State of the Endpoint

IT Security & IT Operations Practitioners in the United States, United Kingdom, Australia, New Zealand & Germany

Sponsored by Lumension

Independently conducted by Ponemon Institute LLC

Publication Date: November 30, 2009

State of the Endpoint

By Ponemon Institute, November 30, 2009

I. Executive Summary

State of the Endpoint study was conducted by Ponemon Institute to understand if IT security and IT operations practitioners believe the endpoint is more or less secure today. In addition, this study examines if these two groups have different perceptions about the risk resulting from insecure endpoints to networks and enterprise systems. This study is sponsored by Lumension.

The scope of this research includes respondents from five countries including: United States, United Kingdom, Germany, Australia and New Zealand.[1] In total, 1,427 respondents in IT security (hereafter referred to as security) and 1,582 respondents in IT operations (hereafter referred to as operations) provided usable survey returns.

Endpoint security involves protecting the enterprise's network from such threats as virus and malware attacks, cyber crime and employees' unauthorized use of mobile devices and illegal applications on organizations' laptops, desktops and other Internet connected devices.

This study reveals the challenges organizations face in managing the security risk to endpoints. According to the IT practitioners in our study, both in operations and security, the following are reasons why the endpoint in many organizations is so vulnerable:

- Organization's increasing use of technologies that improve productivity and reduce costs but create endpoint risks. These include open source software, Web 2.0 applications, cloud computing, virtualization and others. Moreover, the use of these technologies is expected to become more prevalent over the next 12 to 24 months. Especially cloud computing, Web 2.0 applications and virtualization.

- Employees connecting their own computing devices, such as laptops and PDAs, to the organization's network or enterprise system. A very small percentage of organizations in our study have a policy that permits this practice. As a result, organizations may not have control over who is accessing the network with illegal and unauthorized applications.

- Endpoint management systems are complex. According to the study, on average 3.7 software agents are installed on each endpoint to perform management security and other operations. In addition, they have on average 3.9 different or distinct software management consoles for endpoint operations.

- Respondents report a lack of skilled or knowledgeable personnel, followed by the misalignment of IT and business objectives and difficulty integrating multiple technologies as contributing to the challenge of managing the endpoint.

- The endpoints are constantly under siege by virus or malware network intrusions. According to respondents, this was the most frequent security incident during the past year.

- In many cases, not having adequate budget to invest in technologies and other resources, such as trained and knowledgeable employees, necessary to protecting the endpoint.

- Collaboration between IT security and IT operations in many organizations does not happen as frequently as it should. According to the findings of this study, these two groups tend to have different perceptions about such critical areas as knowing what technologies are used that could put the endpoint at risk and what the major security risks are to the network.

[1] In the analysis of survey returns, Australia and New Zealand are combined (termed ANZ).

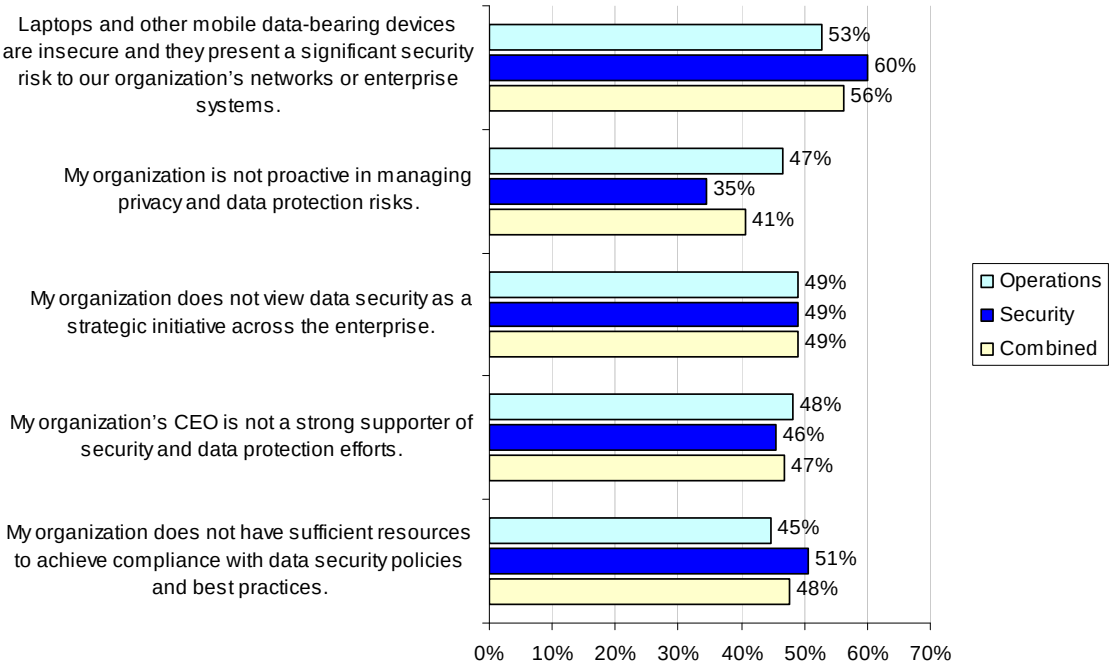
II. Key Findings

Following are the most salient findings of our study presented in a bar chart format.

Bar Chart 1 summarizes the strongly agree and agree response for respondents in the security and operations groups. [2] These attributions are used to assess the attitudes and beliefs of survey respondents. Please note these results are aggregated across five countries.

As can be seen, 56 percent of respondents recognize that laptops and other mobile data-bearing devices are insecure and present a significant security risk to their organization's networks or enterprise systems. Security practitioners are more concerned than operations about endpoint security (60 percent versus 53 percent).

Bar Chart 1
Attributions about endpoint security
Each bar reflects the strongly agree and agree response combined



Forty-one percent of respondents do not believe their organizations are proactive in managing privacy and data protection risks. Here, operations hold a more negative view than security about their organization's commitment in managing these risks. Other responses suggest a large number of respondents have concerns about their CEO's commitment to security and data protection, lack of sufficient resources to get the job done properly, and lack of a strategic orientation to managing security risk.

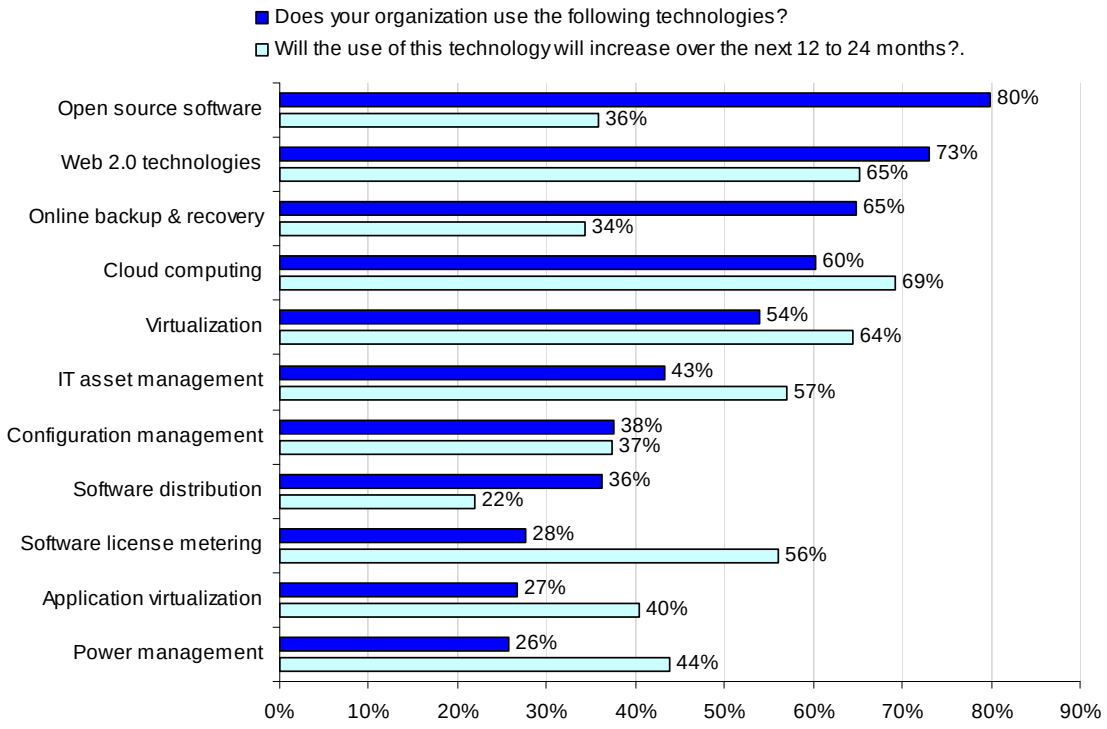
Bar Chart 2 reports 11 different technologies and summarizes the frequency of the use of each technology within respondents' organizations. It also reports the percentage of respondents who believe a given technology will increase in use over the next one or two years.

The information technologies currently in use and create endpoint risks for organizations include: open source software, Web 2.0 applications, cloud computing, virtualization and others. The

[2] Each attribution was negatively framed and reversed scored.

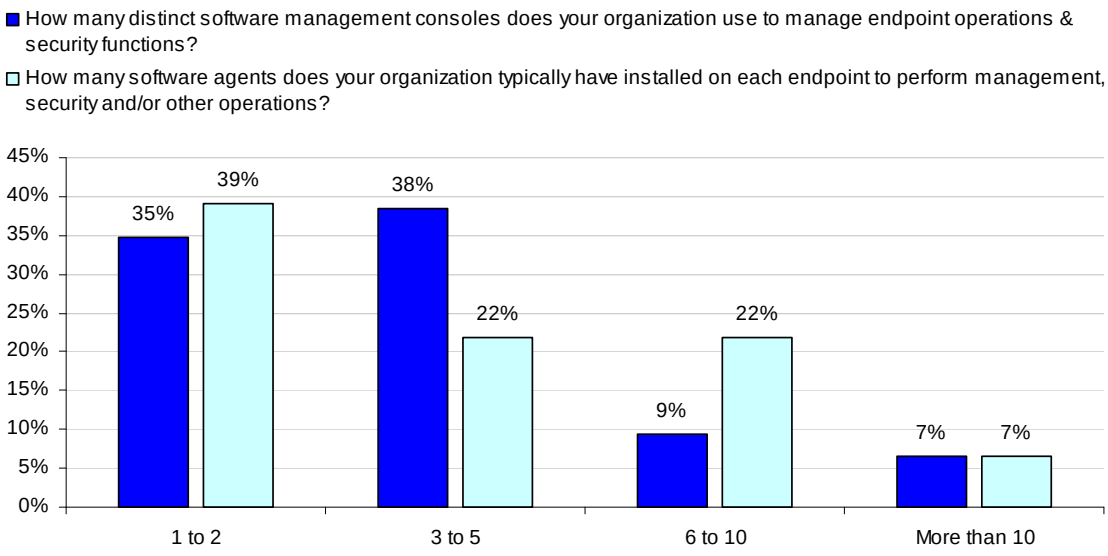
information technologies most often projected to increase in use over the next 12 to 24 months include cloud computing, Web 2.0 applications and virtualization.

