



Understanding Security Complexity in 21st Century IT Environments:

A study of IT practitioners in the US, UK, France, Japan & Germany

Sponsored by

Check Point Software Technologies

Independently conducted by Ponemon Institute^{LLC}

Publication Date: February 2011

Understanding Security Complexity in 21st Century IT Environments

A study of IT practitioners in the US, UK, France, Japan and Germany
Ponemon Institute, February 2011

Part 1. Executive Summary

Organizations face costly security risks from both internal and external sources often risking network security, customer information, loss of intellectual property, financial losses and corporate brand damage. Among the 47 organizations participating in Ponemon Institute's benchmark study on the *Cost of Cyber Crime*, it was determined that one cyber attack can range from a low of \$237,000 to \$52 million.¹ Further, the organizations participating in the study experienced 205 separate and discernible cyber attacks over a four-week period.

How well are organizations able to protect themselves against these risks? According to the findings from this study, the most significant information security challenge facing organizations in the five countries we studied is managing the complexity of security. Preventing data loss by employees and other insiders and dealing with industry and/or government compliance mandates also are difficult challenges.

Sponsored by Check Point Software Technologies, Ponemon Institute independently conducted a survey of 2,426 highly experienced IT practitioners located in five nations: United States, United Kingdom, France, Japan and Germany. Seventy-three percent of IT practitioners participating in our study are employed by companies with more than 1,000 employees.

Using an omnibus survey design, the purpose of this research is to better understand what IT practitioners in five countries think about important global IT security issues. The topics of the survey range from managing the growing complexity of IT security to determining what issues worry IT practitioners most. The study also asked respondents how much awareness they believe employees in their organizations have about data security compliance and policies.

We believe the main conclusion to be drawn from the findings is that organizations recognize the need to reduce the complexity in their IT environments. However, they face challenges in consolidating the technologies or products they currently have. It seems, therefore, that a good first step to achieving better security and simplicity in their IT environments is to assess the technologies they really need to support business and IT priorities in their organizations.

In addition, because IT environments tend to be complex, employees may not be aware or have a good understanding of the data security compliance practices and policies they need to follow. Evidence of a lack of awareness is the finding that the number one cause of a data breach, according to respondents, is lost or stolen equipment presumably due to employee and user negligence.

As revealed in this study, IT practitioners are very much worried about meeting the growing number of regulations governing the security of data. Achieving a strong but streamlined security posture should help reduce these concerns and make their IT environments more cost effective.

Following is a summary of key findings:

Pricing and/or total cost of ownership is the number one obstacle faced by organizations when trying to consolidate the number of vendors and reduce the complexity of network security operations.

On average, respondents in Japan and France have eight or more separate vendors for securing their organization's networks. Respondents in the US and Germany have about seven separate

¹ 2010 *Cost of Cyber Crime Study*, Ponemon Institute, July 31, 2010

vendors, and respondents in the UK have about five separate vendors. The most difficult obstacles to reducing the number of vendors to a more manageable size, according to respondents in the US, France and Japan, concerns pricing and/or total cost of ownership. In Germany it is the limited availability of integrated solutions and in the UK it is ensuring optimal performance.

Managing complexity in the security environment is the most significant challenge facing companies.

In all countries studied, the inability to manage complexity of security operations is viewed as the number one obstacle. In the US and UK, complexity is followed by preventing data loss by employees or other insiders. In Germany, France and Japan it is the challenge of dealing with industry and/or government compliance mandates. According to respondents in Japan, another equally major challenge is enforcing security policies.

IT practitioners in the countries studied have very different priorities for 2011.

In the US and UK it is meeting IT governance, risk and compliance requirements. In France and Germany it is to secure all fixed and mobile endpoints. In Japan it is to secure virtualized and cloud computing environments.

The ability to manage policies by user, in addition to devices or IP address, is a key functionality today or in the future for most organizations in the study.

With the exception of France, the majority of IT practitioners see the ability to manage policies by users, in addition to devices or IP addresses as a key functionality today and in the future.

Compliance and staffing/IT resources are on average the top concerns of respondents in all locations.

As the number of regulations governing the security of data continues to increase throughout the world, IT practitioners are understandably concerned about compliance. IT practitioners in the US, UK, France and Germany say it is the number one concern for them. In Japan it is concern over security uncertainty. When asked about the level of awareness employees have about data security compliance and policies, 74 percent of respondents in France say their employees have little or no awareness. Countries that have a low or no awareness of organizational security policies are UK (53 percent of respondents) and US (51 percent of respondents).

For organizations that experienced a loss of sensitive data, the number one cause in all countries is lost or stolen equipment.

In the US, UK and France the second cause was a hacked network. In Japan the second major cause is insecure mobile devices and in Germany it is web-based application or file sharing sites. On average for all countries, the type of information frequently lost is customer information and consumer information. In the US, UK, and France the loss of intellectual property was in the top three types of information lost. Japan and Germany had the highest percentage of unsure as to the types of information lost.

