



State of Endpoint Risk

Sponsored by Lumension

Independently conducted by Ponemon Institute LLC

Publication Date: December 6, 2010

State of Endpoint Risk

Ponemon Institute: December 6, 2010

Part 1. Executive Summary

If you worry about your organization's ability to prevent cyber attacks or provide visibility over endpoints, you are not alone. In the *State of Endpoint Risk* study sponsored by Lumension and conducted by Ponemon Institute, IT executives acknowledge that the people, processes and technologies necessary to deal with a changing IT risk environment are not supported by adequate budgets and enforced security policies. As a result, organizations are wasting valuable time, money and resources while continuing to expose their IT environment to unnecessary risks.

A key finding from this study is despite the increasing availability of new technologies to address endpoint risks, 64 percent say their networks are not more secure than they were a year ago or they are unsure. Despite the insecurity, 48 percent say their operating expenses are increasing and a main driver of those costs is tied directly to an increase in malware incidents. Fifty-nine percent of those respondents who say costs are increasing say malware is a very significant and significant factor in those cost drivers.

Further, these malware attack vectors are focusing more on third-party and web-based applications and an increasingly mobile workforce has grown accustomed to unrestricted access to their corporate IT environment. All told, IT organizations are now faced with a very vulnerable endpoint. And, they have limited visibility into the endpoint to truly and effectively mitigate the risk of network intrusions. Yet, they are armed with the wrong technologies and/or have ineffective policies in place to enact any sort of change.

The 564 respondents in our study are deeply involved in their organization's IT function. Fifty-one percent are managers or hold higher positions in their organizations. Fifty percent report directly to the chief information officer (CIO) and 21 percent report to the chief information security officer (CISO). Twenty-eight percent work in IT security, 22 percent are in IT operations and 21 percent are in IT management.

The purpose of this study is to determine how effective organizations are in the protection of their endpoints and what they perceive are the biggest obstacles to reducing risk. Given the volume and severity of endpoint attacks it is easy to understand why respondents are not confident in their ability to manage these risks. Specifically, organizations in our study are experiencing the following threats:

- 62 percent of respondents say their organizations have had more than 50 malware attempt incidents each month. On average, organizations in our study are having one or more malware attacks each day.
- 98 percent have had a virus or malware network intrusion.
- 95 percent have had desktops and laptops or other devices stolen.
- 89 percent have lost sensitive data because of a negligent insider and 61 percent have lost sensitive data because of a malicious insider.

Organizations also are realizing that the information risk environment is shifting. Of less concern are threats to their data centers, operating systems and network infrastructures. On the increase, respondents say, are the potentially more lethal and difficult to detect cyber attacks and malware incidents. Other risks more difficult to manage are those created by employees who are increasingly mobile, working from remote locations and downloading third-party applications.

Unfortunately, respondents in our study do not seem to be optimistic that they have the arsenal in place to deal with this new risk environment. People, process and technologies supported by an

adequate budget are lacking. They also believe that existing anti-virus and anti-malware technologies could be more effective.

The study also finds that technologies being used are not always considered by respondents to be the most effective. For example, more than half use intrusion detection and patch & remediation management (57 percent and 53 percent, respectively) yet only 19 percent believe intrusion detection is one of the most effective technologies in reducing risk and 38 percent say patch & remediation management is most effective.

On the other hand, 70 percent of users say vulnerability assessment is one of the most effective in reducing IT risk but just over half (51 percent) say they use this approach. Other technologies that are considered to be among the most effective solutions yet are not frequently deployed include application whitelisting (used by only 29 percent) and endpoint management & security suites platform (used by 40 percent).

Part 2. Key Findings

In this section we present the key findings of the study according to the following three topics:

- The state of endpoint risk in organizations
- How organizations are investing in IT security readiness
- How organizations are addressing endpoint application risks

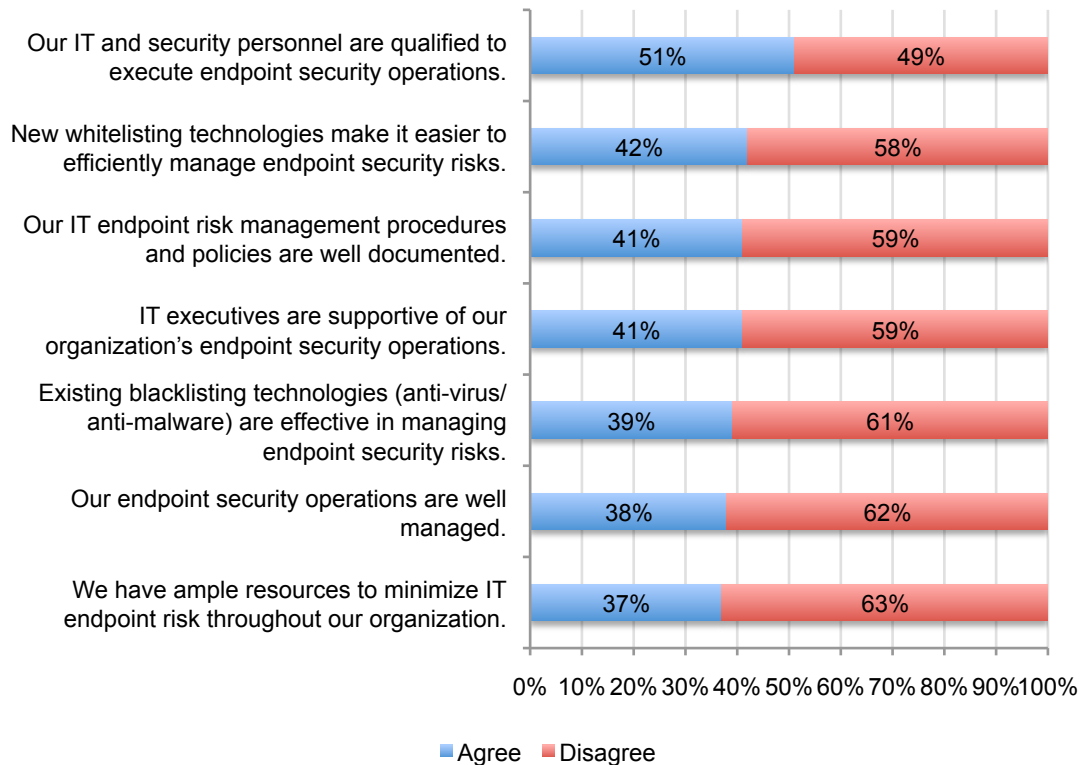
The state of endpoint risk in respondents' organizations

The first part of the study asked respondents their perceptions about the current state of endpoint security within their organizations. Bar Chart 1 summarizes the respondents' perceptions. An "agree" response indicates a favorable impression and a "disagree" response indicates the opposite.

In general, the pattern of agree and disagree responses summarized for seven attributions about endpoint security suggests many respondents do not hold favorable impressions about endpoint security operations, budgetary resources and skilled personnel. The lowest level of agreement (37 percent) concerns the lack of resources to minimize endpoint risk. Similarly, only 38 percent of respondents agree their company's endpoint security operations are presently well managed. Moreover, only 39 percent of respondents agree that existing blacklisting technologies (i.e. anti-virus and anti-malware) are effective in managing endpoint security risks.

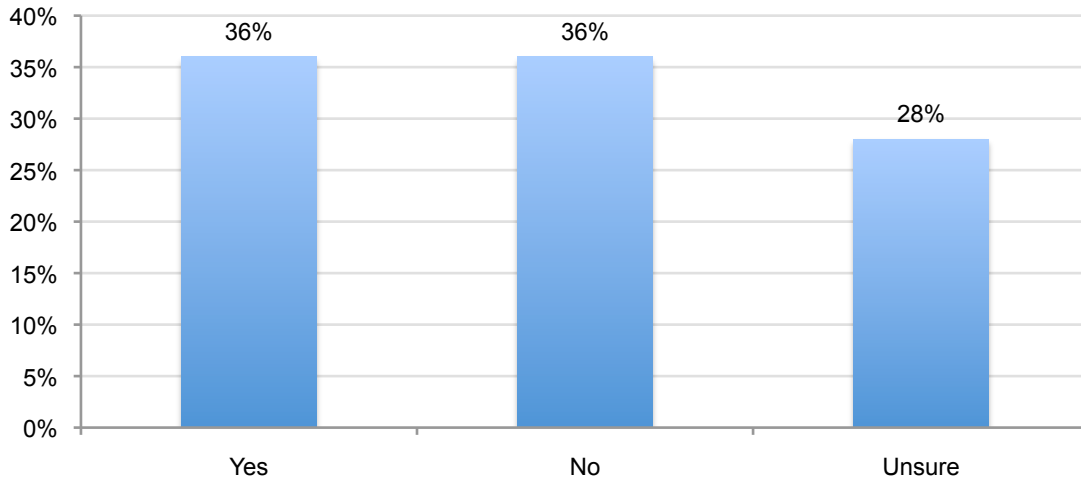
Bar Chart 1: Attributions about endpoint security

Agree = strongly agree and agree combined. Disagree = unsure, disagree and strongly disagree combined.