Bar Chart 2
Technologies that affect endpoint security
Percentage Yes response



Bar Chart 3 reports the average number of agents contained on endpoint devices. It also reports the number of different or distinct consoles used for endpoint operations and security.

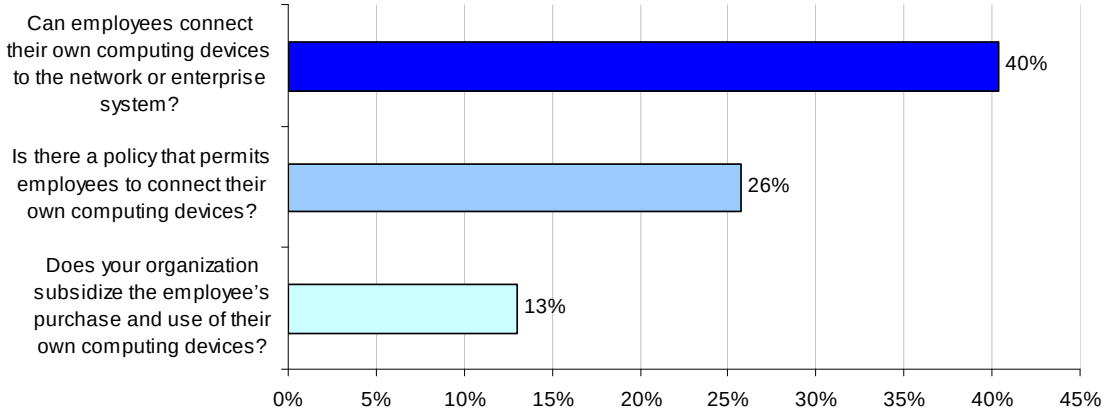
Bar Chart 3
Agents on endpoints and software management consoles



The large number of agents and consoles suggests the endpoint management systems of participating organizations are complex. Accordingly, they have, on average, 3.7 software agents installed on each endpoint to perform management, security and other operations. In addition, participating organizations have, on average, 3.9 different or distinct software management consoles for endpoint operations and security.

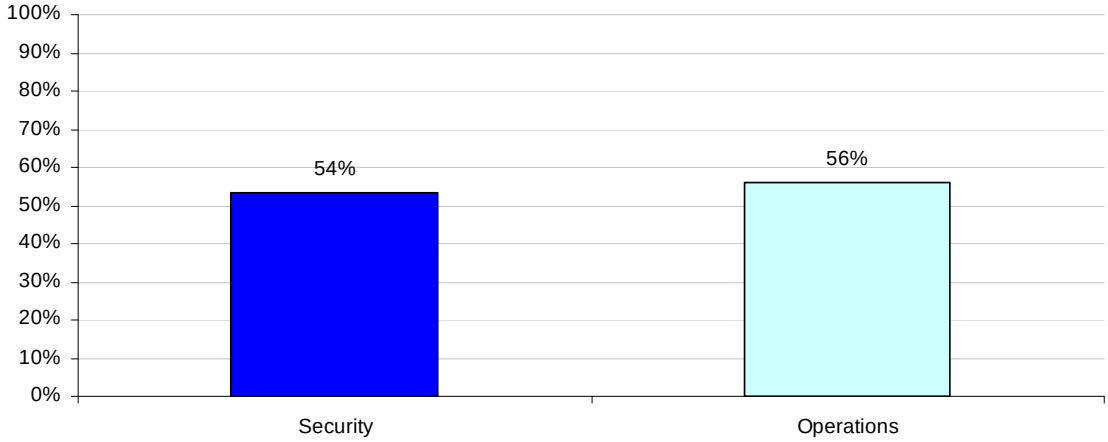
Bar Chart 4 shows 40 percent of respondents say their organizations permit employees to connect their own computing devices to its network or enterprise systems.[3] However, only 26 percent of organizations have a policy that permits organizations to connect their own computing devices to their organization's systems. This suggests many organizations are not taking appropriate steps to secure mobile devices owned by employees.

Bar Chart 4
Employee owned mobile data-bearing devices



As shown in Bar Chart 5, more than half of respondents in both the security and operations group believe their organization's IT network is more secure now than it was a year ago. However, there are significant differences across countries.

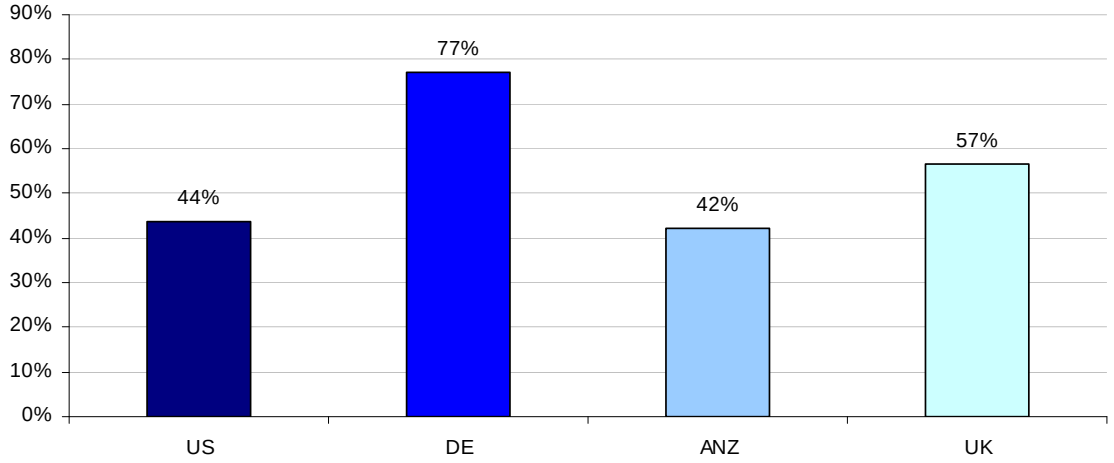
Bar Chart 5
Is your IT network more secure than it was a year ago?



[3] Analysis by country revealed a significant difference between security and operations in the US samples. Accordingly, 63 percent of operations versus only 37 percent of security practitioners said Yes to the question "Can employees connect their own computing devices to the network or enterprise systems?" This difference is further evidence of a gap between operations and security.

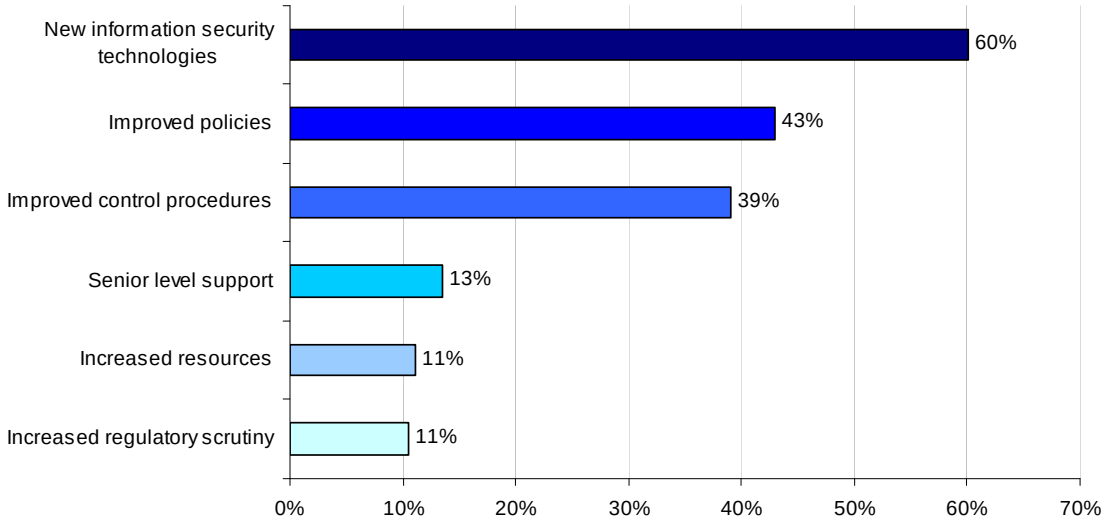
As shown in Bar Chart 6, German respondents hold the most favorable view, while respondents from the U.S. and ANZ have a less favorable view about their organization's IT network security.

Bar Chart 6
Is your IT network more secure than it was a year ago?
Analysis by country



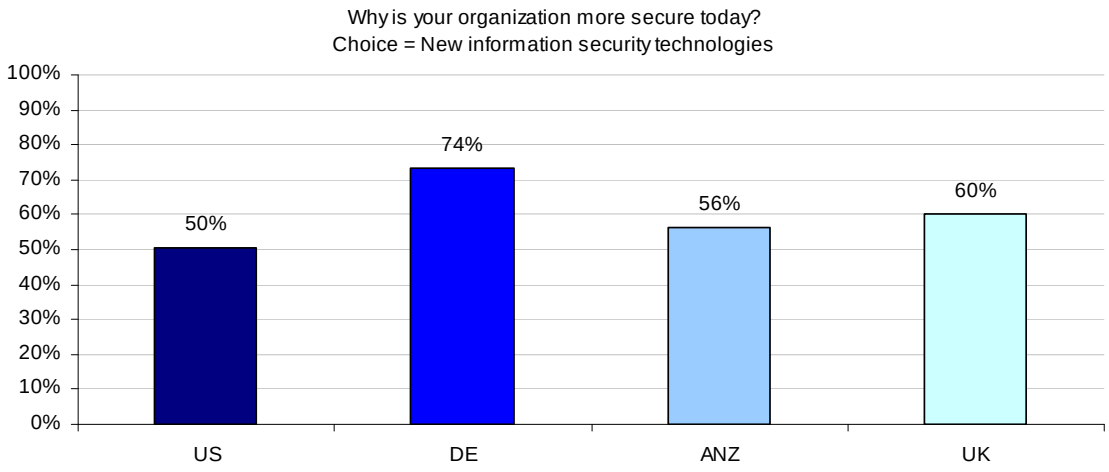
The number one reason why respondents believe their organizations' network security has improved over the past year concerns the availability of new information security technologies (60 percent), followed by improved policies (43 percent) and improved control procedures (39 percent).