Part 2. Analysis of Responses to Global IT Security Issues Survey

In this section, we provide additional analysis of the key findings. Responses to the 10 questions we asked survey respondents are expressed as percentage frequencies in tabular form. In addition, results are provided in line graphs, bar charts, and pie charts to better illustrate our most salient results.

Table 1 presents the number of different vendors organizations in all five countries use to secure their networks. As shown in Figures 1 and 2, the median number of vendors ranges from a low of 5.0 (UK) to a high of 8.4 (Japan).

Table 1. On average, how many different vendors do you use to secure your organization's network?	US	UK	France	Japan	Germany
1 to 2	19%	30%	10%	11%	30%
3 to 6	21%	42%	24%	23%	14%
7 to 10	42%	20%	33%	21%	31%
More than 10	18%	8%	33%	45%	25%
Total	100%	100%	100%	100%	100%
Median	6.96	5.00	7.97	8.40	6.71

Figure 1: Less than and more than (or equal to) seven different security vendors

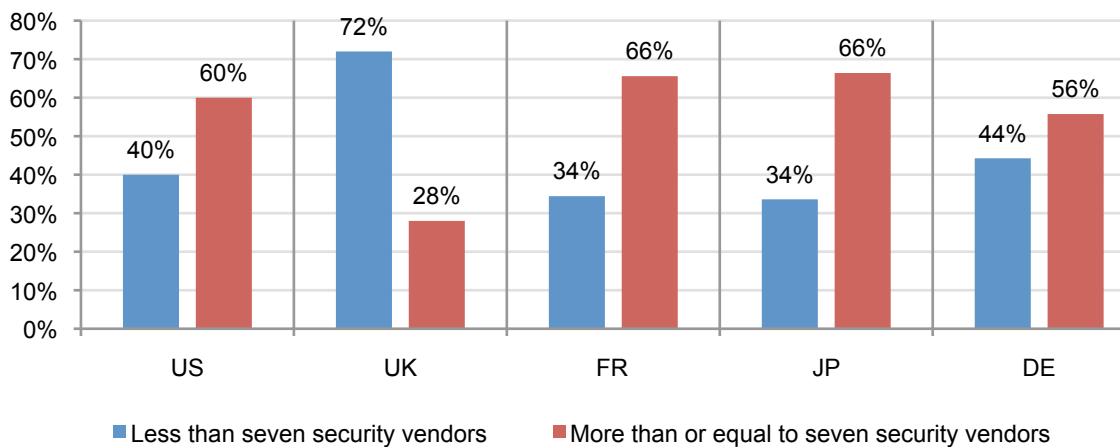


Figure 2: Median number of vendors used to secure networks

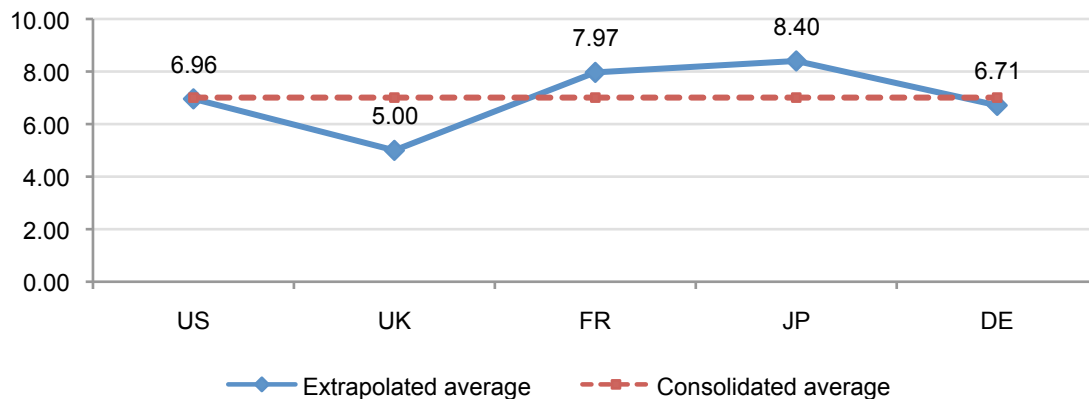


Table 2 shows respondents' ranking of the three primary obstacles or difficulties they experience when attempting to consolidate vendors in order to reduce complexity and make the IT organization more efficient.²

Table 2. Please rank the following three obstacles when consolidating the number of vendors (3 = most concern to 1 = least concern)	US	UK	France	Japan	Germany
Limited availability of integrated solutions	2.01	1.47	1.44	1.04	2.44
Ensuring optimal performance	1.13	2.81	1.77	1.76	1.99
Pricing and/or total cost of ownership	2.47	2.59	2.65	2.82	1.43

As shown in Figure 3, respondents in the US, France and Japan view pricing and/or the total cost of ownership as the obstacle of most concern. Respondents in the UK see ensuring optimal performance as most concerning, while German respondents see the limited availability of integrated solutions as the obstacle of most concern.