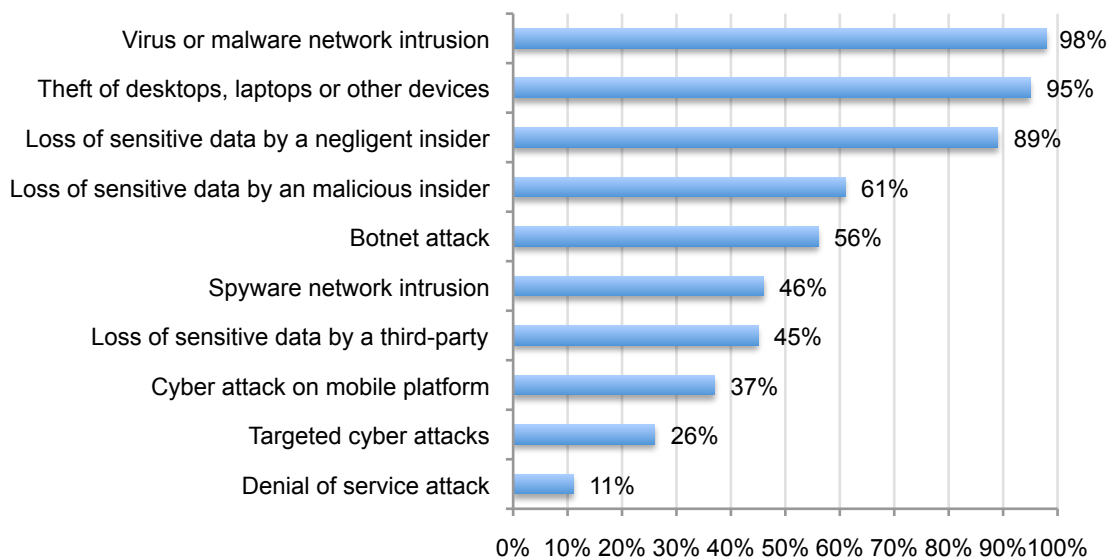
The study finds that the majority of respondents believe their organizations' endpoints are vulnerable to attacks. As shown in Bar Chart 2, 64 percent of respondents say their organizations' IT networks **are not more secure** than last year percent or are unsure (36 percent + 28 percent).

Bar Chart 2: Is your IT network more secure now than it was a year ago?



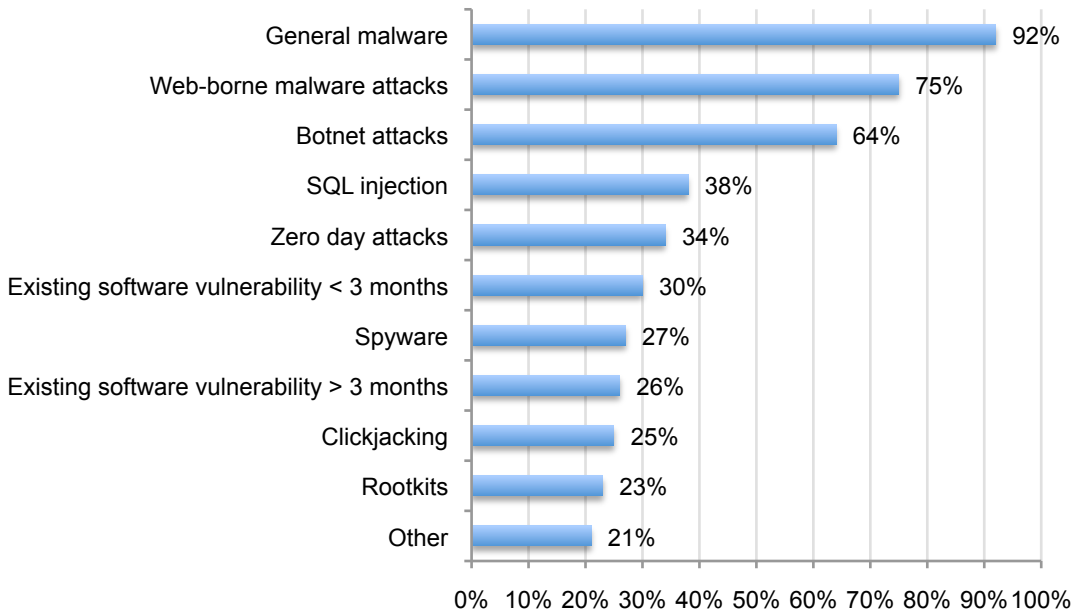
As noted in Bar Chart 3, organizations face a variety of incidents that threaten the security of the endpoint. During the past year, 98 percent have had virus or malware network intrusions, 95 percent have had desktops and laptops or other devices stolen. Eighty-nine percent have lost sensitive data because of a negligent insider and 61 percent lost sensitive data because of a malicious insider. The least frequent incident is a denial of service attack (11 percent).

Bar Chart 3: Which of the following incidents happened during the past year?



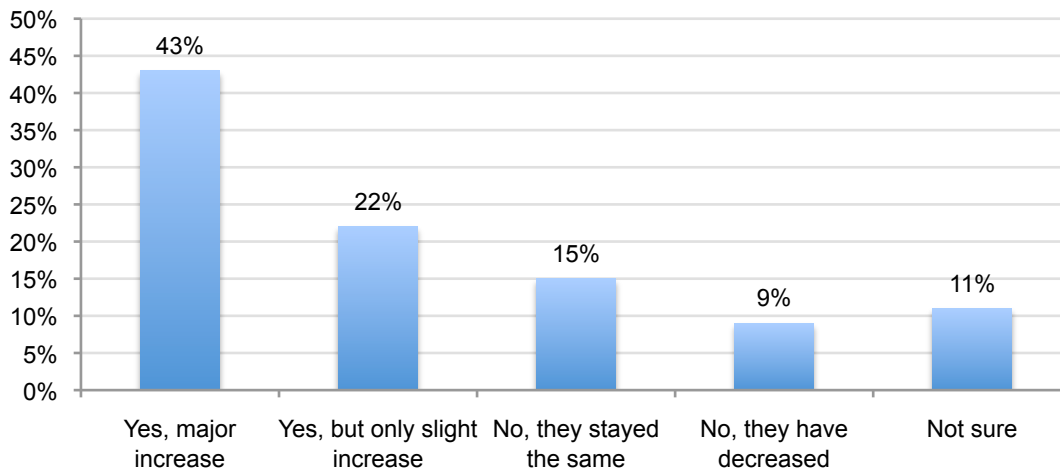
As noted in Bar Chart 4, the most frequently encountered IT network incidents are general malware attacks (92 percent of respondents), web-borne malware attacks (75 percent of respondents), botnet attacks (64 percent of respondents) and SQL injections (38 percent of respondents).

Bar Chart 4: Which incidents are you seeing frequently in your IT network?



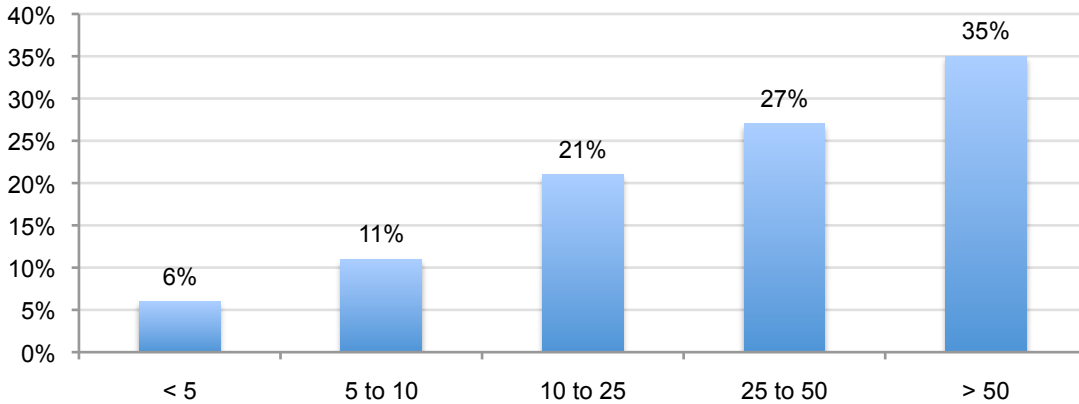
Bar Chart 5 shows 43 percent of respondents say there has been a major increase in malware attacks and 22 percent say there has been a slight increase over the past year. Only 9 percent of respondents believe malware attacks have decreased over the past year.

Bar Chart 5: Have your malware incidents increased over the past year?



Bar Chart 6 shows 35 percent of respondents say they have had more than 50 malware attempt incidents each month. Another 27 percent believe their organizations encounter between 25 to 50 malware attacks each month. On average, that means that there can be one or more malware attacks per day.

Bar Chart 6: How many malware incidents does your organization deal with monthly?