Bar Chart 7
The reasons why IT networks are more secure now



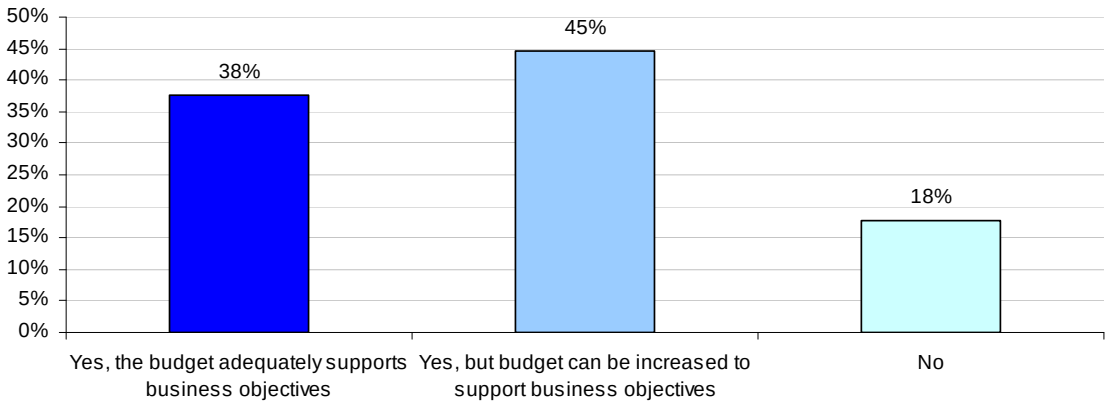
Bar Chart 8 shows results by country for the choice "new information security technologies." As shown, 74 percent of German respondents (as opposed to only 50 percent of U.S. respondents) rate this attribute as their number one reason for believe that their organization's IT networks are more secure today than one year ago.

Bar Chart 8
The reasons why IT networks are more secure now
Analysis by country for the choice "information security technologies"



Forty-five percent of respondents believe their organization's IT security budget is adequate but can be increased to support business objectives. Another 18 percent of respondents believe their organization's IT budget does not support business objectives. Hence, the majority of respondents do not see their organization's IT security budget as adequate (see Bar Chart 9).

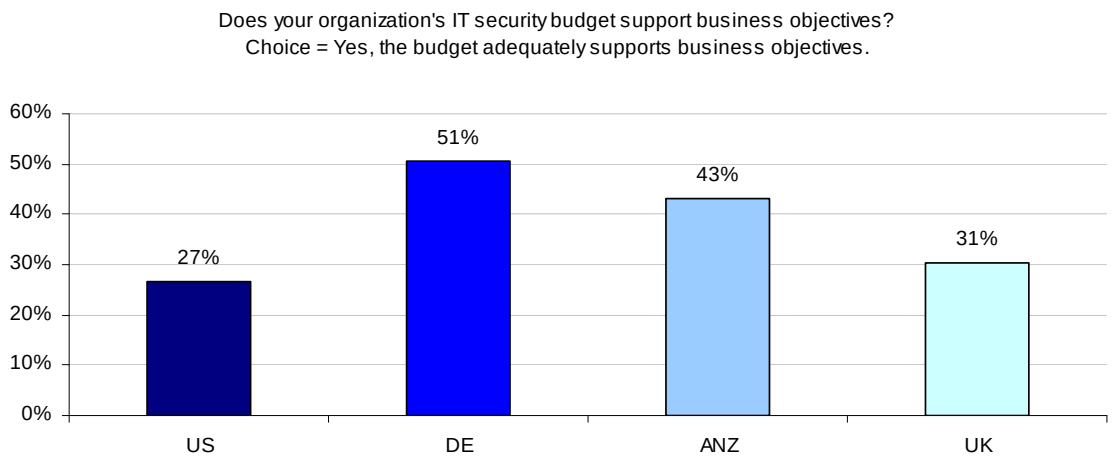
Bar Chart 9
Does your organization's IT security budget support business objectives?



Furthermore, the perception about the adequacy of the organization's security budget varies by country. Specifically, German respondents are more likely, and U.S. respondents are much less likely, to perceive the organization's IT security budget as adequate.

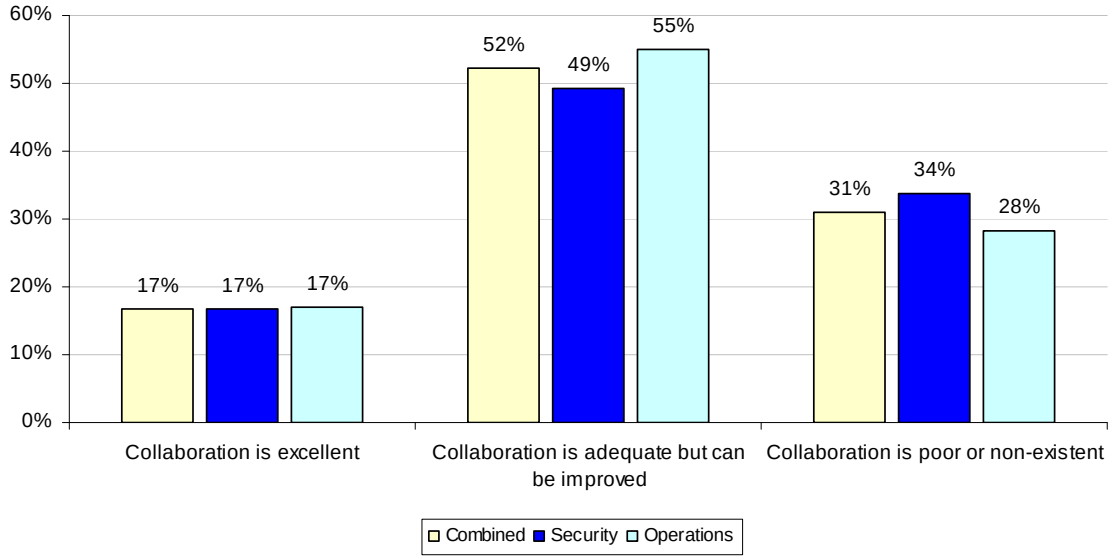
As shown in Bar Chart 10. U.S. respondents have the most negative view (27 percent) and German respondents have the least negative view (51 percent) about the sufficiency of the organization's IT security budget.

Bar Chart 10
Does your organization's IT security budget support business objectives?
Analysis by country



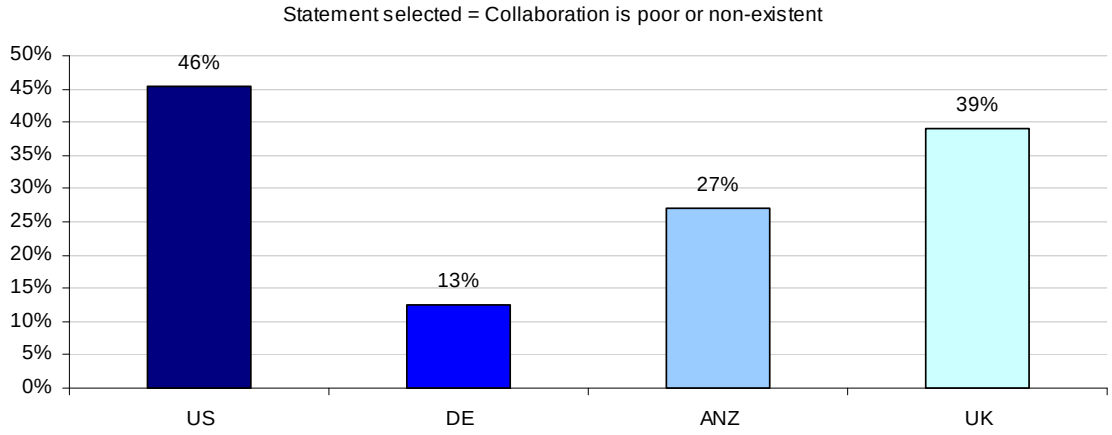
Bar Chart 11 shows that only 17 percent of respondents see collaboration between security and operations as excellent. More than 52 percent of respondents believe collaboration between security and operations can be improved, and 31percent believe collaboration between security and operations is poor or non-existent within their organizations.

Bar Chart 11
What statement best describes how IT operations and IT security work together?



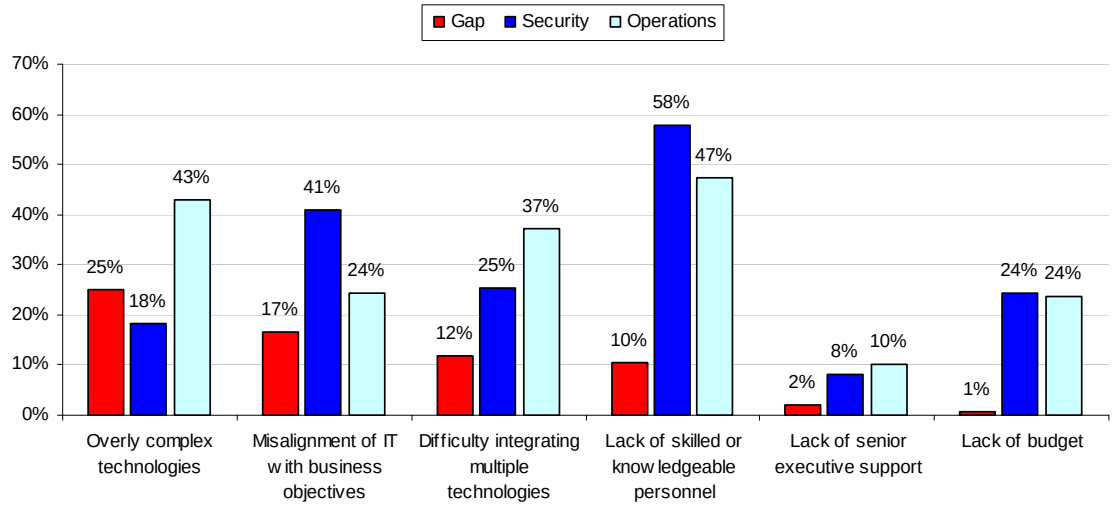
As shown in Bar Chart 12, respondents in the U.S. hold the most negative view, and German respondents hold the least negative view, about how well security and operations work together to support planning, communications, and information sharing functions. As shown, more than 46 percent of US respondents believe collaboration between security and operations is poor or non-existent. In contrast, only 13 percent of German respondents see collaboration between security and operations as poor or non-existent. This finding suggests that cultural impediments within U.S. organizations appear to stymie collaboration between security and operations, which could have a negative impact on the ways endpoint are managed and kept secure.