Figure 3: Average rank of three obstacles to consolidating network security vendors

Rank order reversed to show highest rank as the highest priority

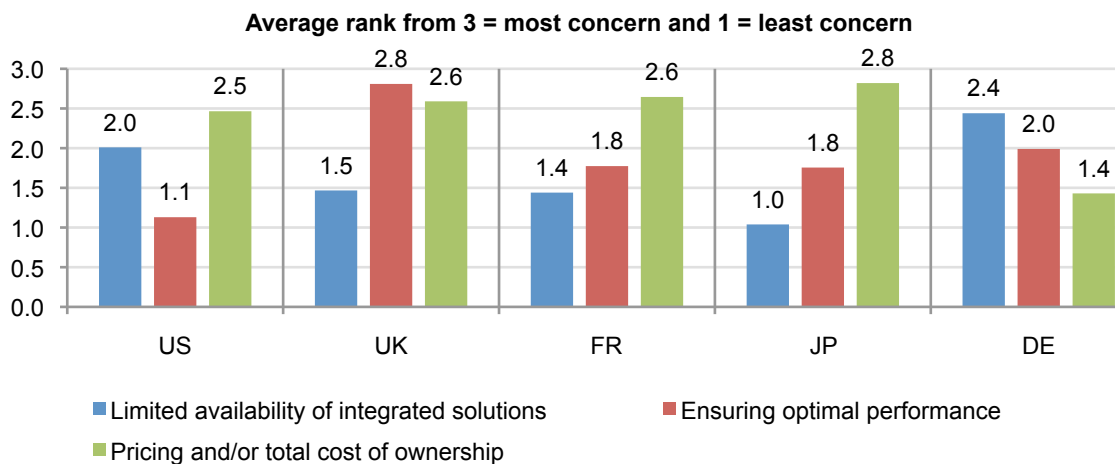


Table 3 focuses on what respondents perceive as the most significant information security challenges facing their organizations. In all countries, the inability to manage complexity of security operations is viewed as the number one obstacle. In the US and UK, complexity is followed by preventing data loss by employees or other insiders. In Germany and France, it is the challenge of dealing with industry and/or government compliance mandates.

Table 3. Which of the following is the most significant information security challenge facing your company? Please select only one choice.	US	UK	France	Japan	Germany
Industry and/or government compliance mandates	19%	16%	28%	21%	29%
Managing the complexity of security	33%	35%	35%	24%	36%
Enforcing security policies	15%	7%	7%	24%	12%
Preventing data breaches from outside attackers	12%	14%	14%	14%	7%
Preventing data loss by employees or others	21%	28%	17%	17%	16%
Total	100%	100%	100%	100%	100%

² Please note that the actual question provided in the Appendix used a reverse ranking, where 1 = most concerned and 3 = least concerned. This transformation was conducted for graphical illustration purposes.

Figure 4 shows the average response for all five countries. “Managing the complexity of security” is the most significant challenge followed by industry and/or government compliance mandates. The average for all five countries is shown in the Appendix to this paper.

Figure 4: Five significant challenges in descending order of importance

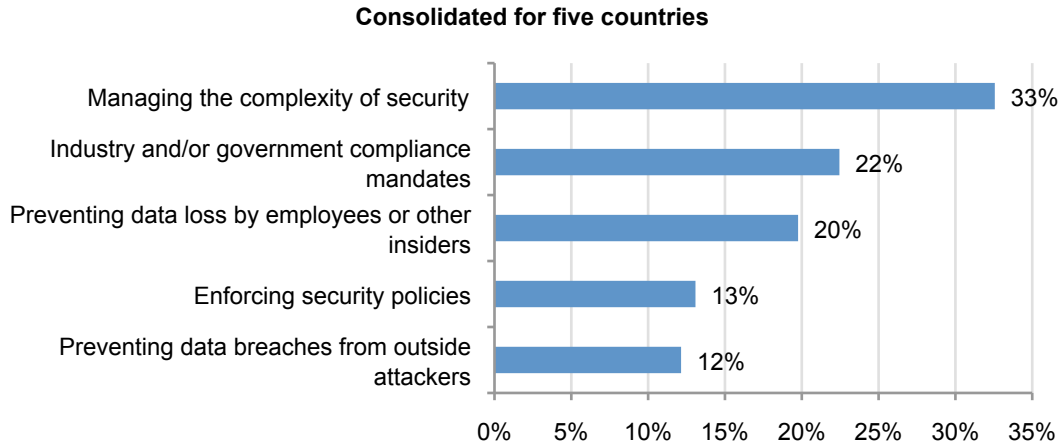


Figure 5 provides a country level analysis. As shown in Figure 5, with the exception of Japan, the results show that managing the complexity of security is consistently viewed as the most significant challenge for respondents in the US, UK, France and Germany.