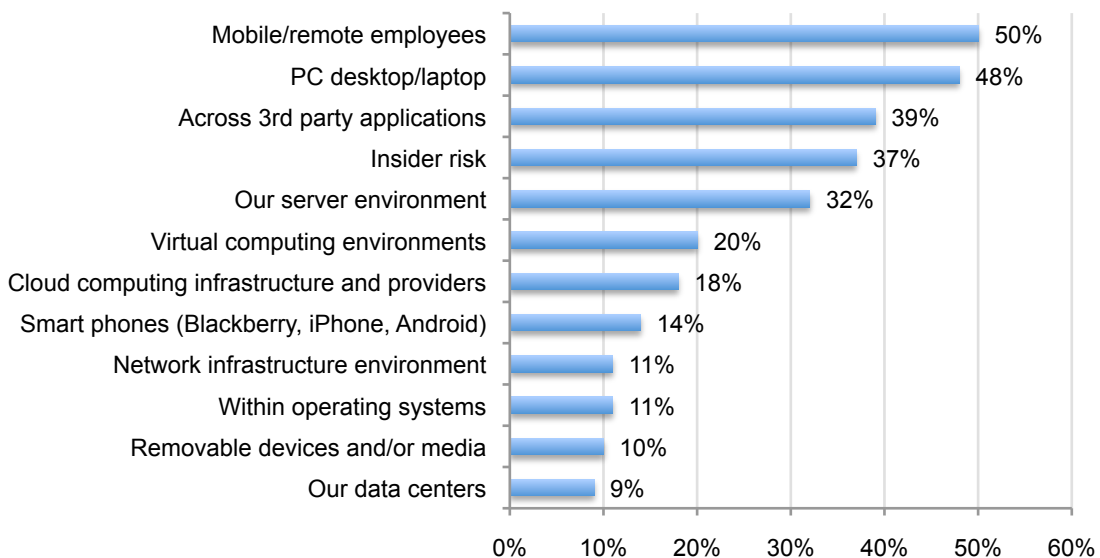


The endpoint risk environment is shifting from data centers, operating systems and network infrastructure to one that involves remote users, the PC and third-party applications. According to Bar Chart 7, respondents identified the following as the top three factors causing the greatest rise in IT risks: mobile/remote employees (50 percent), PC desktop/laptops (48 percent) and use of third-party applications (39 percent). Also creating greater risk are malicious or negligent insiders (37 percent) and the server environment (32 percent).

Only 11 percent say the network infrastructure environment (gateway to endpoint) and vulnerabilities within their operating systems are driving greater potential IT risks. Also fewer respondents (10 percent) say removable devices such as USB sticks and/or media such as CDs and data centers are contributing to IT risks.

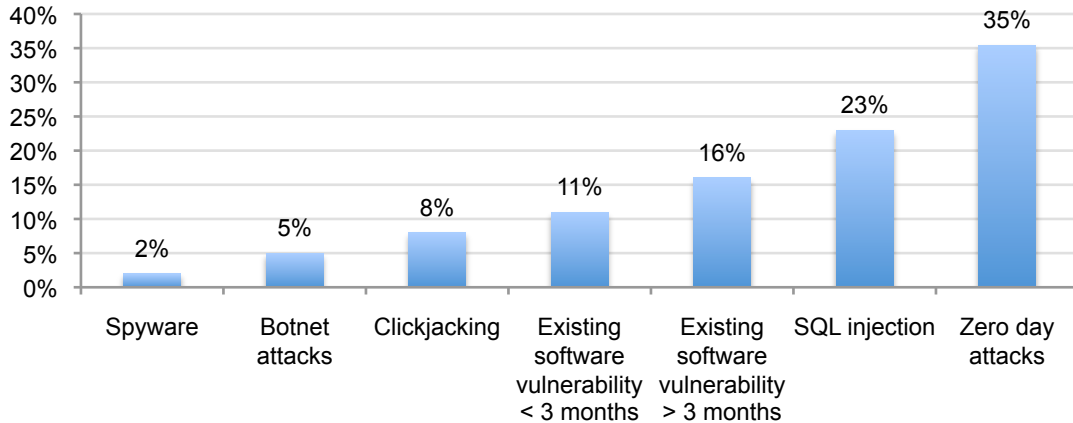
Bar Chart 7: Where are you seeing the greatest rise of potential IT risk?

Top three choices



As shown as Bar Chart 8, the top three incidents that present the most difficult challenges for respondents are zero day attacks (35 percent), SQL injections (23 percent) and the exploit of existing software vulnerabilities greater than three months old (16 percent).

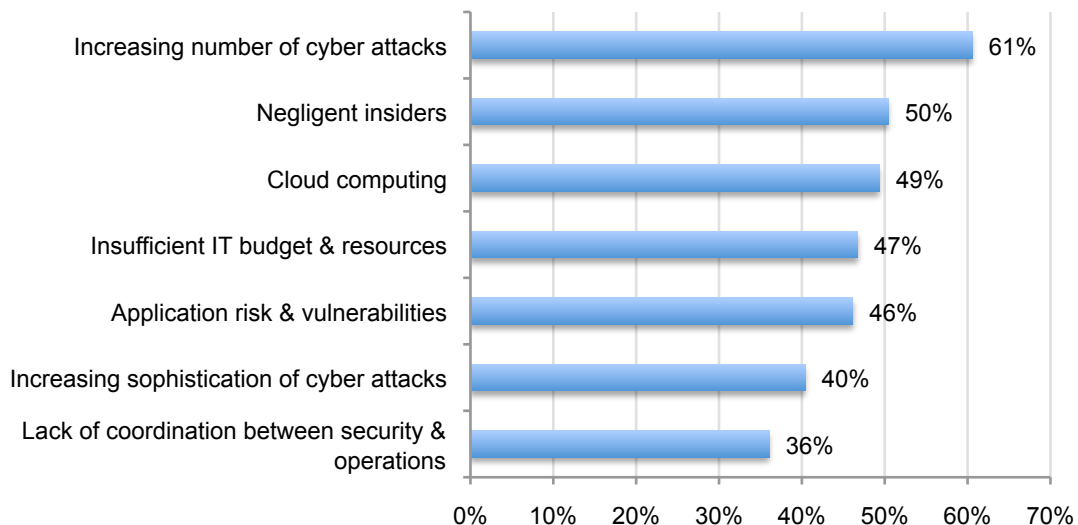
Bar Chart 8: Which one incident represents your biggest headache?



Bar Chart 9 lists in descending order what respondents perceive as the seven most serious security risks their organizations will face in the near future. Respondents predict the top three IT security risks in the next 12 months will be: an increasing volume of cyber attacks and malware incidents (61 percent), negligent insiders/employees (50 percent) and cloud computing (internal & third party providers). Considered to be of less concern are: targeted attacks on smart phone platforms (i.e., iPhone, Blackberry, Android) (15 percent), virtualization on server-side (13 percent) and operating system vulnerability (11 percent).

Bar Chart 9: Which of the following poses the greatest IT security risks over the next year?

Top three concerns

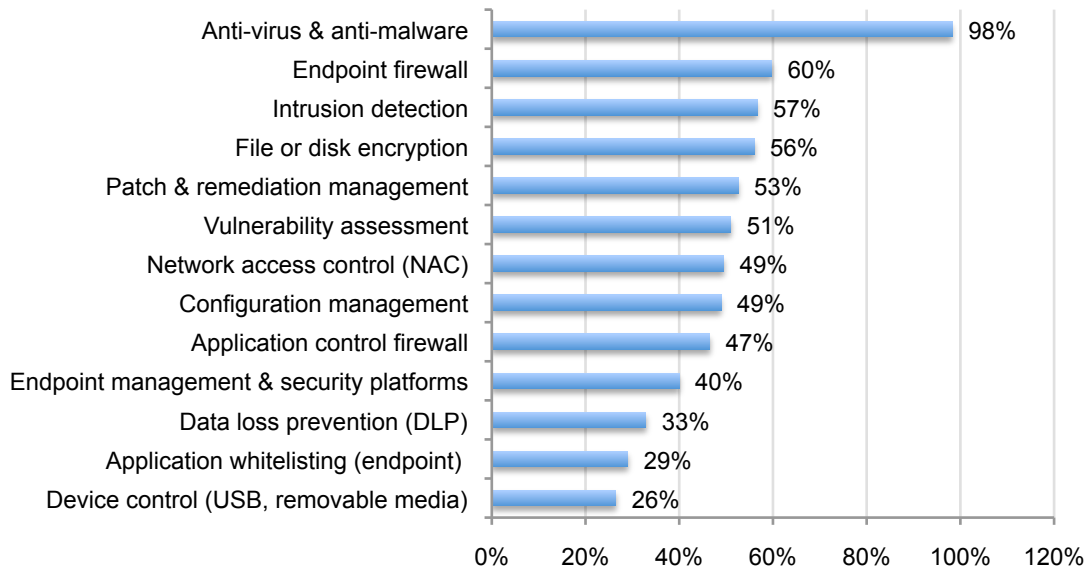


How organizations are investing in IT security readiness

Organizations in this study seem to be staying with what they may consider the “tried and true” technologies and approaches to managing their information risks. However, based on a comparison of Bar Chart 10 and Bar Chart 11 what they are using may not be the ones they consider most effective.