Bar Chart 12
What statement best describes how IT operations and IT security work together?
Analysis by country



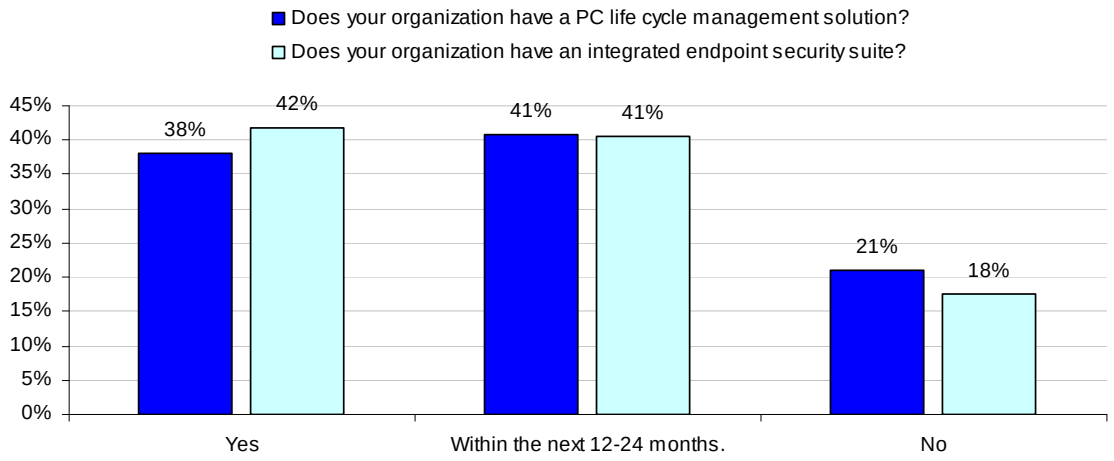
Bar Chart 13 shows the main difficulties in managing endpoint operations and security. The number one difficulty concerns the lack of skilled or knowledgeable personnel, followed by the misalignment of IT and business objectives, and difficulty integrating multiple technologies. There are significant gap areas or differences (noted in red) between respondents in security and operations. The three largest gaps between the security and operations groups include: overly complex technologies, misalignment of IT with business objectives, and difficulty integrating multiple technologies.

Bar Chart 13
Difficulties in managing endpoint operations and security



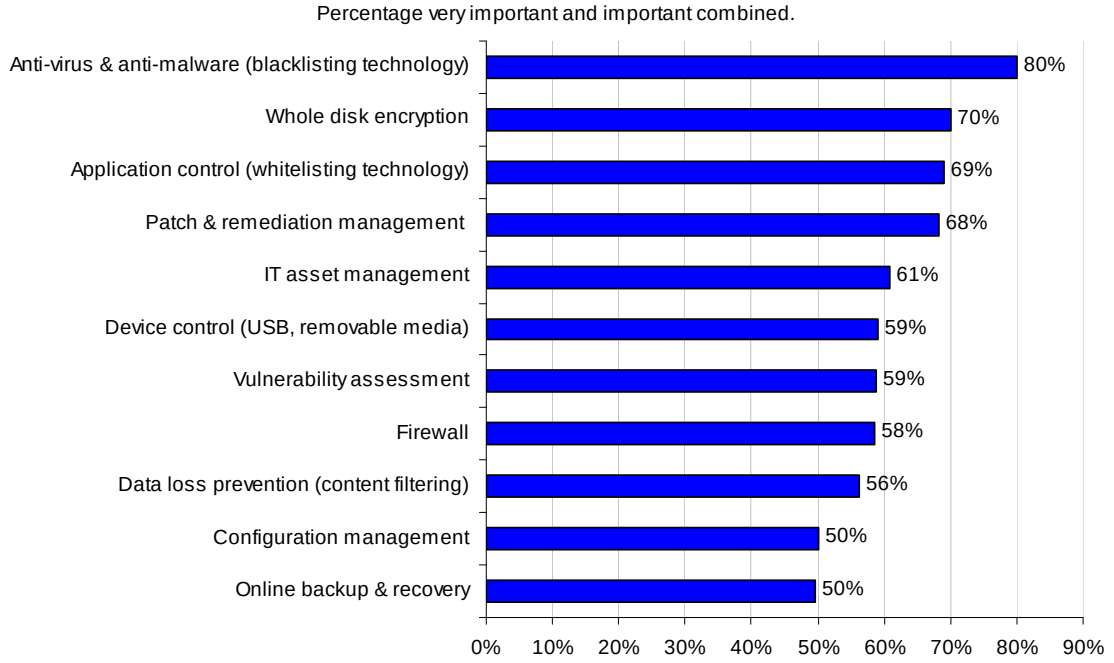
According to Bar Chart 14, respondents say they have (38 percent) or will have (41 percent) within the next 12 to 24 months a PC life cycle management solution such as asset management, configuration management, patch management, and other related features. Eighty-three percent of respondents say they have or will have within the next 12 to 24 months an integrated endpoint security suite including vulnerability assessment, data loss prevention, anti-virus/anti-malware and others.

Bar Chart 14
PC life cycle management and integrated endpoint security suite



According to Bar Chart 15, 80 percent of respondents believe anti-virus and anti-malware is the most important feature in an integrated endpoint management suite that combines operations and security functions. Other important features in descending order of importance include: whole disk encryption, application control (whitelisting technology), patch and remediation management, IT asset management, device control, vulnerability assessment, firewalls, data loss prevention, configuration management and online backup and recovery.

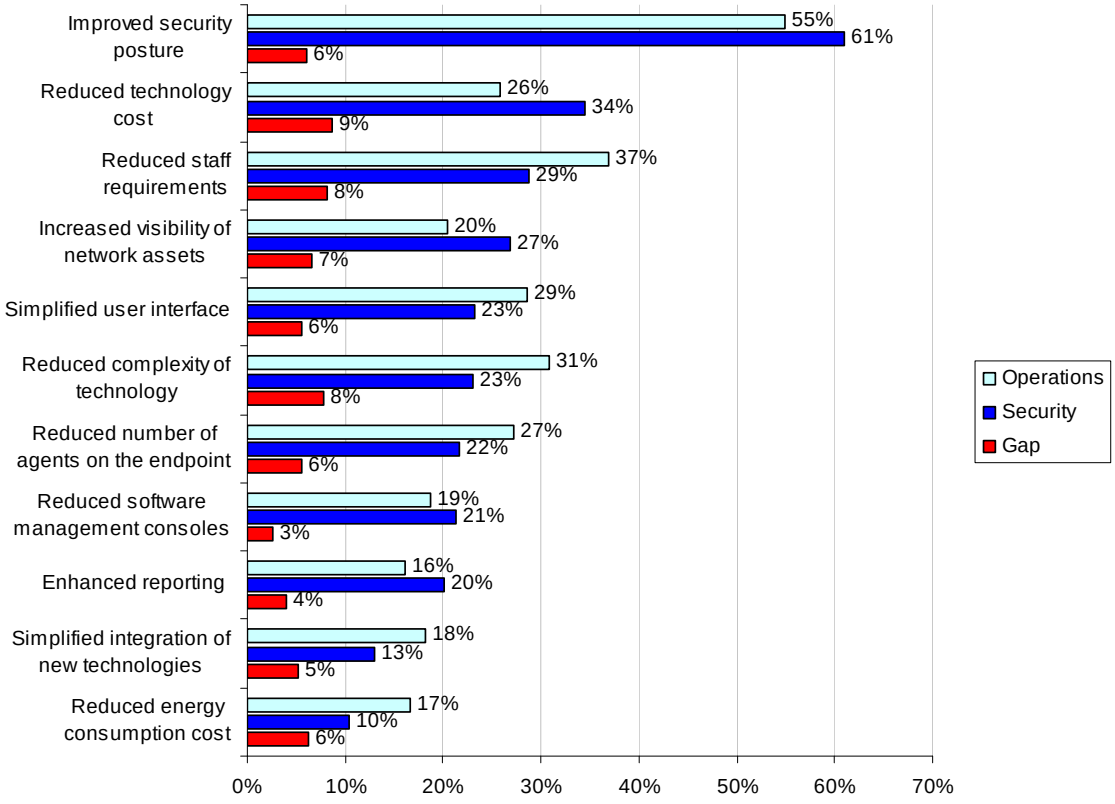
Bar Chart 15
What features are important in an integrated endpoint management suite?



In general, respondents believe improved security posture, reduced technology cost, and reduced staff cost as the three most important benefits of an integrated endpoint management suite that combines operations and security functions. Other benefits cited by respondents include: increased visibility of network assets, simplified user interface, and reduced complexity of

technology. There are differences between respondents in security and operations (shown as red bar). Specifically, respondents in operations seem to attach more importance to reduced staff requirements, reduced complexity of technology, and a simplified user interface. In contrast, security practitioners seem to attach more importance to improved security posture, reduced technology cost, and increased visibility of network assets.