Figure 5: Country level comparison of the top security challenge

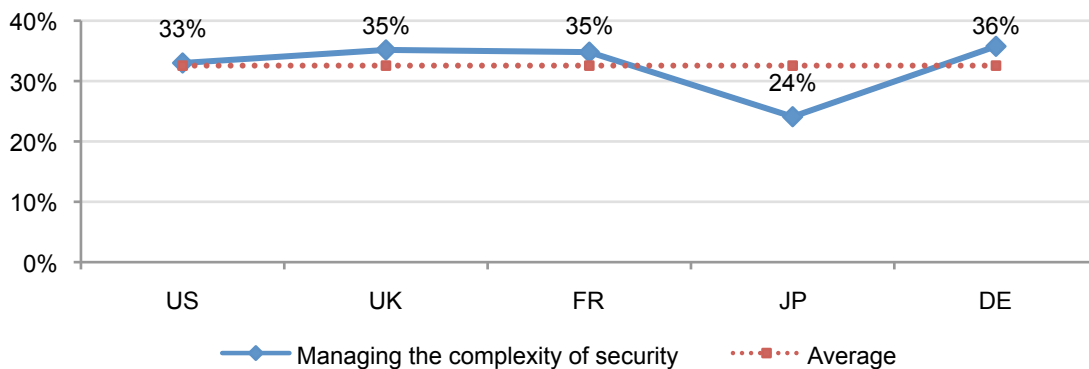


Table 4 shows respondents ranking of seven security priorities for the present year.³ In the US and UK, it is meeting IT governance, risk and compliance requirements. In France and Germany, it is to secure all fixed and mobile endpoints. In Japan it is to secure virtualized and cloud computing environments.

Table 4. Rank the following security priorities for 2011 (7 = highest priority to 1 = lowest priority):	US	UK	France	Japan	Germany
Meet IT governance, risk and compliance	6.04	6.48	4.13	4.73	4.54
Increase focus on data protection	4.20	5.07	4.09	3.82	5.35
Secure and manage Web 2.0 applications	4.88	3.36	4.32	3.64	3.93
Secure all fixed and mobile endpoints	4.64	5.99	5.89	2.98	6.07
Protect against attacks and evolving threats	5.55	4.15	4.71	4.25	4.60
Secure virtualized and cloud environments	3.40	3.36	3.29	5.82	4.71
Reduce IT security spending	2.65	3.56	5.56	3.44	2.48

³ Ibid 2. The actual question as shown in the Appendix ranked 1 = highest priority and 7 = lowest priority.

Figure 6 provides the average of responses for all five countries of the most significant priorities in descending order. Meeting IT governance, risk and compliance requirements and securing all fixed and mobile endpoints are the top priorities.

Figure 6: Most significant security priorities for fiscal year 2011

Rank order reversed to show highest rank as the highest priority

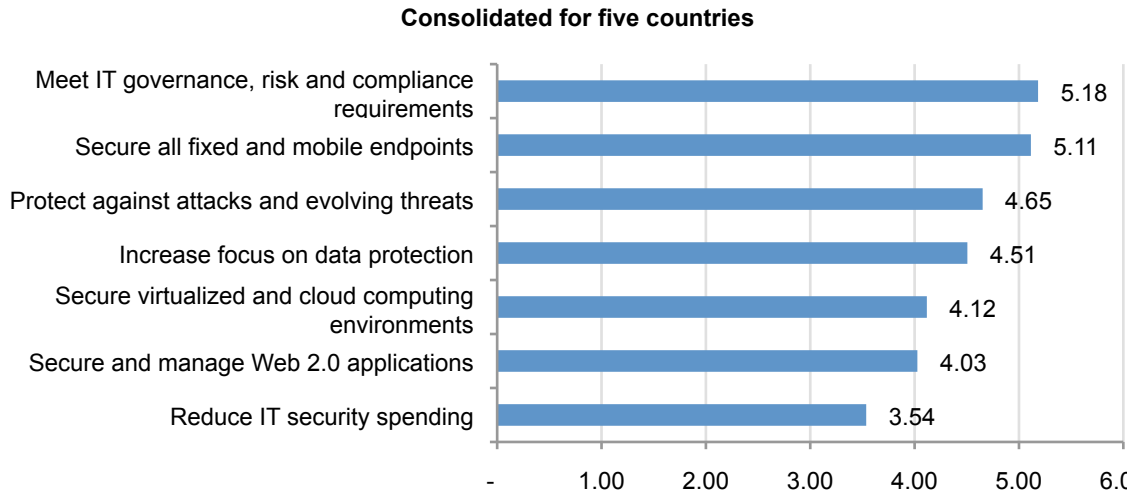


Figure 7 shows the response, “meet IT governance, risk and compliance requirements” varies as a security priority across country samples. Respondents in the UK assign the highest average rank of 6.48, while respondents in France assign the lowest average rank of 4.13.

