increase	37%	31%	26%
Yes, but only slight increase	18%	22%	21%
No, they stayed the same	22%	25%	25%
No, they have decreased	8%	8%	9%
Not sure	15%	14%	17%
Total	100%	100%	98%

Q6. Which of these types of incidents are you seeing frequently in your organization's IT networks? Please check all that apply.	FY 2012	FY 2011	FY 2010
Zero day attacks	31%	29%	30%
Exploit of existing software vulnerability less than 3 months old	28%	33%	30%
Exploit of existing software vulnerability greater than 3 months old	26%	31%	26%
SQL injection	29%	32%	35%
Spyware	45%	49%	57%
Botnet attacks	55%	56%	64%
Clickjacking	43%	37%	25%
Rootkits	65%	63%	57%
General malware	86%	89%	92%
Web-borne malware attacks	79%	83%	75%
Advanced persistent threats (APT) / Targeted attacks*	54%	36%	
Hacktivism	41%	33%	
Other (please specify)	5%	6%	13%
Total	587%	577%	504%
*Termed Targeted Attacks in the 2011 survey			

Q7. Which one incident represents your biggest headache?	FY 2012	FY 2011	FY 2010
Zero day attacks	13%	23%	35%
Exploit of existing software vulnerability less than 3 months old	5%	11%	11%
Exploit of existing software vulnerability greater than 3 months old	6%	10%	16%
SQL injection	12%	21%	23%
Spyware	0%	1%	2%
Botnet attacks	8%	5%	8%
Clickjacking	7%	7%	5%
Rootkits	4%		
General malware	2%		
Web-borne malware attacks	3%		
Advanced persistent threats (APT) / Targeted attacks*	25%	22%	
Hacktivism	15%		
Other (please specify)	0%	0%	0%
Total	100%	100%	100%
*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.	**FY 2012**	**FY 2011**	**FY 2010***
Our server environment	19%	29%	32%
Our data centers	6%	12%	14%
Within operating systems (vulnerabilities)	8%	10%	11%
Across 3rd party applications (vulnerabilities)	67%	56%	45%
Our PC desktop/laptop	45%	41%	44%
Mobile devices such as smart phones (Blackberry, iPhone, IPad, Android)	73%	48%	9%
Removable media (USB sticks) and/or media (CDs, DVDs)	39%	42%	10%
Network infrastructure environment (gateway to endpoint)	10%	14%	11%
Malicious insider risk	15%	16%	
Negligent insider risk	44%	43%	
Insider risk (malicious and accidential)			41%
Cloud computing infrastructure and providers	41%	43%	18%
Virtual computing environments (servers, endpoints)	19%	28%	20%
Mobile/remote employees	53%	49%	44%
Lack of system connectivity/visibility	25%	29%	
Lack of organizational alignment	36%	39%	
Total	500%	499%	299%
*Top 3 choices in the 2010 survey			

Q9. 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.	**FY 2012**	**FY 2011**	**FY 2010***
Use of insecure cloud computing resources	28%	31%	49%
Advanced persistent threats	36%	24%	24%
Malicious insider risk	12%	11%	19%
Negligent insider risk	15%	28%	50%
Insufficient budget resources	30%	32%	47%
Increased use of mobile platforms (smart phones, iPads, etc.)	47%	36%	
Growing volume of malware	30%	29%	61%
Increasingly sophisticated and targeted cyber attackers	31%	26%	40%
Lack of an organizational wide security strategy	12%	13%	
Insufficient collaboration among IT and business operations	13%	16%	
Lack of integration between endpoint operations and security technologies	18%	17%	20%
Inability to measure policy compliance	6%	12%	
Intrusions and data loss within virtual environments	22%	23%	13%
Other (please specify)	0%	0%	
Total	300%	299%	323%
*More than three responses permitted in 2010			