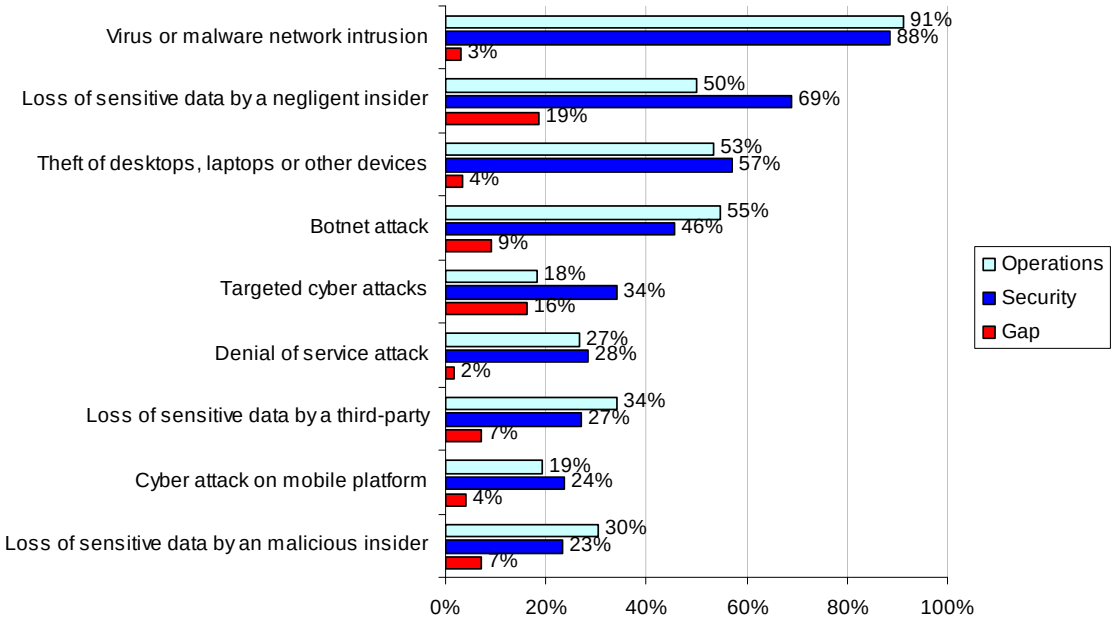
Bar Chart 16
What are the most important benefits of an integrated endpoint management suite?



Bar Chart 17 reports the security incidents most frequently experienced by respondents. According to respondents, virus or malware network intrusions were the most frequently encountered incidents experienced in the past year.

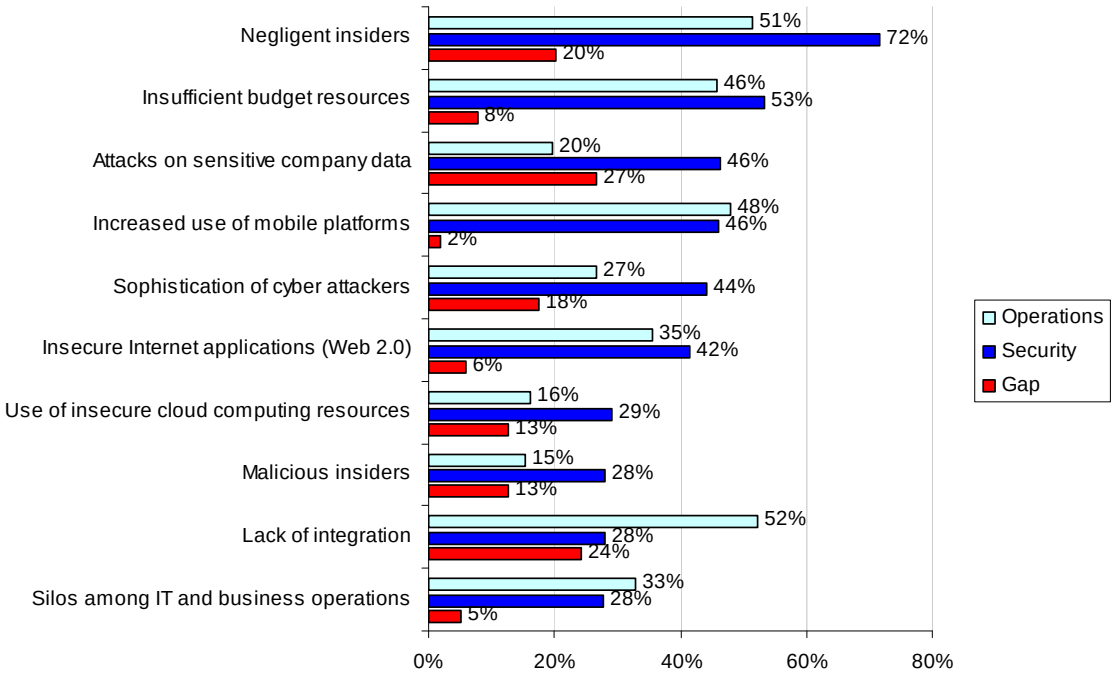
Other frequent incidents include: the loss of sensitive data by negligent insiders, theft of computing devices, botnets, targeted cyber attacks, denial of service, third-party flubs, and others. It is interesting to note, the security group cites negligent insiders and cyber attacks as more prevalent than the operations group. In contrast, the operations group is more likely to cite botnets and third-party flubs as more prevalent than the security group.

Bar Chart 17
Have any of the following incidents happened during the past year?



With respect to security risks in the next 12 months, respondents appear to be most concerned about negligent insiders, insufficient budget resources, the lack of integration between endpoint operations and security technologies, attacks on sensitive company data, sophisticated cyber attacks and increased use of mobile platforms (see Bar Chart 18).

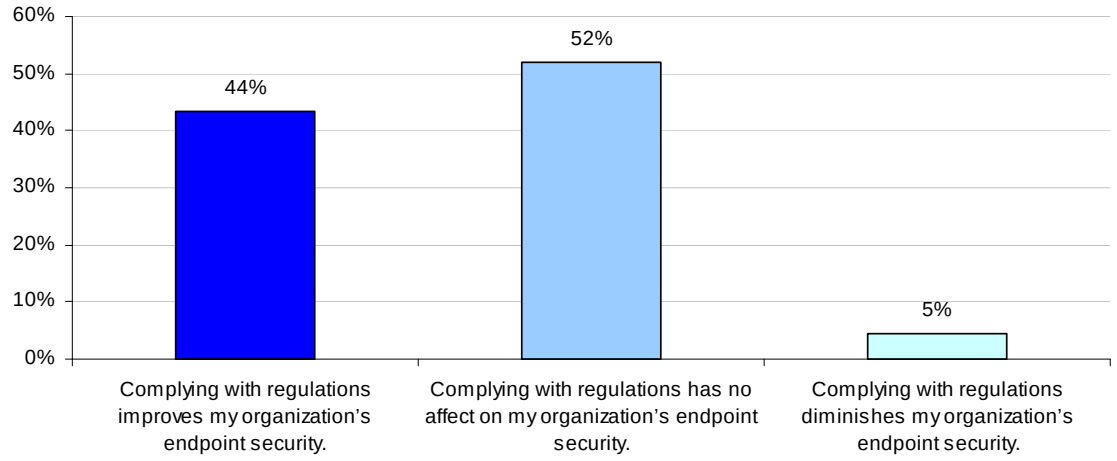
Bar Chart 18
Which of the following security risks are most important to you in the coming year?



Respondents in the security group appear to be more concerned about security risks than operations, with two exceptions. First, the operations group appears to be much more concerned about the lack of integration between endpoint operations and security technologies than the security group. Second, the operations group appears to be more concerned about silos and insufficient collaboration among IT and business operations than the security group.

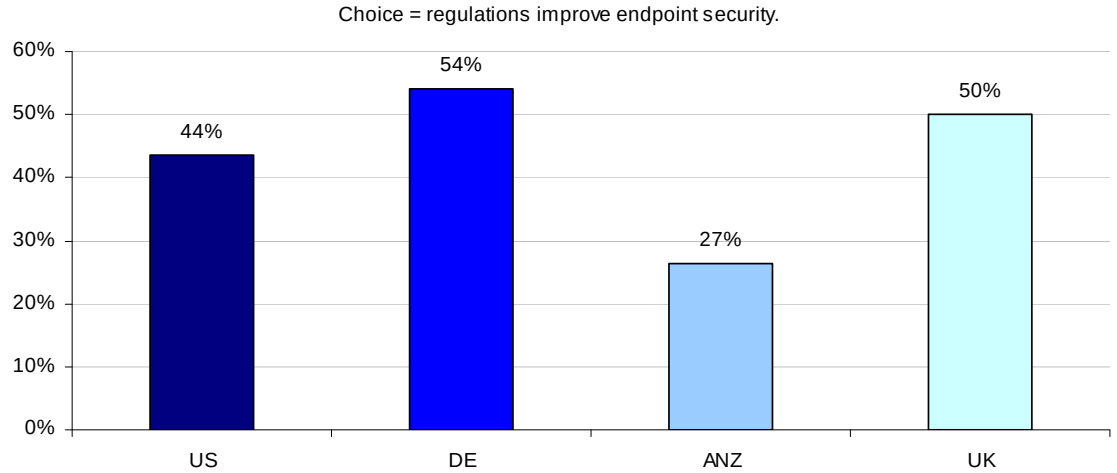
Bar Chart 19 shows that privacy and data security regulations improve the organization's endpoint security posture for 44 percent of respondents. Another 52 percent of respondents believe regulations have no affect on the state of endpoint security, and only 5 percent believe regulations diminish endpoint security.

Bar Chart 19
How do regulations affect your organization's endpoint security?



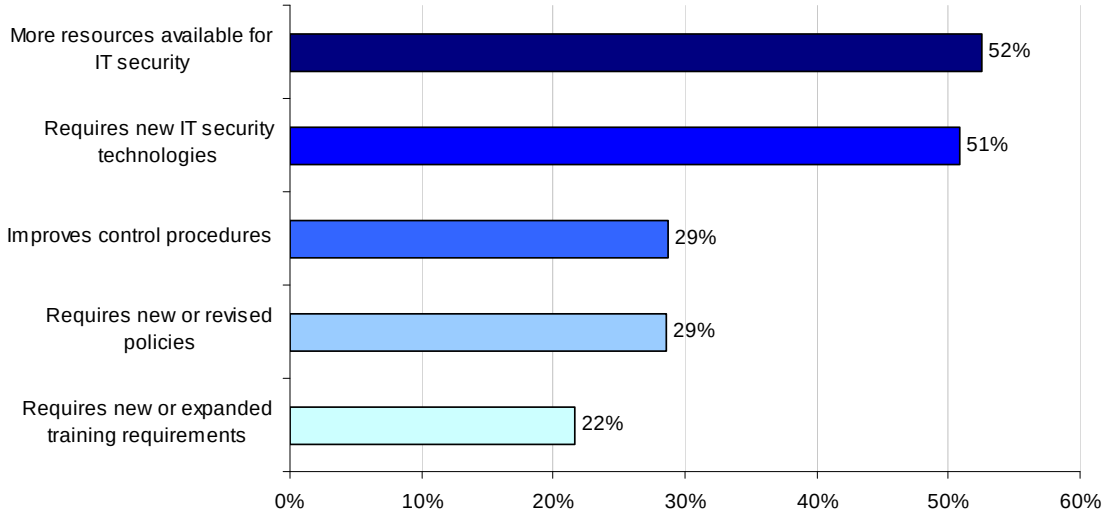
Results in Bar Chart 20 show significant differences among respondents in terms of their perceptions about the impact of regulations on security. Specifically, 54 percent of German respondents believe regulations improve their organization's endpoint security posture. In contrast, only 27 percent of respondents from Australia and New Zealand believe regulations improve endpoint security.