According to Bar Chart 10, nearly everyone (98 percent) has anti-virus and anti-malware technologies in place followed by endpoint firewalls (60 percent) and intrusion detection systems (57 percent). Only 26 percent say they have security device controls in place for USB and removable media. That response is consistent with the finding that only 10 percent of respondents consider USB sticks and other removable media are contributing to IT risk.

Bar Chart 10: Which endpoint technologies does your organization currently use?

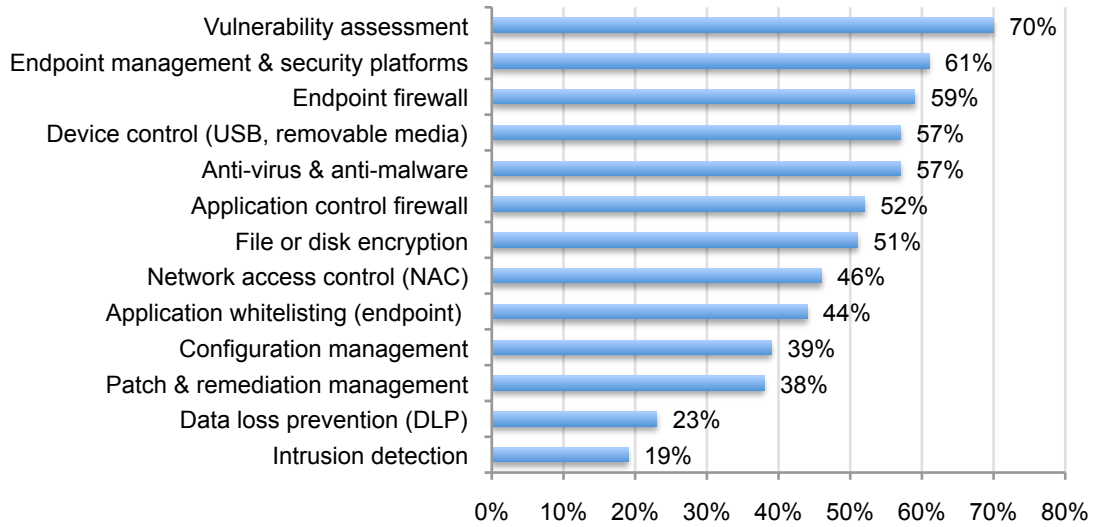


While not shown in a chart, respondents say their organizations basically will stay the course when investing in endpoint security during the next 12 months. The technologies with the greatest increase in investment are application control firewalls (increase of 10 percent), application whitelisting (increase of five percent) and vulnerability assessment (an increase of four percent). Investment in endpoint management and security suites and platforms is expected to decrease by six percent.

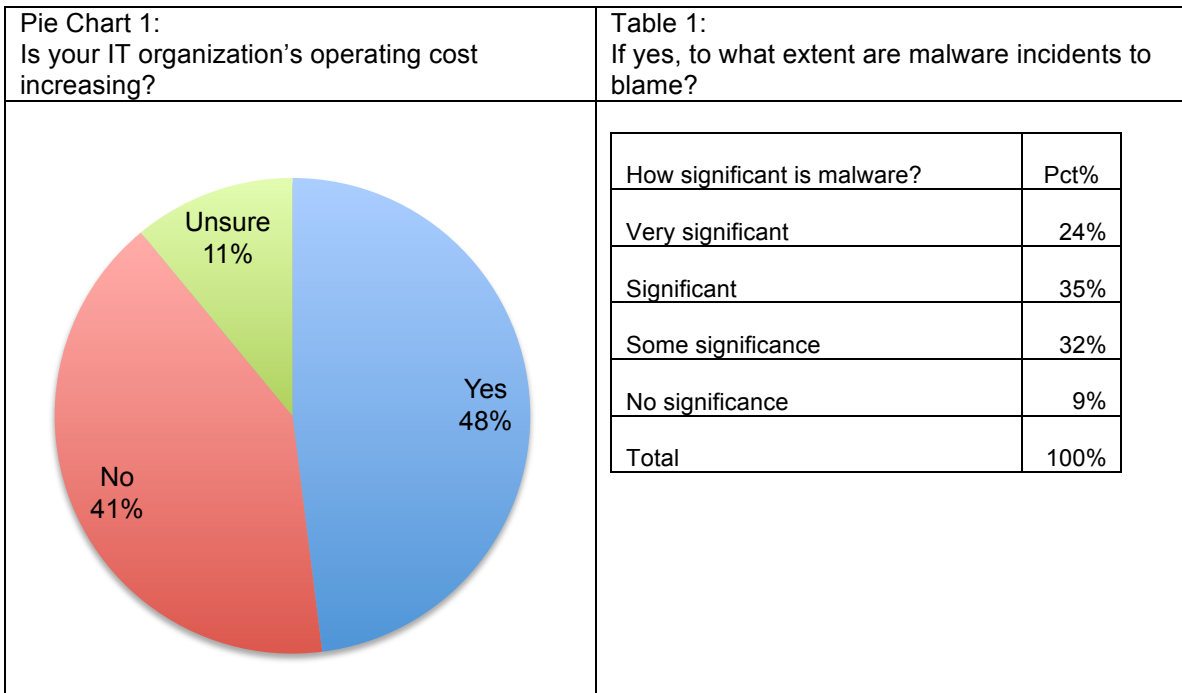
Respondents also reveal what we refer to as the gap between the technologies used and the technologies considered most effective. If you compare Bar Chart 10 with Bar Chart 11, this gap exists with the following: vulnerability assessment (used by 51 percent but considered effective by 70 percent), application whitelisting (used by only 29 percent but considered effective by 44 percent), device control (used by 26 percent but considered effective by 57 percent) and endpoint management & security suites platform (used by 40 percent but considered effective by 61 percent). As noted above, organizations will increase investment in application whitelisting and vulnerability assessments but will decrease their investment in endpoint management and security suites and platforms.

Bar Chart 11: Which endpoint technologies are most effective?

Includes respondents who acknowledge their organizations currently uses this technology

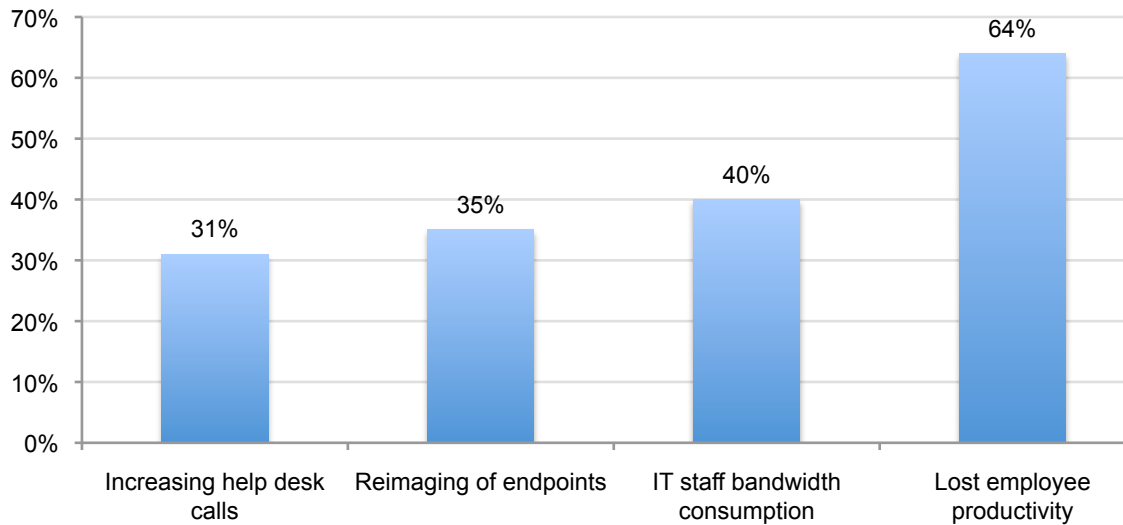


IT operating expenses are increasing according to 48 percent of respondents. However, 11 percent are unsure. Among those who say their expenses are increasing, 24 percent say the increase is very significant, 35 percent say it is significant and 32 percent say it is somewhat significant all due to malware incidents.



According to Bar Chart 12, the two main cost drivers are lost employee productivity (64 percent) and IT staff bandwidth consumption (40 percent). With respect to bandwidth, this has become a critical issue as IT and end-users access Internet sites that provide rich content such as videos.

Bar Chart 12: What are the main cost drivers to increasing IT operating expenses?