Figure 7: Country comparison of the top security priority

Rank order reversed to show highest rank as the highest priority

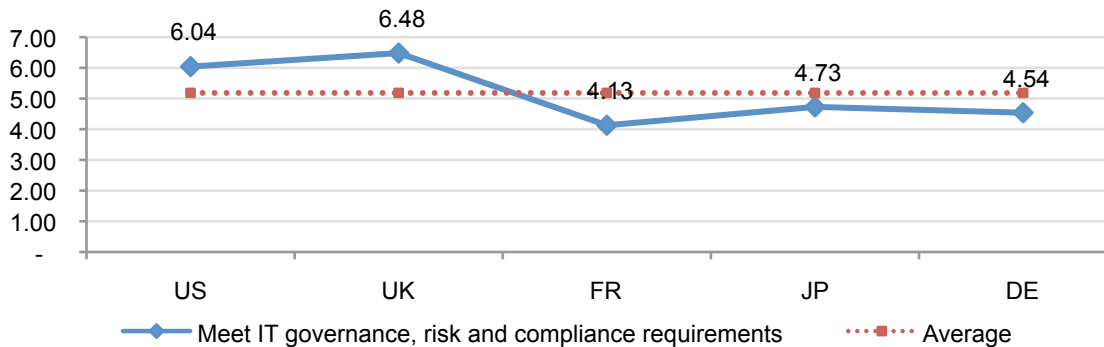


Table 5 summarizes a question focused on functionality of one security feature (i.e., the ability to manage policies by user and device level IP address).

Table 5. Is the ability to manage policies by user, in addition to devices or IP address, a key functionality for your organization today or in the future?	US	UK	France	Japan	Germany
Yes	60%	52%	46%	68%	65%
No	24%	40%	36%	17%	29%
Unsure	16%	8%	18%	15%	6%
Total	100%	100%	100%	100%	100%

Figure 8 clearly shows that managing policies by user, device and IP address is a key functionality for the majority of respondents in all five countries.

Figure 8: Managing policies by user, devices and IP address is a key functionality

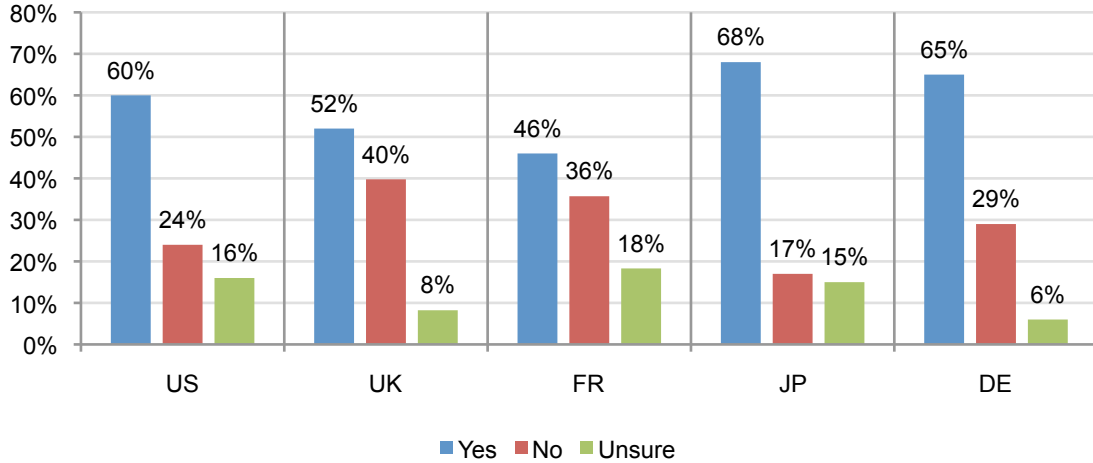


Table 6 lists four top concerns about emerging technology adoption, including cloud computing, virtualization, mobility, Web 2.0 apps and more.

Table 6. What is your top concern about emerging technology adoption, such as cloud computing, virtualization, mobility, Web 2.0 application and others?	US	UK	France	Japan	Germany
Security uncertainty	17%	23%	13%	35%	16%
Costs/budgets	19%	19%	21%	24%	18%
Staffing/IT resources	31%	28%	13%	29%	32%
Compliance	32%	28%	52%	9%	32%
Other (please specify)	1%	2%	1%	2%	2%
Total	100%	100%	100%	100%	100%

Figure 9 shows the average response for all five countries about the top concerns when adopting emerging technologies. (The average for all five countries is shown in the Appendix to this paper).