Bar Chart 20
How do regulations affect your organization's endpoint security?
Analysis by country



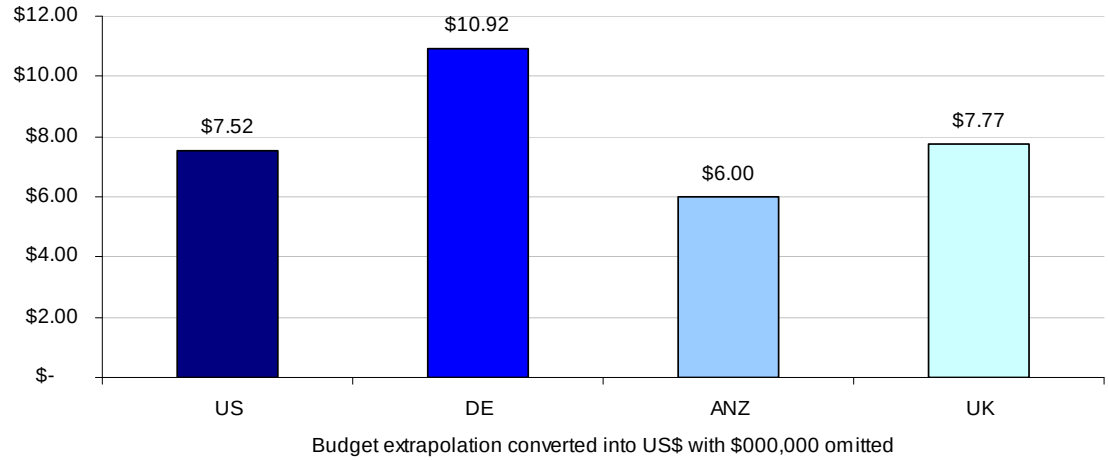
According to Bar Chart 21, 52 percent of respondents believe the number one reason compliance improves endpoint security is that it is essential to obtaining resources. With these resources, they are able to invest in the technologies that improve the organization's overall security (including the security of endpoints). Other reasons include improved control procedures, new or revised policies and expanded training requirements.

Bar Chart 21
Why does compliance improve your organization's endpoint security?



As shown in Bar Chart 22, respondents estimate significant budgets allocated for privacy and data security compliance. On average, German organizations appear to have the highest budget allocated to compliance at $10.9 million, and Australia and New Zealand have the lowest average budget allocation at $6.0 million.

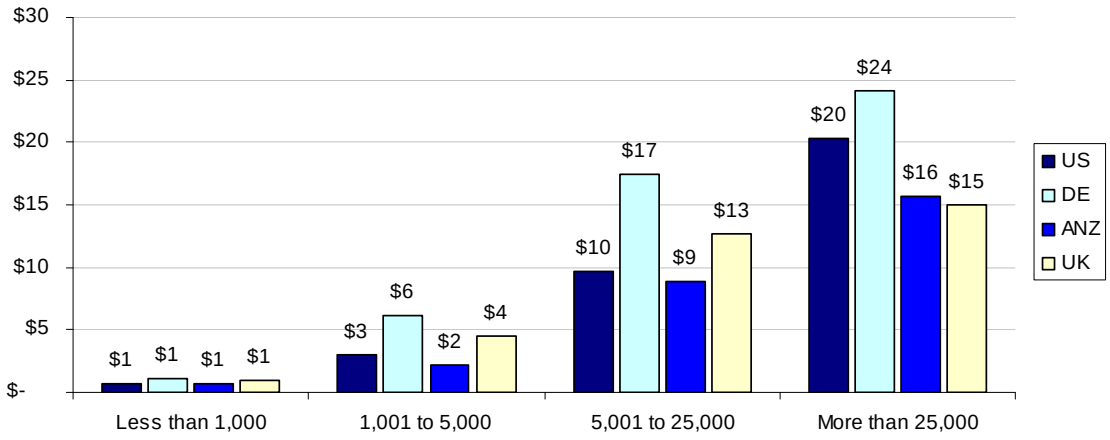
Bar Chart 22
Extrapolated values for annual compliance budgets
Analysis by Country



Budget extrapolation converted into US$ with $000,000 omitted

According to Bar Chart 23, budget allocation for privacy and data security compliance vary proportionately by organizational size.

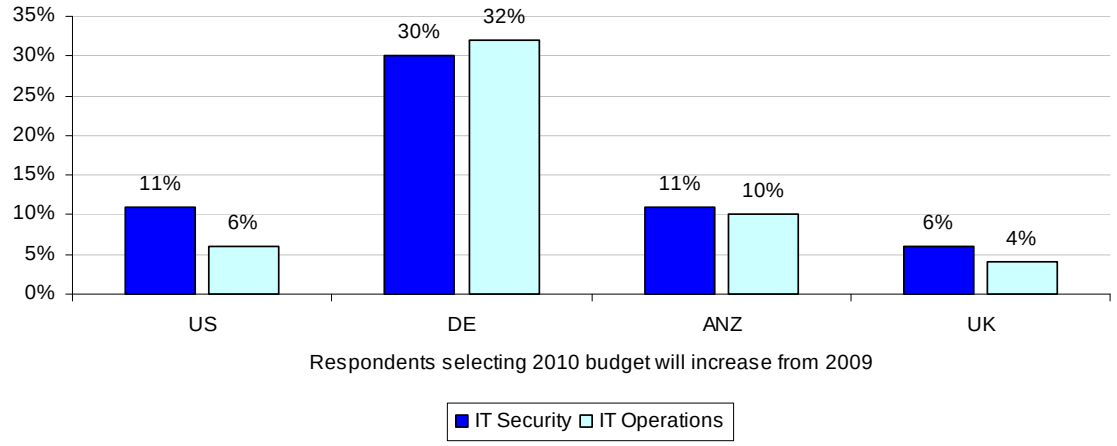
Bar Chart 23
Extrapolated values for annual compliance budgets by organizational size
Analysis by Country



Budget extrapolation converted into US$ with $000,000 omitted

More than 53 percent of respondents believe their organization's 2010 IT security budget will stay the same from the prior year (not shown in bar chart). However, as shown in Bar Chart 24, German respondents are much more likely to see their compliance budgets increase than respondents in other countries.

Bar Chart 24
Estimate that the budget for IT security will increase in FY 2010
Analysis by Country



III. Conclusion

We believe this study provides important insights into the state of the endpoint and its affect on an organization's security posture. We conclude from our findings that organizations are at risk because of the following:

- The management of endpoint security appears to be overly complex and often a disjointed set of control activities. This is evidenced by a plethora of endpoint agents and management software consoles used within respondents' organizations.

- Technologies and applications such as cloud computing, Web 2.0, open source software, and virtualization put the endpoint at risk because they create computing environments outside the direct control of the organization.

- Mobility of the workforce presents a significant security risk because it is hard to enforce policies, especially when employees use devices owned by them or work through insecure wireless channels.

- With respect to endpoint security, operations and security appear to have different priorities. For example, security is most concerned about the lack of skilled or knowledgeable personal to help mitigate threats to endpoints and networks. Whereas, respondents in operations are most concerned about dealing with overly complex endpoint technologies that are difficult to implement or integrate into existing systems.

- Collaboration between operations and security does not occur as frequently as it should for planning, communications and information security purposes. Silos between these two groups make it difficult to execute an enterprise-wide strategy for endpoint security.

- In the countries we surveyed, both operations and security approach endpoint management and security from different perspectives. This suggests the possibility of significant challenges for organizations that operate globally.[4]

- While the risk of insecure endpoints seems to be on the rise, C-level executives may not fully understand and support endpoint management and security efforts. This could result in organizations not allocating appropriate resources to address the rash of problems caused by insecure endpoints.

Despite the challenges, our findings also point to opportunities for improving the state of endpoint security. For example, respondents say their organizations have or will soon implement PC life cycle management tools and integrated endpoint security suites. These solutions will improve the organization's security posture as well as reduce technology and staffing costs.

The features of the ideal endpoint management solution include: anti-virus and anti-malware (blacklisting technology), whole disk encryption, and application control (whitelisting technology). Other important features include patch and remediation management, IT asset management and device controls especially for USB memory sticks.

In addition to technology solutions, we recommend operations and security begin to consider the benefits of collaboration. These benefits include removing the silos and creating a more holistic approach to improving the state of the endpoint. Operations and security should share the common goal of supporting the organization's business objectives while securing the endpoint.

[4] In contrast with other countries, German practitioners have the most confidence that their organization's networks are safe and secure. They are also more likely to have an enterprise-wide security policy, and are less likely to allow employees to connect their personal devices to the organization's systems.

IV. 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 in IT security and IT operations in five countries, 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 sample is representative of individuals in the IT security and IT operations fields. We also acknowledge that the results may be biased by external events.

  We also acknowledge bias caused by compensating respondents 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 certain respondents did not provide accurate responses.

V. Methods

The survey instrument was developed with direct input from Lumension (our sponsor). An expert panel of information security leaders, mostly Ponemon Institute Fellows, provided comments and constructive suggestions for improvement to the draft survey instrument. Survey field work was conducted in October 2009 in all countries. The final debriefing and audit of survey results was completed in November 2009.

Eight separate sampling frames of adult-aged individuals who reside within the United States, Germany, Australia & New Zealand (combined), and United Kingdom were used to recruit participants to this web survey.[5] Our randomly selected sampling frames were selected from national lists of IT, security, compliance, data protection and privacy professionals. Over 90% of respondents completed all survey items within 25 minutes. Table one summarizes the survey response experienced using a web-based survey instrument.