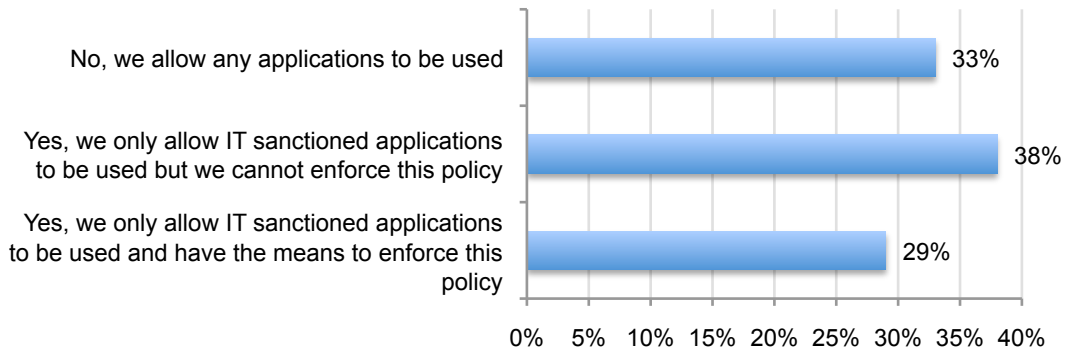


How respondents are addressing endpoint application risks

According to respondents, what concerns them most about reducing the endpoint risk are preventing applications from being installed or executing on their endpoints, discovering what applications are residing on the network and ensuring that vulnerable applications are patched.

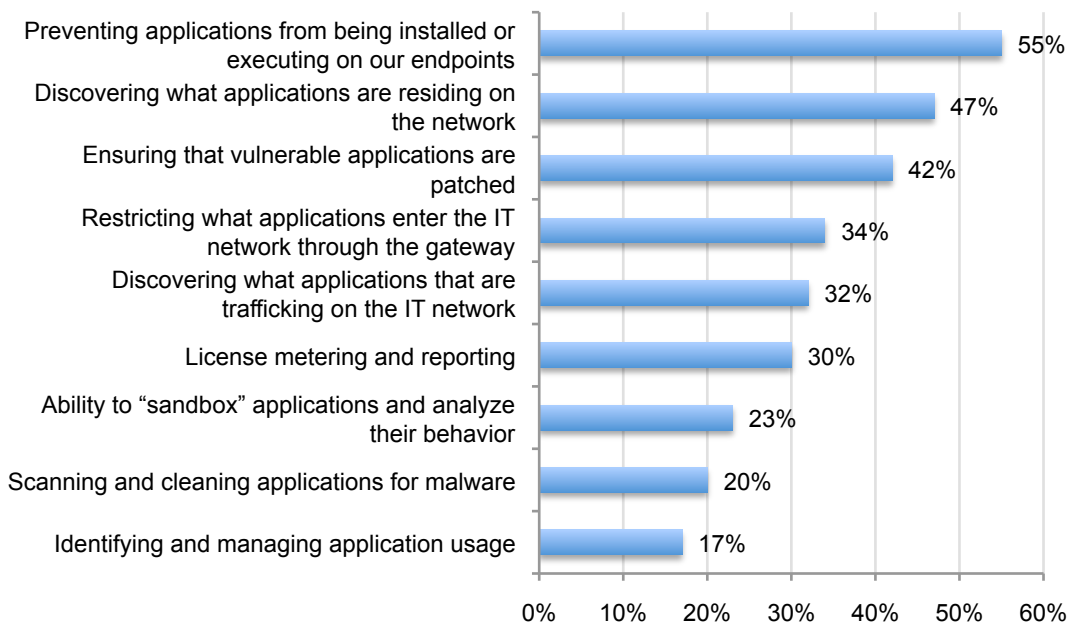
They are, however, leaving their endpoints vulnerable by allowing the indiscriminate use of applications or not enforcing policies governing the appropriate use of applications. As shown in Bar Chart 13, 38 percent of respondents have policies regarding application installation and usage but do not enforce them and one-third of organizations allow any applications to be used.

Bar Chart 13: Does your organization have application installation and usage policies?



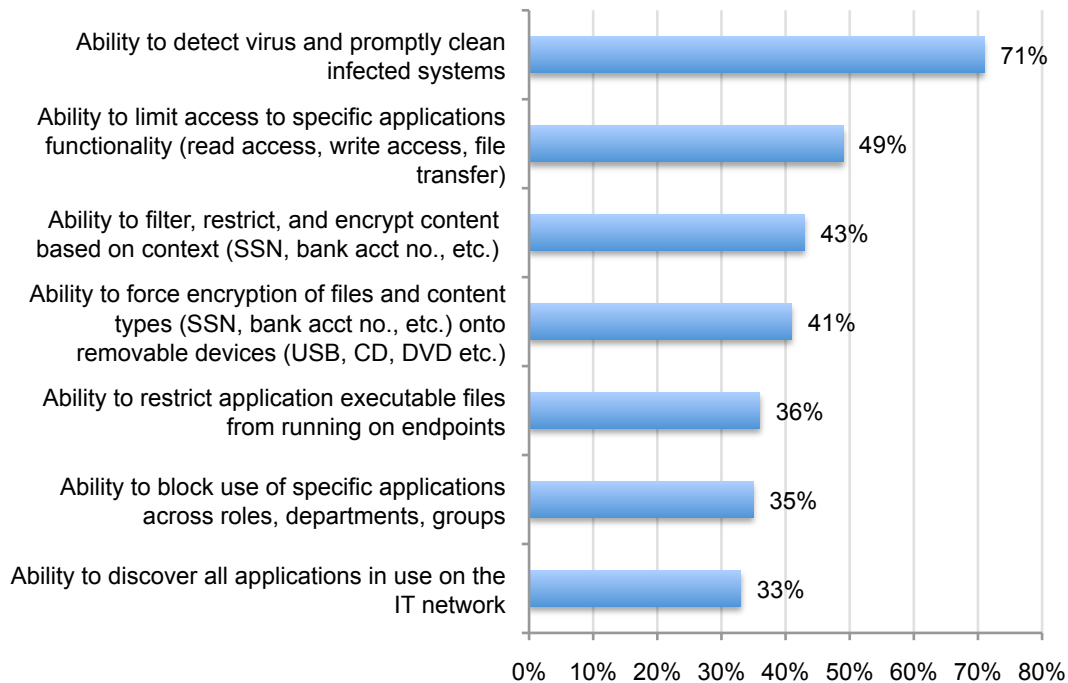
As discussed above, Bar Chart 14 shows the top three challenges with respect to their endpoint applications are: preventing applications from being installed or executing on their endpoints (55 percent), discovering what applications are residing on the network (47 percent) and ensuring that vulnerable applications are patched (42 percent). Another challenge is scanning and cleaning applications for malware infection (20 percent) and identifying and managing application usage (17 percent).

Bar Chart 14: With respect to endpoint applications, what are the greatest challenges?
Top three choices



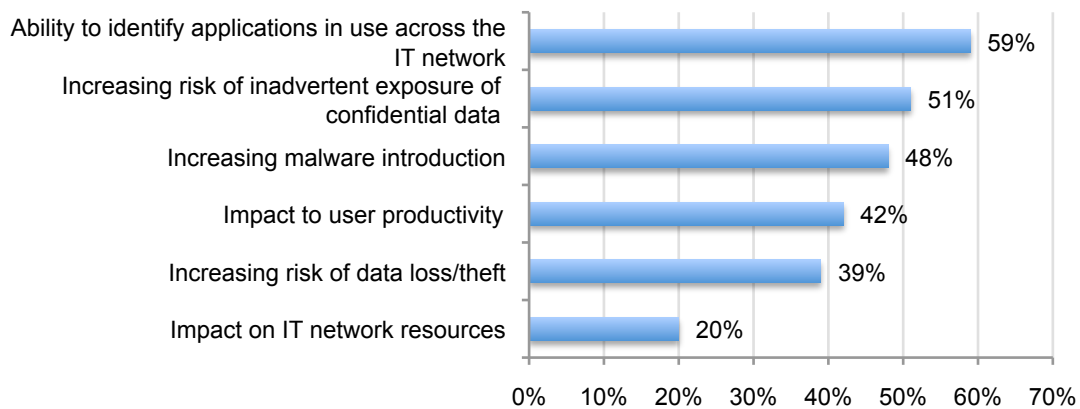
According to Bar Chart 15, respondents say they have the following capabilities in place or plan to implement in the next 12 months: ability to detect virus and promptly clean infected systems (71 percent), ability to limit access to specific applications functionality (read access, write access, file transfer) (49 percent) and ability to filter, restrict, and encrypt content based on context (SSN, bank account number) (43 percent) and ability to force encryption of files and content types (SSN, bank account number) onto removable devices (USB, CD, DVD) (41 percent).

Bar Chart 15: What application management capabilities does your organization have?