Figure 9: Concerns about emerging technology adoption

Consolidated for five countries

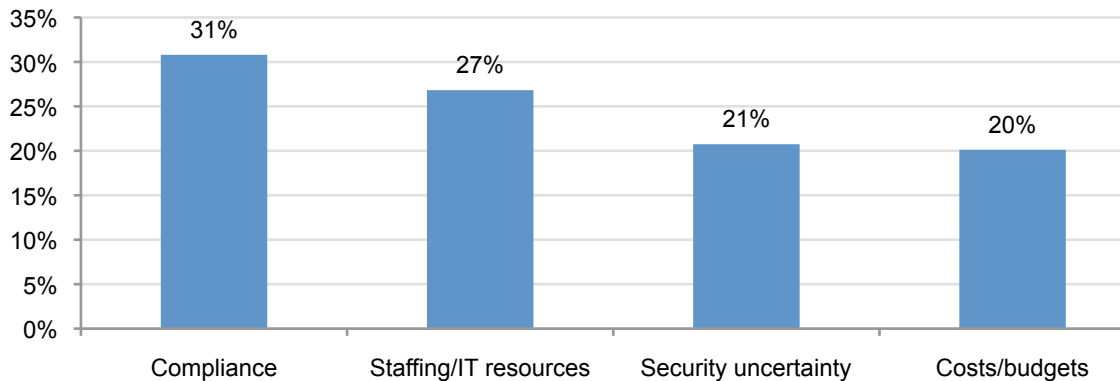


Figure 10 compares respondents' concerns about being in compliance when adopting new technologies. There is significant variation among countries, with respondents in France having the highest level of concern for compliance (52 percent of respondents) and Japan has the lowest level of concern at 9 percent.

Figure 10: Country-level analysis of compliance

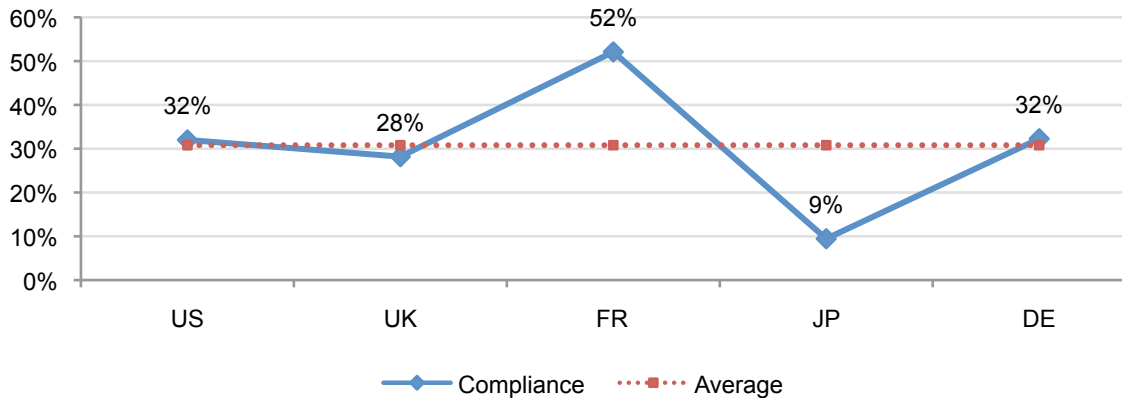


Table 7 presents the percentage of servers organizations plan to virtualize over the next 18-month period.

Table 7. What percentage of servers does your organization plan to virtualize in the next 18 months?	US	UK	France	Japan	Germany
Less than 25%	15%	29%	51%	15%	15%
25-49%	36%	51%	35%	16%	35%
50-74%	19%	16%	10%	21%	30%
75-90%	16%	2%	2%	17%	8%
Greater than 90%	14%	2%	2%	31%	12%
Total	100%	100%	100%	100%	100%
Median	55%	40%	35%	65%	53%

Figure 11 summarizes the percentage of organizations that plan to adopt virtualization for more than 50 percent of their servers. Sixty-nine percent of respondents in Japan project more than 50 percent virtualization followed by Germany at 50 percent and the US at 49 percent. In sharp contrast, respondents in the UK and France are much less likely to project more than 50 percent of their organizations' servers will be virtualized.

Figure 11: Less than 50 percent and more than 50 percent of server virtualization

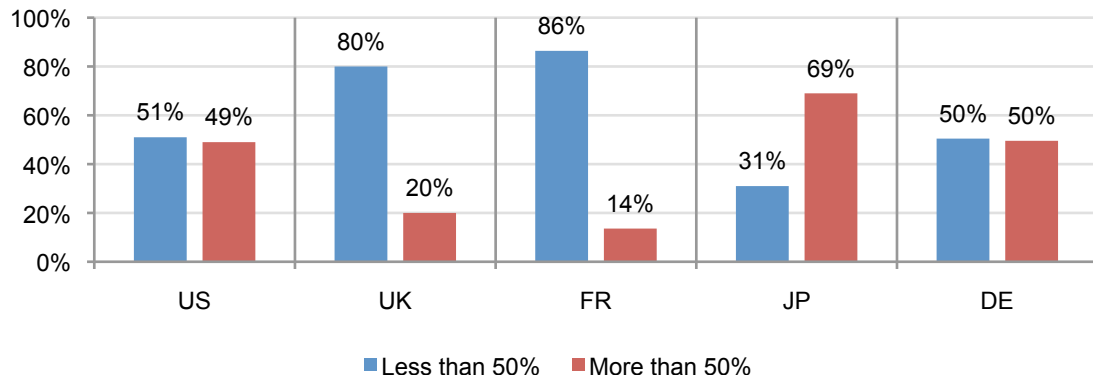


Figure 12 reports the extrapolated median number of virtualized services for respondents in five countries.