Table 1 Response statistics	Sampling frame	Sent to subjects	Returns	Rejects	Final sample	Response rate
US Operations	8,132	7,850	529	86	443	5.4%
US Security	9,908	9,458	540	95	445	4.5%
DE Operations	7,550	6,992	530	103	427	5.7%
DE Security	8,100	7,085	555	115	440	5.4%
ANZ Operations	3,503	2,950	248	43	205	5.9%
ANZ Security	5,500	4,880	341	45	296	5.4%
UK Operations	6,253	5,829	407	55	352	5.6%
UK Security	6,855	5,796	457	56	401	5.8%

In total, 1,427 respondents in operations and 1,582 respondents in security completed the survey and provided usable results within an eight-day research window. Of returned instruments, about 1% was omitted because of reliability tests. The final samples represent a net response rate of 5.6% and 5.2% for operations and security, respectively.

The mean experience level for respondents in operations is 10.3 years and for security is 9.6 years. Table 2 reports the organizational level of respondents in operations and security. As can be seen, the majority of respondents are at or above the supervisory level.

Table 2 Organizational level of respondents consolidated for the US, DE, ANZ and UK samples	Combined	Security	Operations
Executive	1%	1%	1%
Director	15%	15%	14%
Manager or Supervisor	27%	27%	27%
Staff	22%	23%	21%
Technician	27%	26%	29%
Contractor	6%	7%	6%
Other (please specify)	2%	2%	2%
Total	100%	100%	100%

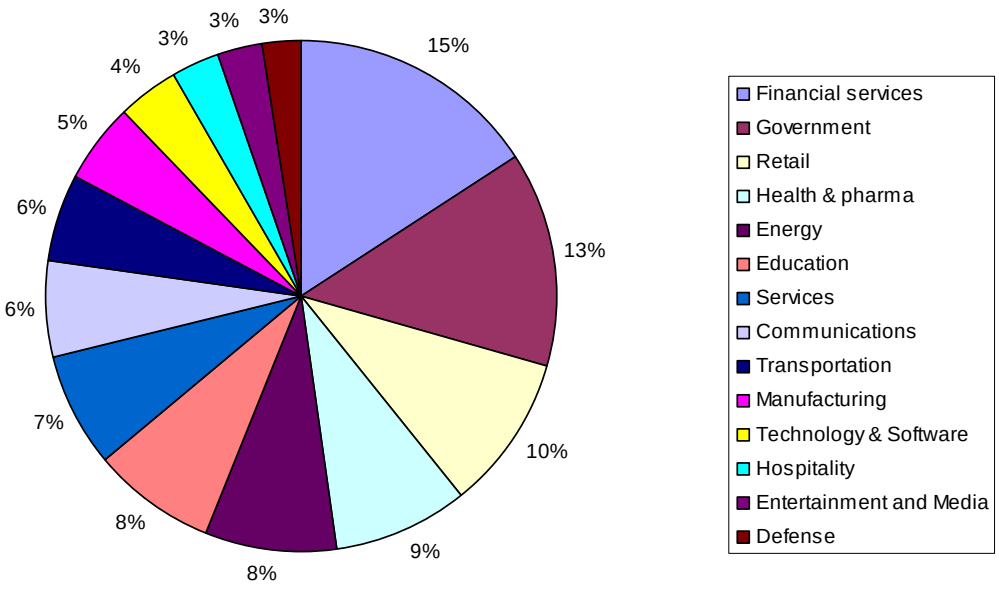
Table 3 reports the respondent organization's approximate headcount as a surrogate for size. As can be seen, the majority of respondents are employed by organizations with more than 1,000 employees.

[5] Respondents were given nominal compensation to complete all survey questions.

Table 3 Worldwide headcount of respondents' organizations	Combined	ITS	ITO
Less than 500 people	15%	14%	15%
500 to 1,000 people	20%	20%	20%
1,001 to 5,000 people	23%	23%	23%
5,001 to 25,000 people	19%	20%	19%
25,001 to 75,000 people	15%	16%	15%
More than 75,000 people	8%	8%	8%
Total	100%	100%	100%

Pie Chart 1 reports the industry distribution of respondents in all eight samples by their organization's primary industry classification. As shown, 15% of respondents are employed by financial service companies (including insurance, banking, credit cards, brokerage and investment management), and 13% work for central (federal) or local government.

Pie Chart 1
Industry distribution of the combined operations and security samples
Consolidated view for US, DE, ANZ and UK



In total, 63% of respondents are male and 37% female. While these results are skewed on the gender variable (more male than female respondents), our results are consistent with known demographics in the five countries studied. Appendix I provides additional details about survey responses.

If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote from or reuse this report), please contact us by letter, phone call or e-mail:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49686 USA
1.800.887.3118
research@ponemon.org

Ponemon Institute LLC

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.

Appendix 1: Survey Findings

US, DE, ANZ and UK samples combined

The following tables provides the summarized results for IT operations and IT security samples in conducted in five countries (consolidated).

1. Attributions for Security: Please rate each one of the following five statements using the scale provided below each item. Strongly agree = 1, Agree = 2, Unsure = 3, Disagree = 4, Strongly disagree = 5	Security	Operations
Q1a. My organization has sufficient resources to achieve compliance with data security policies and best practices.	49%	55%
Q1b. My organization's CEO is a strong supporter of security and data protection efforts.	54%	52%
Q1c. My organization views data security as a strategic initiative across the enterprise.	51%	51%
Q1d. My organization is proactive in managing privacy and data protection risks.	65%	53%
Q1e. Laptops and other mobile data-bearing devices are secure and do not present a significant security risk to our organization's networks or enterprise systems.	40%	47%
Average	52%	52%

Q2a. Does your organization use the following technologies?	Security	Operations
Open source software	76%	84%
Cloud computing	56%	64%
Virtualization	50%	58%
Web 2.0 technologies (social networking, applications, wikis, blogs & others)	71%	75%
Software distribution	30%	43%
IT asset management	39%	48%
Online backup & recovery	72%	57%
Configuration management	41%	34%
Power management/wake on LAN	28%	23%
Application virtualization	30%	24%
Software license metering	29%	27%
Other (please specify)	2%	1%

Q2b. Please state whether the use of this technology will increase over the next 12 to 24 months.	Security	Operations
Open source software	36%	36%
Cloud computing	65%	73%
Virtualization	59%	70%
Web 2.0 technologies (social networking, applications, wikis, blogs & others)	70%	60%
Software distribution	25%	19%
IT asset management	52%	62%
Online backup & recovery	23%	46%
Configuration management	32%	43%
Power management/wake on LAN	29%	59%
Application virtualization	42%	39%
Software license metering	53%	59%
Other (please specify)	4%	4%

Q3. 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.	Security	Operations
1 to 2	37%	41%
3 to 5	24%	20%
6 to 10	23%	21%
More than 10	6%	7%
Not sure	10%	11%
Total	100%	100%

Q4. On a typical day, how many different or distinct software management consoles does your organization use to manage endpoint operations & security functions? Please provide your best estimate.	Security	Operations
1 to 2	36%	34%
3 to 5	37%	40%
6 to 10	10%	9%
More than 10	6%	7%
Not sure	12%	10%
Total	100%	100%

Q5a. Does your organization allow employees to connect their own computing devices (such as laptops, smart phones or PDAs) to its network or enterprise systems? Please check the following that apply:	Security	Operations
Yes, it allows full access	10%	13%
Yes, it provides a DMZ or other isolated access	27%	31%
No, it does not provide access today but may in the future	35%	29%
No, and there are no plans to provide access	29%	27%
Total	100%	100%

Q5b. Does your organization subsidize the employee's purchase and use of their own computing devices (such as laptops, smart phones or PDAs)?	Security	Operations
Yes	13%	14%
No, but my organization is planning to offer this in the future.	29%	32%
No, and there are no plans to offer this in the future.	58%	55%
Total	100%	100%

Q5c. Does your organization have a policy that permits employees to connect their own computing devices (such as laptops, smart phones or PDAs) to the organization's network or enterprise systems?	Security	Operations
Yes	27%	24%
No, but my organization is considering a policy	28%	30%
No, and there no plans to have a policy	45%	46%
Total	100%	100%

Q6. Why does your organization invest in endpoint security solutions? Please select your top three choices.	Security	Operations
Mobility of sensitive data	34%	34%
New data privacy/compliance regulations	36%	34%
Endpoint TCO	41%	40%
End user productivity	51%	52%
Compliance & IT risk management	44%	49%
Insider risk	18%	18%
Security incidents (virus, malware, and so forth)	49%	49%
Data loss prevention (DLP)	14%	13%
Total	286%	290%

Q7a. Do you believe your IT network is more secure now than it was a year ago?	Security	Operations
Yes	54%	56%
No	47%	44%
Total	100%	100%

Q7b, If yes, why it is more secure today? Please check all that apply.	Security	Operations
Improved policies	44%	42%
Improved control procedures	41%	37%
New information security technologies	61%	59%
Increased resources	10%	13%
Senior level support	13%	14%
Increased regulatory scrutiny	12%	10%
Total	180%	174%

Q8. Does your organization have one company-wide IT security policy?	Security	Operations
Yes	50%	50%
No, but my organization is considering a company-wide policy	23%	23%
No, and there no plans to have a company-wide policy	27%	27%
Total	100%	100%

Q9. Does your organization's IT security budget support business objectives and priorities?	Security	Operations
Yes, the budget adequately supports business objectives	37%	39%
Yes, but budget can be increased to support business objectives	45%	44%
No	18%	17%
Total	100%	100%

Q10a. What statement best describes how IT operations and IT security work together to support planning, communications and information sharing functions?	Security	Operations
Collaboration is excellent	17%	17%
Collaboration is adequate but can be improved	49%	55%
Collaboration is poor or non-existent	34%	28%
Total	100%	100%

Q10b. Has the level of collaboration improved over the past year?	Security	Operations
Yes	30%	29%
No	70%	71%
Total	100%	100%

Q11. What do you perceive to be the main difficulties in managing endpoint operations and security? Please select your top two reasons.	Security	Operations
Lack of skilled or knowledgeable personnel	58%	47%
Lack of budget	24%	24%
Difficulty integrating multiple technologies	25%	37%
Overly complex technologies	18%	43%
Misalignment of IT with business objectives	41%	24%
Lack of senior executive support	8%	10%
Other (please specify)	3%	1%
Total	178%	187%

Q12. Does your organization have a PC life cycle management solution (such as asset management, configuration management, patch management or others)?	Security	Operations
Yes	38%	38%
Our organizations expects to have a PC life cycle management solution within the next 12-24 months.	41%	41%
No	20%	22%
Total	100%	100%