Part 4. Endpoint Productivity	**FY 2012**		
Q10. 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	Combined
Mobile devices / smart phones	40%	35%	75%
Virtualized environments (servers & desktops)	32%	29%	61%
Use of 3rd party (non-company) cloud computing infrastructure	32%	31%	63%
Use of internal cloud computing infrastructure	25%	28%	53%
Social media / Web 2.0			
Security event and incident management (SEIM)			

Part 4. Endpoint Productivity	**FY 2011**		
Q10. 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	Combined
Mobile devices / smart phones	35%	35%	70%
Virtualized environments (servers & desktops)	24%	28%	52%
Use of 3rd party (non-company) cloud computing infrastructure	26%	30%	56%
Use of internal cloud computing infrastructure	16%	19%	35%
Social media / Web 2.0	40%	32%	72%
Security event and incident management (SEIM)	18%	27%	45%

Q11. What percent of your organization’s employees use their personal mobile devices in the workplace (a.k.a. BYOD)?	**FY 2012**	**FY 2011**
None	2%	3%
1 to 25%	16%	23%
26 to 50%	28%	34%
51 to 75%	29%	20%
More than 75%	18%	13%
Cannot determine	7%	7%
Total	100%	100%

Q12. If employee-owned mobile devices are connected to your organization’s networks, does the organization have an effort in place to secure them?	**FY 2012**	**FY 2011**
No	29%	21%
No, but we plan to	19%	21%
Yes, we secure them in a manner similar to that already in place for corporate devices	39%	46%
Yes, we use stricter security standards for mobile than we do for corporate-owned devices	13%	12%
Total	100%	100%

Q13a. Does your organization allow or permit local admin privileges to all or part of your user environment?	**FY 2012**
No	40%
Yes, to part of the user environment	41%
Yes, to the entire user environment	19%
Total	100%

Q13b. If yes, what are your plans to mitigate or lessen this risk? Please select all that apply.	**FY 2012**
Replace local admin with standard users	32%
Wait for Windows 8 improvements	45%
Implement application whitelisting	29%
Implement privilege management software	36%
We have no plans to change	51%
Total	193%

	FY 2012		
Q14. 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.	Use rate	Use will increase	Use will decrease
Anti-virus	99%	5%	0%
Application control firewall (gateway) (NGFW)	45%	55%	4%
Application control/whitelisting (endpoint)	38%	55%	9%
Data loss/leak prevention (content filtering)	34%	34%	8%
Device control (removable media i.e., USB, CD/DVD)	29%	27%	14%
Endpoint firewall	61%	11%	5%
Endpoint management and security suite (integrated technologies like AV, patch, etc.)	34%	49%	15%
Intrusion detection	59%	15%	27%
Mobile device management		37%	4%
Network access control (NAC)	50%	23%	13%
Patch & remediation management	56%	26%	2%
Security Event and Incident Management (SEIM)	42%	47%	8%
Vulnerability assessment (vulnerability scanning)	43%	16%	14%
Whole disk encryption	33%	32%	11%

Q14. 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.	FY 2011 Use rate	 Use will increase	 Use will decrease
Anti-virus	100%	10%	1%
Application control firewall (gateway) (NGFW)	49%	55%	10%
Application control/whitelisting (endpoint)	36%	56%	4%
Data loss/leak prevention (content filtering)	32%	29%	7%
Device control (removable media i.e., USB, CD/DVD)	31%	20%	10%
Endpoint firewall	60%	18%	13%
Endpoint management and security suite (integrated technologies like AV, patch, etc.)	32%	46%	9%
Intrusion detection	58%	23%	15%
Mobile device management	26%	45%	3%
Network access control (NAC)	48%	30%	9%
Patch & remediation management	54%	12%	18%
Security Event and Incident Management (SEIM)	40%	38%	8%
Vulnerability assessment (vulnerability scanning)	49%	9%	9%
Whole disk encryption	30%	15%	9%