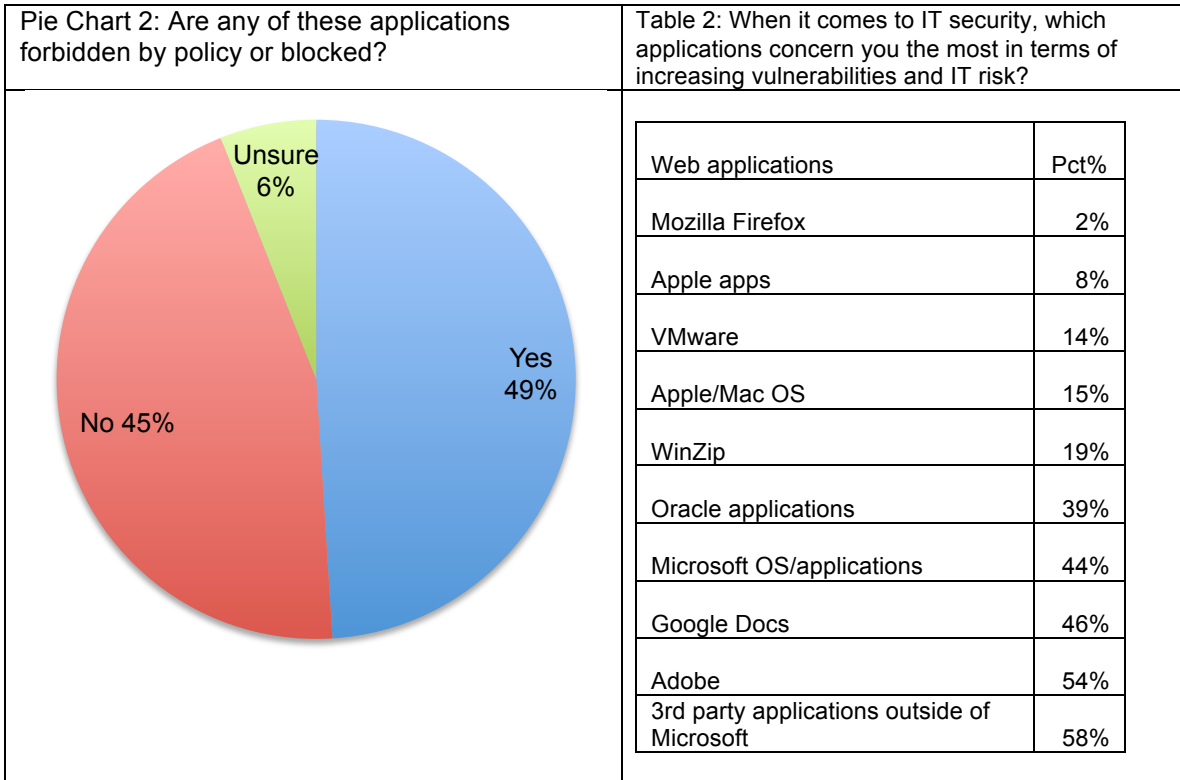


The concern respondents have about negligent and malicious insiders is reflected in their response to how Web 2.0/social media will affect their information risk environment. Bar Chart 16 shows that the top Web 2.0/social media challenges facing respondents' organizations are: ability for IT to identify applications in use across the IT network (59 percent), ability to manage the risk of inadvertent exposure of data (51 percent) and increasing malware (48 percent).

Bar Chart 16: Which Web 2.0 challenges are of greatest concern?

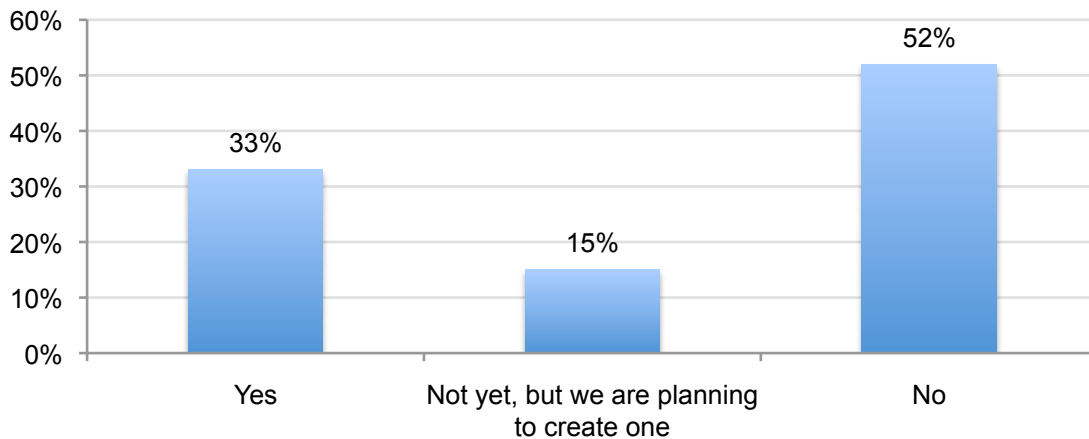


The top three Web applications in terms of risk to the organization are: general third-party applications outside of Microsoft, Adobe (54 percent), and Google documents. Respondents believe Apple apps (8 percent) and Mozilla Firefox (2 percent) are considered the least risky. Forty-nine percent say they block these risky applications and six percent are unsure.



Twenty-six percent have not changed their priorities regarding patch/vulnerability management. Fifty-two percent say they do not have a dedicated team for patch/vulnerability management. One-third of respondents say they do have a dedicated team and 15 percent are planning to create one.

Bar Chart 17: Do you have a dedicated team for patch/vulnerability management?



Part 3. Implications for organizations

The information risk environment is shifting and as a result requires new technologies and approaches to managing endpoint risk. Respondents in this study acknowledge that the new risk environment is characterized by malware attacks that can occur on a daily basis and cyber attacks that are difficult to detect and prevent. In addition, there are negligent or malicious insiders who have access to third-party and Web 2.0/social media applications that can put an organization's endpoints at greater risk. The following are recommendations based on the findings from this study:

- Consider investing in technologies that will be the most effective in addressing malware and cyber attacks.
- Create policies that address the acceptable use of third-party and Web 2.0 applications in the workplace and when working remotely. Have mechanisms in place to enforce these policies.
- Implement training and awareness programs on the importance of using only IT sanctioned applications in the workplace and when working remotely.
- Recruit IT personnel skilled in dealing with cyber and malware attacks. These threats are acknowledged to be the most difficult to detect and prevent. Many consider these threats will increase in frequency and sophistication.
- Convince senior management of the perils of ignoring the threats of a new information risk environment and the need for resources to put the appropriate technologies and personnel in place.

Part 4. Methods

A sampling frame of 11,896 adult-aged individuals who reside within the United States was used to recruit and select participants to this survey. Our randomly selected sampling frame was built from several proprietary lists of experienced IT and IT security practitioners. In total, 782 respondents completed the survey. Of these returned instruments, 65 failed reliability checks. A total of 717 surveys were deemed usable. Applying four screening questions that assessed the respondents' experience and knowledge about IT endpoint risk resulted in a final sample of 564, or a 4.7 percent response rate. The average completion time per survey was 22.4 minutes.

Table 3: Survey response	Freq.	Pct%
Total sampling frame	11,896	100.0%
Bounce-backs	1,875	15.8%
Total survey responses	782	6.6%
Rejected surveys	65	0.5%
Final sample before screening	717	6.0%
Final sample	564	4.7%

Pie Chart 3 reports the primary industry sector of respondents' organizations. As shown, the largest segments include financial services (19 percent), public sector (13 percent), and healthcare and pharmaceuticals (11 percent).

Pie Chart 3: Industry distribution of respondents' organizations

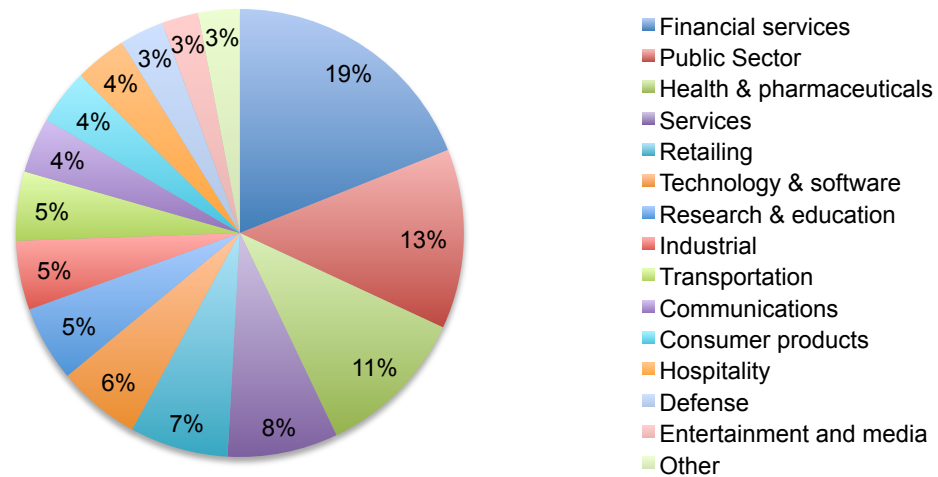


Table 4 reports the respondent organization's global headcount. As shown, a majority of respondents work within companies with more than 1,000 employees. Over 62 percent of respondents are located in larger-sized companies with more than 5,000 employees.