Q13. Does your organization have an integrated endpoint security suite (vulnerability assessment, DLP, anti-virus, anti-malware or others)?	Security	Operations
Yes	41%	42%
Our organization expects to have an integrated endpoint security suite within the next 12-24 months.	41%	40%
No	18%	18%
Total	100%	100%

Q14. What features are important in an integrated endpoint management suite (combining operations and security functions)? Please use the following five-point scale to rate each feature from very important to irrelevant. 1=Very important & 2=Important.	Security	Operations
Patch & remediation management	65%	72%
Application control (whitelisting technology)	68%	70%
Device control (USB, removable media)	59%	59%
Whole disk encryption	73%	67%
Data loss prevention (content filtering)	60%	52%
Compliance & IT risk management	52%	43%
Reporting	23%	26%
Software distribution	46%	45%
IT asset management	60%	62%
Software inventory/usage monitoring	37%	41%
Online backup & recovery	53%	46%
Configuration management	51%	49%
Power management/ wake on LAN	40%	44%
Application virtualization	33%	32%
Anti-virus and anti-malware (blacklisting technology)	81%	79%
Firewall	56%	61%
Intrusion detection	39%	44%
Network access control (NAC)	32%	45%
Vulnerability assessment	58%	60%

Q15. What do you believe are the most important benefits of an integrated endpoint management suite (combining operations and security functions)? Please select your top three choices.	Security	Operations
Reduced complexity of technology	23%	31%
Enhanced reporting	20%	16%
Reduced number of agents on the endpoint	22%	27%
Simplified integration of new technologies	13%	18%
Reduced software management consoles	21%	19%
Simplified user interface	23%	29%
Reduced technology cost	34%	26%
Reduced energy consumption cost	10%	17%
Increased visibility of network assets	27%	20%
Improved security posture	61%	55%
Reduced staff requirements	29%	37%
Total	284%	294%

Q16. Which of the following technologies does your organization currently use?	Security	Operations
Anti-virus & anti-malware	84%	82%
Application control/whitelisting	45%	46%
Configuration management	49%	52%
Data loss/leak prevention (content filtering)	23%	22%
Device control (USB, removable media)	35%	28%
Firewall	99%	99%
Intrusion detection	45%	54%
Network access control (NAC)	48%	51%
Patch & remediation management	52%	54%
Vulnerability assessment	40%	44%
Whole disk encryption	54%	55%

Q17. During the past year, have any of the following incidents occurred in your organization? Select all that apply.	Security	Operations
Loss of sensitive data by a negligent insider	69%	50%
Loss of sensitive data by an malicious insider	23%	30%
Loss of sensitive data by a third-party vendor or cloud computing partner	27%	34%
Virus or malware network intrusion	88%	91%
Denial of service attack	28%	27%
Botnet attack	46%	55%
Cyber attack on mobile platforms (phone, PDAs, netbook and others)	24%	19%
Software, O/S vulnerability attacked	14%	11%
Regulatory fines and lawsuits	15%	12%
SQL injection attack	19%	22%
Targeted cyber attacks	34%	18%
Theft of desktops, laptops or other devices	57%	53%
Total	443%	423%

Q18. In the coming year (2010), which of the following IT security risks are of most concern to you? Please select the top five risks.	Security	Operations
Use of insecure cloud computing resources	29%	16%
Attacks on sensitive company data	46%	20%
Negligent insiders	72%	51%
Malicious insiders	28%	15%
Insufficient budget resources	53%	46%
Inability to measure policy compliance	3%	12%
Sophistication of cyber attackers	44%	27%
End-user use of insecure Internet applications (including Web 2.0/social media)	42%	35%
Lack of a security strategy	25%	14%
Lack of policies or procedures	7%	17%
Silos and insufficient collaboration among IT and business operations	28%	33%
Complexity of security technologies	14%	24%
Lack of integration between endpoint operations and security technologies	28%	52%
Increased use of mobile platforms (smart phones, PDA, netbook, and others)	46%	48%
Total	465%	410%

Q19b. How do these regulations affect your organization's endpoint security? Please select the one statement that best describes your opinion.	Security	Operations
Complying with regulations improves my organization's endpoint security.	43%	44%
Complying with regulations has no affect on my organization's endpoint security.	52%	51%
Complying with regulations diminishes my organization's endpoint security.	4%	5%
Total	100%	100%

Q19c. Why does compliance improve your organization's endpoint security? Please check all that apply.	Security	Operations
Requires new or revised policies	29%	28%
Requires new or expanded training requirements	20%	23%
Improves control procedures	27%	30%
Requires new IT security technologies	54%	48%
More resources available for IT security	53%	52%
Total	183%	181%

Q20a. On average, how much does it cost your organization to comply with privacy and data security compliance per year? Use your best estimate or gut feel. Please note that this question was framed in the local currency of the respondent and then converted into US dollars for comparability.	Security	Operations
Less than $1 million	11%	10%
Between $1 to 2 million	11%	11%
Between $3 to $4 million	19%	20%
Between $5 to $6 million	15%	16%
Between $7 to $8 million	12%	13%
Between $9 to $10 million	16%	13%
Between $11 to $12 million	6%	7%
Between $13 to $14 million	5%	5%
Between $15 to $16 million	1%	1%
Between $17 to $18 million	2%	4%
Between $19 to $20 million	0%	0%
Between $21 to $22 million	1%	0%
Between $23 to $25 million	0%	1%
Over $25 million	1%	1%
Total	100%	100%

Q20b. On a percent basis, how much of your departmental resources are spent on privacy and data security compliance? Use your best estimate or gut feel.	Security	Operations
Less than 5%	5%	29%
Between 5% to 10%	8%	27%
Between 10% to 20%	17%	27%
Between 20% to 30%	25%	6%
Between 30% to 40%	18%	6%
Between 40% to 50%	9%	3%
Between 50% to 60%	8%	1%
Between 60% to 70%	3%	0%
Between 70% to 80%	2%	0%
Between 80% to 90%	2%	0%
Between 90% to 100%	2%	0%
Total	100%	100%

Q21. How does your organization's 2009 IT security budget compare to 2008?	Security	Operations
Increase	28%	25%
Stay the same	55%	53%
Decrease	14%	17%
Unsure	3%	5%
Total	100%	100%

Q22. How will your organization's IT security budget for 2010 compare to 2009?	Security	Operations
Increase	15%	13%
Stay the same	53%	53%
Decrease	24%	26%
Unsure	9%	8%
Total	100%	100%

Q23. Approximately what percentage of your overall IT budget is dedicated to each of the following areas?	Overall	US
Q23a. IT security. Please use your best estimate or gut feel.	Security	Security
Less than 5%	39%	32%
Between 5% to 10%	22%	22%
Between 10% to 20%	10%	15%
Between 20% to 30%	16%	18%
Between 30% to 40%	7%	11%
Between 40% to 50%	2%	2%
Between 50% to 60%	2%	0%
Between 60% to 70%	1%	0%
Between 70% to 80%	1%	0%
Between 80% to 90%	0%	0%
Between 90% to 100%	1%	0%
Total	100%	100%

Q23b. IT operations. Please use your best estimate or gut feel.	Operations	Operations
Less than 5%	4%	3%
Between 5% to 10%	4%	5%
Between 10% to 20%	6%	6%
Between 20% to 30%	9%	7%
Between 30% to 40%	14%	13%
Between 40% to 50%	12%	15%
Between 50% to 60%	15%	17%
Between 60% to 70%	12%	16%
Between 70% to 80%	8%	8%
Between 80% to 90%	8%	9%
Between 90% to 100%	7%	1%
Total	100%	100%

Q23c. IT compliance. Please use your best estimate or gut feel.	All	All
Less than 5%	33%	33%
Between 5% to 10%	19%	16%
Between 10% to 20%	18%	16%
Between 20% to 30%	14%	11%
Between 30% to 40%	8%	8%
Between 40% to 50%	4%	8%
Between 50% to 60%	4%	7%
Between 60% to 70%	0%	0%
Between 70% to 80%	0%	0%
Between 80% to 90%	0%	0%
Between 90% to 100%	0%	0%
Total	100%	100%

D1. What organizational level best describes your current position?	Security	Operations
Senior Executive	0%	0%
Vice President	1%	1%
Director	15%	14%
Manager/Supervisor	27%	27%
Associate/Staff	23%	21%
Technician	26%	29%
Contractor	7%	6%
Other (please specify)	2%	2%
Total	100%	100%

D2. Check the Primary Person you or your IT organization reports into within the organization.	Security	Operations
CEO/Executive Committee	0%	0%
Chief Financial Officer	3%	0%
General Counsel	1%	0%
Chief Information Officer	43%	75%
Chief Technology Officer	9%	18%
Compliance/Ethics Officer	5%	0%
Chief Marketing Officer/VP	0%	0%
Human Resources VP	0%	0%
Chief Security Officer	13%	0%
Chief Information Security Officer	18%	0%
Chief Privacy Officer	1%	0%
Chief Risk Officer	6%	2%
Other (please specify)	0%	4%
Total	100%	100%

D3. What industry best describes your organization's industry focus?	Security	Operations
Airlines	3%	2%
Automotive	1%	1%
Brokerage & Investments	2%	2%
Communications	5%	5%
Chemicals	2%	5%
Credit Cards	2%	2%
Defense	3%	2%
Education	5%	5%
Energy	4%	5%
Entertainment and Media	1%	4%
Federal Government	9%	8%
Food Service	3%	3%
Healthcare	5%	6%
Hospitality	3%	3%
Manufacturing	5%	5%
Insurance	3%	3%
Internet & ISPs	1%	1%
State or Local Government	5%	5%
Pharmaceuticals	3%	3%
Professional Services	5%	4%
Research	3%	2%
Retailing	7%	7%
Retail Banking	9%	9%
Services	3%	2%
Technology & Software	4%	4%
Transportation	3%	1%
Total	100%	100%

D4. Where are your employees located? (check all that apply):	Security	Operations
United States	85%	87%
Canada	40%	39%
Europe	79%	80%
Asia-Pacific	46%	46%
Latin America (including Mexico)	19%	20%

D5. What is the worldwide headcount of your organization?	Security	Operations
Less than 500 people	14%	15%
500 to 1,000 people	20%	20%
1,001 to 5,000 people	23%	23%
5,001 to 25,000 people	20%	19%
25,001 to 75,000 people	16%	15%
More than 75,000 people	8%	8%
Total	100%	100%