Q15. Which of the following technologies or approaches are most effective in meeting your organization's IT risk mitigation requirements? Choose only your top five choices.	FY 2012	FY 2011	FY 2010*
Anti-virus & anti-malware	33%	40%	57%
Application control firewall (gateway) (NGFW)	37%	42%	52%
Application control/whitelisting (endpoint)	36%	37%	44%
Configuration management	28%		39%
Data loss/leak prevention (content filtering)	16%	20%	23%
Device control (USB, removable media)	37%	44%	57%
Endpoint firewall	39%	43%	59%
Endpoint management & security suites/platforms (includes multiple integrated technologies i.e. AV, patch, configuration management, etc.)	40%	41%	48%
Intrusion detection	19%	17%	19%
Network access control (NAC)	30%	35%	46%
Patch & remediation management	24%	23%	38%
Vulnerability assessment	45%	55%	70%
Whole disk encryption	30%	35%	45%
Privilege management	46%		
Mobile device management		24%	
Security event and incident management (SEIM)	40%	43%	
Total	500%	500%	597%
*The 2010 survey permitted all that apply rather than top five			

Q16. 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.	FY 2012 Points	FY 2011 Points
Windows o/s	53	57
Mac o/s	16	13
Linux	15	12
Unix	13	14
Other	3	4
Total points	100	100

Q17. [For those using the Apple Mac], How concerned are you about Mac malware infections?	FY 2012	FY 2011
Very concerned	45%	41%
Increasingly concerned	40%	44%
Not at all concerned	11%	12%
Not applicable	4%	3%
Total	100%	100%

Q18a. Are your organization's IT operating expenses increasing?	FY 2012	FY 2011	FY 2010
Yes	46%	43%	41%
No	39%	46%	48%
Unsure	15%	11%	11%
Total	100%	100%	100%

Q18b. If yes, to what extent are malware incidents to blame?	FY 2012	FY 2011	FY 2010
Very significant	21%	22%	14%
Significant	43%	41%	40%
Some significance	28%	29%	32%
None	8%	8%	14%
Total	100%	100%	100%

Q19. How effective do you believe that your current anti-virus/anti-malware technology is in terms of protecting your IT endpoints from today's malware risk?	FY 2012	FY 2011	FY 2010
Very effective	12%	11%	12%
Somewhat effective	29%	33%	34%
Somewhat ineffective	34%	30%	28%
Not effective at all	22%	21%	26%
Cannot determine	3%	5%	
Total	100%	100%	100%

Q20. From the list below, what has been the greatest challenge in meeting federal compliance regulations? Please select no more than two choices.	FY 2012
Lack of resources (including skilled personnel, bandwidth, budget)	75%
Increasing audit burden (including time, paperwork frequency of audit cycles)	73%
Explaining issues and requirements to management	15%
Inconsistent reporting	11%
Manual data collection (i.e., compliance by spreadsheet)	9%
None of the above	12%
Total	195%

Q21. From the list below, what impact have external compliance requirements had on your organization's IT security function? Please select no more than two choices.	FY 2012
More personnel and funding for meeting compliance initiatives	56%
More funding for purchasing security technologies	53%
Improved control procedures	20%
Better understanding of organizational IT risk	24%
Formal audits to ensure policy enforcement	9%
Requirements to update or create new policies	12%
Requirements to update or create new training procedures	10%
None of the above	13%
Total	197%

Part 5. Endpoint Resources		
Q22. How does your organization's IT security budget this year compare to last year?	**FY 2012**	**FY 2011**
Increase	29%	25%
Stay the same	48%	56%
Decrease	12%	10%
Unsure	11%	9%
Total	100%	100%

Q23a. Does your organization have a centralized cloud security policy?	**FY 2012**
Yes	40%
No	36%
Unsure	24%
Total	100%

Q23b. If yes, do you enforce employees' use of private clouds (i.e., DropBox)?	**FY 2012**
Yes	41%
No	45%
Unsure	14%
Total	100%