Table 4. The worldwide headcount of respondents' organization	Pct%
Less than 500 people	6%
500 to 1,000 people	13%
1,001 to 5,000 people	19%
5,001 to 25,000 people	32%
25,001 to 75,000 people	21%
More than 75,000 people	9%
Total	100%

Table 5 reports the respondent's primary reporting channel. As can be seen, 50 percent of respondents are located in the organization's IT department (led by the company's CIO). Twenty-one percent report to the company's security officer or CISO.

Table 5. Respondents' primary reporting channel	Pct%
Chief Information Officer	50%
Chief Information Security Officer	21%
Chief Compliance Officer	9%
Chief Security Officer	6%
Chief Risk Officer	5%
Chief Financial Officer	2%
General Counsel	2%
Human Resources VP	2%
Other	2%
CEO/Executive Committee	1%
Total	100%

Table 6 reports the respondent organization's global footprint. As can be seen, a large number of participating organizations are multinational companies that operate outside the United States, Canada and Europe.

Table 6: Geographic footprint of respondents' organizations.	Pct%
United States	100%
Canada	63%
Europe	68%
Middle East	19%
Asia-Pacific	41%
Latin America (including Mexico)	29%
Africa	8%

Table 7 reports the approximate position level or title of respondents. As shown, a majority of respondents state they are at or above the manager level (51 percent). The mean experience of respondents in this study is 8.93 years and the median is 8.5 years.

Table 7: Respondent's self-reported position level	Pct%
Senior Executive	2%
Vice President	1%
Director	23%
Manager	25%
Supervisor	19%
Technician	16%
Staff	9%
Contractor	3%
Other	2%
Total	100%

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. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.
- 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 Responses

Following are the survey results for a final sample of 564 IT and IT security practitioners. Fieldwork concluded on October 16, 2010.

Survey response	Freq.	Pct%
Total sampling frame	11896	100.0%
Bounce-backs	1875	15.8%
Total survey responses	782	6.6%
Rejected surveys	65	0.5%
Final sample	717	6.0%
Final sample after screening	564	4.7%

Part 1. Screening		
S1. What best describes your level of involvement in endpoint security within your organization?	Freq.	Pct%
None (stop)	27	4%
Low (stop)	13	2%
Moderate	77	11%
Significant	398	56%
Very significant	202	28%
Total	717	100%

S2. What best describes the number of employees (end users) who have access to your organization's network?	Freq.	Pct%
Less than 50 (stop)	19	3%
51 to 100	6	1%
101 to 500	53	8%
501 to 1,000	118	17%
More than 1,000	481	71%
Total	677	100%

S3. What best describes your role within your organization's IT department?	Freq.	Pct%
IT management	135	21%
IT operations	146	22%
Data administration	81	12%
IT compliance	57	9%
IT security	183	28%
Applications development	35	5%
I'm not involved in my organization's IT function (stop)	21	3%
Total	658	100%

S4. Please check all the activities that you see as part of your job or role.	Freq.	Pct%
Managing budgets	319	50%
Evaluating vendors	228	36%
Setting priorities	201	32%
Securing systems	260	41%
Ensuring compliance	159	25%
None of the above (stop)	73	11%
Final sample after screening	564	

Part 2: Attributions: Rating on a five-point scale	Strongly agree	Agree
Q1a. Our endpoint security operations are well managed.	17%	21%
Q1b. IT executives are supportive of our organization's endpoint security operations.	23%	18%
Q1c. We have ample resources to minimize IT endpoint risk throughout our organization.	17%	20%
Q1g. Our IT endpoint risk management procedures and policies are well documented.	18%	23%
Q1e. Our IT and security personnel are qualified to execute endpoint security operations.	23%	28%
Q1f. Existing blacklisting technologies (anti-virus/anti-malware) are effective in managing endpoint security risks.	16%	23%
Q1g. New whitelisting technologies make it easier to efficiently manage endpoint security risks.	19%	23%

Part 3: IT Risk	
Q2. Is your IT network more secure now than it was a year ago?	Pct%
Yes	36%
No	36%
Unsure	28%
Total	100%

Q3. Which of these types of incidents are you seeing frequently in your IT network? Check all that apply.	Pct%
Other	21%
Rootkits	23%
Clickjacking	25%
Exploit of existing software vulnerability greater than 3 months old	26%
Spyware	27%
Exploit of existing software vulnerability less than 3 months old	30%
Zero day attacks	34%
SQL injection	38%
Botnet attacks	64%
Web-borne malware attacks	75%
General malware	92%

Q4. Which one incident represents your biggest headache?	Pct%
Other	0%
Spyware	2%
Botnet attacks	5%
Clickjacking	8%
Exploit of existing software vulnerability less than 3 months old	11%
Exploit of existing software vulnerability greater than 3 months old	16%
SQL injection	23%
Zero day attacks	35%
Total	100%

Q5. Do you currently use virtual computing environments?	Pct%
Yes	70%
No	21%
Unsure	9%
Total	100%

Q6. Where are you seeing the greatest rise of potential IT risks within your IT environment? Choose only your top three choices.	Pct%
Our data centers	9%
Removable devices (USB sticks) and/or media (CDs, DVDs)	10%
Within operating systems (vulnerabilities)	11%
Network infrastructure environment (gateway to endpoint)	11%
Smart phones (Blackberry, iPhone, Android)	14%
Cloud computing infrastructure and providers	18%
Virtual computing environments (servers, endpoints)	20%
Our server environment	32%
Insider risk (malicious and accidental)	37%
Across 3rd party applications (vulnerabilities)	39%
Our PC desktop/laptop	48%
Mobile/remote employees	50%
Total	299%

Q7. Which of the following incidents happened during the past year in your IT environment? Check all that apply.	Pct%
Denial of service attack	11%
Targeted cyber attacks	26%
Cyber attack on mobile platform	37%
Loss of sensitive data by a third-party	45%
Spyware network intrusion	46%
Botnet attack	56%
Loss of sensitive data by an malicious insider	61%
Loss of sensitive data by a negligent insider	89%
Theft of desktops, laptops or other devices	95%
Virus or malware network intrusion	98%

Q8. How many malware attempt incidents on average does your IT organization deal with monthly?	Pct%
Less than 5	6%
5 to 10	11%
10 to 25	21%
25 to 50	27%
More than 50	35%
Total	100%

Q9. Have your malware incidents increased over the last year?	Pct%
Yes, major increase	43%
Yes, but only slight increase	22%
No, they stayed the same	15%
No, they have decreased	9%
Not sure	11%
Total	100%

Q10. Which of the following do you think are the biggest IT security risks that your organization will face in the next 12 months? Check all that apply.	Pct%
Operating system vulnerabilities	11%
Virtualization on server-side	13%
Targeted attacks on smart phone platforms (iPhone, Blackberry, Android etc)	15%
Lack of integration between security and systems management software	20%
Malicious insiders/employees	19%
Targeted attacks on sensitive company data (advanced persistent threats)	24%
Virtualization on endpoints	26%
Increasing use of social media/web 2.0 applications	30%
Lack of coordination between IT security and IT operations organizations	36%
Increasing sophistication of cyber attacks	40%
Application risk (vulnerabilities)	46%
Insufficient IT resources (budget/personnel)	47%
Cloud computing (internal & 3rd party providers)	49%
Negligent insiders/employees	50%
Increasing volume of cyber attacks and malware incidents	61%

Part 4. IT System Environment	
Q11. Which of the following technologies does your organization currently use? Check all that apply.	Pct%
Device control (USB, removable media)	26%
Application whitelisting (endpoint)	29%
Data loss/leak prevention (content filtering)	33%
Endpoint management & security suites/platforms	40%
Application control firewall (gateway)	47%
Configuration management	49%
Network access control (NAC)	49%
Vulnerability assessment	51%
Patch & remediation management	53%
File & disk encryption	56%
Intrusion detection	57%
Endpoint firewall	60%
Anti-virus & anti-malware	98%

Q12. Which of the following technologies does your organization plan to invest in over the next 12 months? Check all that apply.	Pct%
Device control (USB, removable media)	29%
Application whitelisting (endpoint)	34%
Endpoint management & security suites/platforms	34%
Data loss/leak prevention (content filtering)	35%
Patch & remediation management	50%
Configuration management	51%
Network access control (NAC)	51%
Vulnerability assessment	55%
Application control firewall (gateway)	57%
Intrusion detection	58%
File & disk encryption	60%
Endpoint firewall	63%
Anti-virus & anti-malware	98%

Q13. Which of the following technologies or approaches are most effective in meeting you're your IT risk mitigation requirements? Choose only your top three choices.	Pct%	Subset*
Intrusion detection	19%	19%
Data loss/leak prevention (content filtering)	8%	23%
Patch & remediation management	20%	38%
Configuration management	16%	39%
Application whitelisting (endpoint)	18%	44%
Network access control (NAC)	21%	46%
File & disk encryption	40%	51%
Application control firewall (gateway)	31%	52%
Anti-virus & anti-malware	56%	57%
Device control (USB, removable media)	5%	57%
Endpoint firewall	35%	59%
Endpoint management & security suites/platforms	13%	61%
Vulnerability assessment	35%	70%
*Only those who say they used this technology at present.		