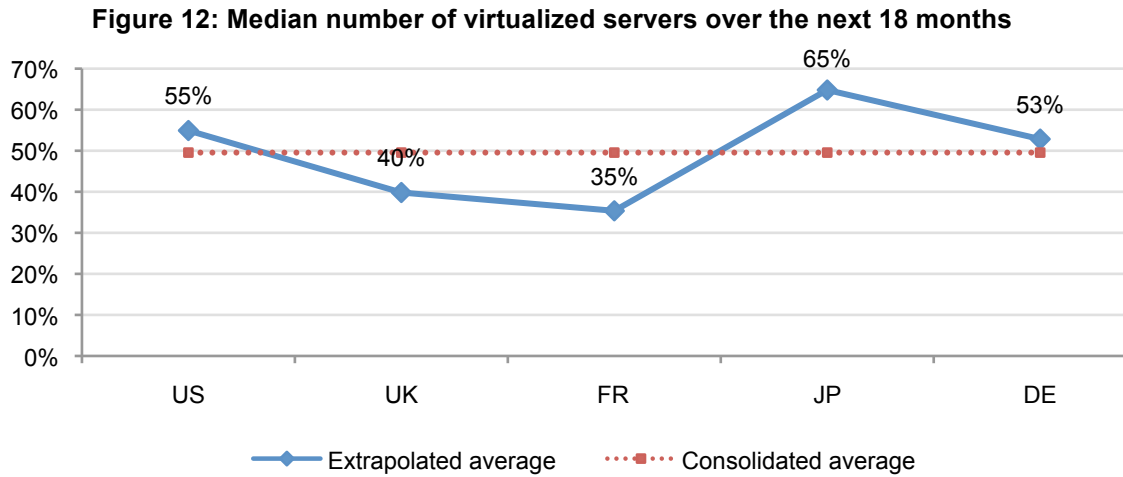


Table 8 lists the primary causes of data loss according to respondents (including those respondents who state they did not experience data loss in the past year).

Table 8. If your organization encountered sensitive data loss last year (regardless of intent) what were the causes?	US	UK	France	Japan	Germany
Respondents who did not encounter data loss	14%	25%	30%	27%	17%
Lost or stolen equipment	32%	35%	29%	31%	29%
Accidentally sending emails to the wrong recipient	7%	6%	4%	5%	7%
Unencrypted USB or media storage device	22%	19%	5%	7%	13%
Web-based application or file sharing site	27%	22%	17%	16%	23%
Insecure mobile devices	15%	8%	10%	18%	12%
Network was hacked	29%	25%	24%	17%	20%
Other	2%	1%	1%	0%	0%
Total	147%	141%	120%	122%	121%

Figure 13 shows that the percentage of respondents who say their organizations encountered the loss or theft of sensitive data is relatively constant across country samples.

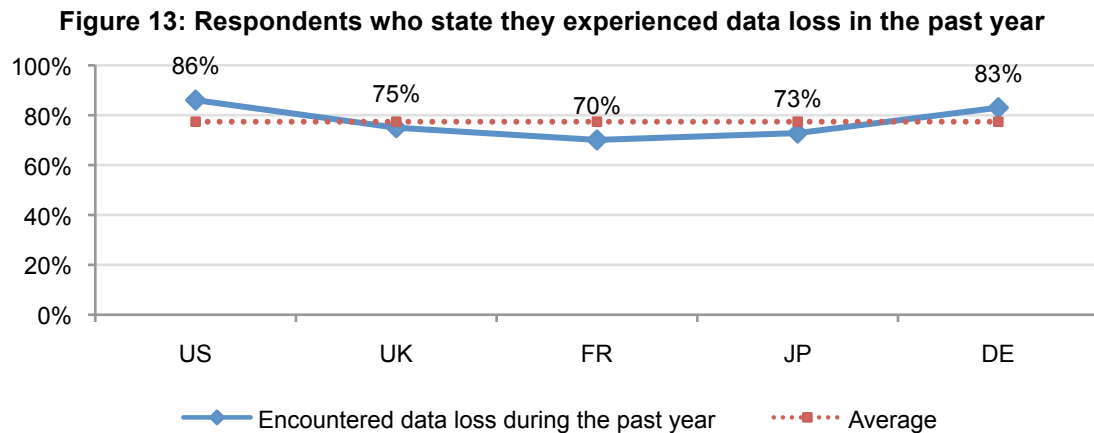


Figure 14 shows that in all five countries the most frequently cited root cause of data loss concerns the loss or theft of equipment including mobile data-bearing devices such as laptop computers. Hacked networks represent the second most frequently cited root cause.