Q24a. Is your organization planning to migrate to Windows 8?	**FY 2012**
Yes, with certainty	38%
Yes, likely to do so	31%
No	21%
Unsure	10%
Total	100%

Q24b. If yes, what are the most important reasons for migrating to Windows 8? Please select your top two choices.	**FY 2012**
Improvements in security	38%
Stability of the operating system	33%
Improvements in speed and performance	37%
Interoperability issues with other systems	31%
Efficiency and user productivity gains	43%
Improvements in vendor support	19%
Other (please specify)	0%
Total	200%

Q25. In regards to mobile device management, what are the three most important to your organization's needs?	**FY 2012**	**FY 2011**
Provisioning and access policy management	70%	62%
Virus and malware detection or prevention	65%	55%
Asset tracking	43%	47%
Encryption and other data loss technologies	44%	49%
Anti-theft features	39%	42%
Remote wipe capability	38%	41%
Other (please specify)	1%	3%
Total	300%	299%

Q26. 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.	FY 2012	FY 2011	FY 2010
Microsoft OS/applications	44%	49%	57%
Apple/Mac OS	30%	24%	15%
Apple apps (QuickTime, iTunes, etc.)	28%	20%	14%
Adobe (Flash, Adobe Reader, etc.)	55%	50%	54%
WinZip	11%	16%	19%
Oracle applications	15%	22%	10%
VMware	18%	20%	17%
Google Docs	55%	47%	46%
Mozilla Firefox	3%	6%	2%
General 3rd party applications outside of Microsoft	40%	46%	58%
Other (please specify)	0%	1%	4%
Total	299%	299%	298%

Q27. 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?	FY 2012	FY 2011
Yes, with certainty	33%	32%
Yes, likely to do so	35%	31%
No	21%	25%
Unsure	11%	12%
Total	100%	100%

Q28. Does your organization have an integrated endpoint security suite (vulnerability assessment, device control, anti-virus, anti-malware or others)?	FY 2012	FY 2011
Yes	35%	33%
No, but our organization expects to have an endpoint security suite within the next 12-24 months	48%	46%
No	17%	21%
Total	100%	100%

Part 6. Endpoint Complexity

Q29. 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 2012	FY 2011
1 to 2	19%	18%
3 to 5	21%	23%
6 to 10	41%	39%
More than 10	13%	10%
Cannot determine	6%	10%
Total	100%	100%

Q30. 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.	**FY 2012**	**FY 2011**
1 to 2	19%	23%
3 to 5	25%	29%
6 to 10	35%	30%
More than 10	11%	9%
Cannot determine	10%	9%
Total	100%	100%

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

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

D6. What industry best describes your organization's **primary** industry focus?	FY 2012	FY 2011	FY 2010
Consumer products	3%	2%	3%
Communications	3%	5%	4%
Agriculture	2%	1%	2%
Defense	2%	3%	3%
Energy	4%	3%	2%
Entertainment & media	3%	4%	3%
Financial Services	20%	18%	19%
Health & pharmaceuticals	12%	10%	11%
Hospitality	5%	4%	4%
Industrial	5%	4%	5%
Public Sector	10%	12%	13%
Education & research	5%	6%	5%
Retailing	9%	8%	7%
Services	8%	9%	8%
Technology & software	7%	8%	6%
Transportation	2%	3%	5%
Total	100%	100%	100%

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

D5. What is the worldwide headcount of your organization?	FY 2012	FY 2011	FY 2010
Less than 500 people	7%	5%	6%
500 to 1,000 people	16%	16%	13%
1,001 to 5,000 people	21%	22%	19%
5,001 to 25,000 people	33%	31%	32%
25,001 to 75,000 people	19%	21%	21%
More than 75,000 people	4%	5%	9%
Total	100%	100%	100%

Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

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.