Q14a. Are your IT operating expenses increasing?	Pct%
Yes	48%
No	41%
Unsure	11%
Total	100%

Q14b. If yes, to what extent are malware incidents to blame?	Pct%
Very significant	24%
Significant	35%
Some significance	32%
No significance	9%
Total	100%

Q15. If operating expenses are increasing, what are the main cost drivers?	Pct%
Increasing help desk calls	31%
Reimaging of endpoints	35%
IT staff bandwidth consumption	40%
Lost employee productivity	64%
Other	3%

Part 5. Application Centric Risk	
Q16. Does your organization currently have any polices regarding application installation and usage?	Pct%
Yes, we only allow IT sanctioned applications to be used and have the means to enforce this policy	29%
Yes, we only allow IT sanctioned applications to be used but we cannot enforce this policy	38%
No, we allow any applications to be used	33%
Total	100%

Q17. With respect to endpoint applications, what are your greatest challenges? Choose only your top three choices.	Pct%
Other	2%
Identifying and managing application usage	17%
Scanning and cleaning applications for malware	20%
Ability to “sandbox” applications and analyze their behavior	23%
License metering and reporting	30%
Discovering what applications that are trafficking on the IT network	32%
Restricting what applications enter the IT network through the gateway	34%
Ensuring that vulnerable applications are patched	42%
Discovering what applications are residing on the network	47%
Preventing applications from being installed or executing on our endpoints	55%
Total	302%

Q18. Which of these application management capabilities does your organization currently have in place or plan to implement in the next 12 months? Choose all that apply.	Pct%
Ability to discover all applications in use on the IT network	33%
Ability to block use of specific applications across roles, departments, groups	35%
Ability to restrict application executable files from running on endpoints	36%
Ability to force encryption of files and content types (SSN, bank acct no., etc.) onto removable devices (USB, CD, DVD etc.)	41%
Ability to filter, restrict, and encrypt content based on context (SSN, bank acct no., etc.)	43%
Ability to limit access to specific applications functionality (read access, write access, file transfer)	49%
Ability to detect virus and promptly clean infected systems	71%

Q19. Which of these potential web 2.0/social media challenges is most concerning to your IT organization? Choose only your top three choices.	Pct%
No concerns about web 2.0/social media usage	10%
Increasing operating expenses	15%
Loss of trade secrets or intellectual property	16%
Impact on IT network resources (help desk, bandwidth, etc.)	20%
Increasing risk of data loss/theft	39%
Impact to user productivity (increasing personal use)	42%
Increasing malware introduction	48%
Increasing risk of inadvertent exposure of confidential data	51%
Ability for IT to identify applications in use across the IT network	59%
Total	300%

Q20. Have your patch/vulnerability management priorities changed in the last year?	Pct%
Yes, we are now more focused on PC's (desktops/laptops) as a priority	22%
Yes, we are now more focused on Servers	6%
We prioritize Servers and PC's equally	16%
We have no prioritization for IT environments	9%
We don't centrally manage the patch process	20%
Our priorities have not changed in the last year	26%
Total	100%

Q21a. When it comes to IT security, which applications concern you the most in terms of increasing vulnerabilities and IT risk? Choose only your top three choices.	Pct%
Mozilla Firefox	2%
Apple apps (Quicktime, iTunes, etc.)	8%
VMware	14%
Apple/Mac OS	15%
WinZip	19%
Oracle applications	39%
Microsoft OS/applications	44%
Google Docs	46%
Adobe (Flash, Adobe Reader, etc.)	54%
General 3rd party applications outside of Microsoft	58%
Total	300%

Q21b. Consequently, are any of these applications you checked in the question above forbidden by policy or blocked?	Pct%
Yes	49%
No	45%
Unsure	6%

Q22. Do you have a dedicated team for patch/vulnerability management?	Pct%
Yes	33%
Not yet, but we are planning to create one	15%
No	52%
Total	100%

Part 6. Application Control/Whitelisting	
Q23. How effective do you believe that your current anti-virus/anti-malware technology is in protecting your IT endpoints from today's malware risk?	Pct%
Very effective	12%
Effective	28%
Somewhat ineffective	27%
Not effective	33%
Total	100%

Q24. Do believe anti-virus/anti-malware will remain a major part of your overall IT defenses for the next three years?	Pct%
Yes	33%
No	26%
Unsure	41%
Total	100%

Q25a. Do you currently augment your anti-virus/anti-malware with any of the following? Please check all that apply? Leave blank if no.	Pct%
Whitelisting	23%
Automatic backup and recovery	29%
Encryption	36%
Intrusion detection	41%
Firewalls	69%
Other	198%

Q25b. Are you thinking about augmenting your anti-virus/anti-malware technology with other endpoint security technologies?	Pct%
Yes	50%
No	29%
Unsure	21%

Q26. What is your level of understanding of today's application whitelisting technology?	Pct%
Deep understanding of the technology and its use	21%
General understanding	60%
Some awareness, but have little understanding	11%
Not aware of the technology	8%
Total	100%

Q27. Are you currently using application whitelisting technology in your IT environment?	Pct%
Yes	13%
Yes, but only in limited environments (servers, POS etc.) only	16%
No	63%
Unsure	8%
Total	100%

Q28. Are you planning to pilot or expand your usage of application whitelisting technologies on your endpoint environment in the next 12 months?	Pct%
Yes	19%
Likely	32%
No	39%
Unsure	10%
Total	100%

Q29. What concerns do you have with adopting application whitelisting technologies for your IT endpoint environment? Choose only your top three choices.	Pct%
Application whitelisting technology is not suited to dynamic or constantly changing endpoint environments (desktops/laptops)	5%
Current application whitelisting technology cannot manage change well	6%
Application whitelisting technology will negatively impact productivity of our users (difficulty adding new apps, etc.)	15%
Application whitelisting technology will increase demands on IT (help desk, roll out, system integration)	13%
Application whitelisting technology does not integrate with existing security technologies (e.g., AV, patch management, etc.)	5%
Application whitelisting technology is not a recognized compliance alternative to AV	4%
Application whitelisting technology is too new for roll out for broader IT environments	4%
No concerns with using application whitelisting technology	46%
Would never adopt application whitelisting technology	2%
Total	100%

Q30. What price would you expect to pay for an application whitelisting solution?	Pct%
More than my current anti-virus cost per seat	5%
Equal to my current anti-virus cost per node	20%
Less than my current anti-virus cost per node	18%
Nothing as it should be part of my anti-virus solution	57%
Total	100%

Q31. Which IT brands do you associate with providing application whitelisting technology? (Select the top three):	Pct%
Other	5%
Savant	13%
BigFix	15%
Bit9	22%
Solidcore	29%
Securewave	30%
Checkpoint	30%
Palo Alto Networks	31%
Lumension	34%
McAfee	37%
Symantec	39%
Total	285%

Part 7: Organizational Characteristics & Demographics	
D1. What organizational level best describes your current position?	Pct%
Senior Executive	2%
Vice President	1%
Director	23%
Manager	25%
Supervisor	19%
Technician	16%
Staff	9%
Contractor	3%
Other	2%
Total	100%

D2. Is this a full time position?	Pct%
Yes	98%
No	2%
Total	100%

D3. Check the Primary Person you or your IT security leader reports to within the organization.	Pct%
CEO/Executive Committee	1%
Chief Financial Officer (CFO)	2%
General Counsel	2%
Chief Information Officer (CIO)	50%
Chief Information Security Officer (CISO)	21%
Compliance Officer	9%
Human Resources VP	2%
Chief Security Officer (CSO)	6%
Chief Risk Officer	5%
Other	2%
Total	100%

D4. Total years of relevant experience	Mean	Median
Total years of IT or security experience	8.93	8.50
Total years in current position	4.90	5.00

D5. Gender:	Pct%
Female	23%
Male	77%
Total	100%

D6. What industry best describes your organization's primary industry focus?	Pct%
Agriculture & Food Services	1%
Communications	4%
Consumer Products	4%
Defense	3%
Energy	2%
Entertainment and Media	3%
Financial Services	19%
Health & Pharmaceuticals	11%
Hospitality	4%
Industrial	5%
Public Sector	13%
Research & Education	5%
Retailing	7%
Services	8%
Technology & Software	6%
Transportation	5%
Total	100%

D7. Where are your employees located? Check all that apply.	Pct%
United States	100%
Canada	63%
Europe	68%
Middle East	19%
Asia-Pacific	41%
Latin America (including Mexico)	29%
Africa	8%

D8. What is the worldwide headcount of your organization?	Pct%
Less than 500 people	6%
500 to 1,000 people	13%
1,001 to 5,000 people	19%
5,001 to 25,000 people	32%
25,001 to 75,000 people	21%
More than 75,000 people	9%
Total	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.