Figure 14: Most frequently cited root causes of data loss or theft

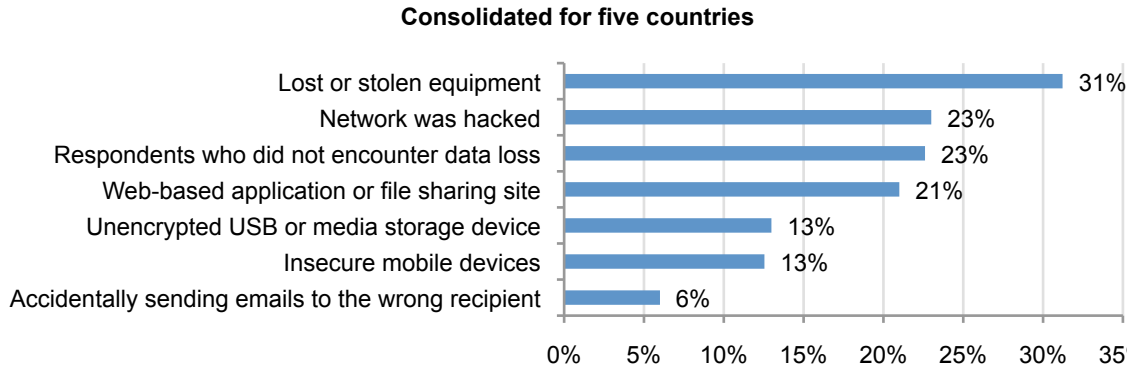


Table 9 summarizes the types of data loss experienced by respondents.

Table 9. If your organization encountered data loss last year, what type of information was disclosed?	US	UK	France	Japan	Germany
Respondents who did not encounter data loss	14%	25%	30%	27%	17%
Corporate plans and strategies	14%	6%	20%	22%	20%
Information about products or services in progress	12%	12%	16%	21%	3%
Financial or accounting information	6%	3%	5%	5%	3%
Employee information	31%	36%	26%	34%	28%
Customer information	56%	52%	51%	50%	52%
Consumer (targeted customer) information	45%	35%	38%	52%	51%
Other intellectual properties such as source code	33%	36%	41%	28%	29%
Unsure	32%	37%	36%	38%	33%

Figure 15 summarizes the most frequently cited information assets that were lost or stolen by respondents' organizations in all five countries sometime during the past year. As can be seen, customer information, consumer information, and intellectual properties are the most likely to be lost or stolen.

Figure 15: Information assets most likely lost or stolen

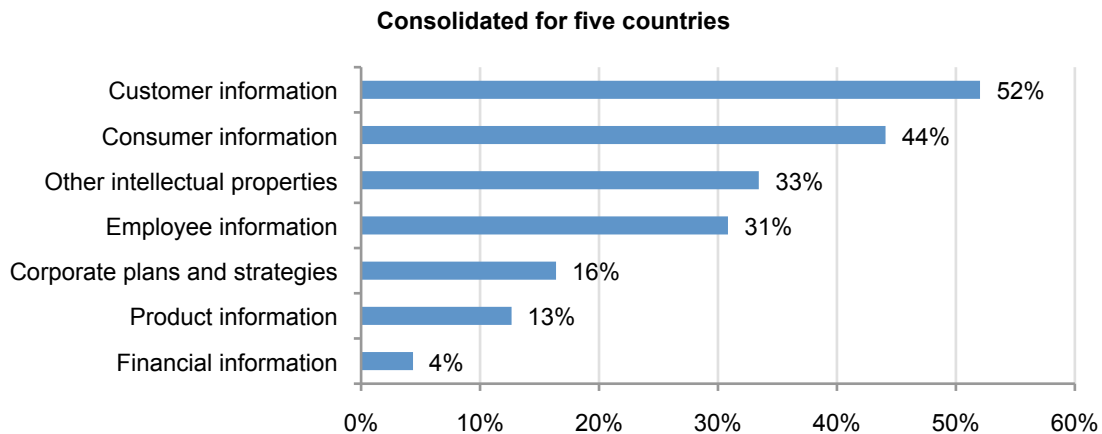


Table 10 summarizes the respondents' perceptions about employees in their organizations in terms of their awareness or knowledge about data security compliance and policies.

Table 10. How would you rate the level of awareness employees in your organization have about data security compliance and policies?	US	UK	France	Japan	Germany
No awareness	15%	19%	29%	9%	9%
Low awareness	36%	34%	45%	23%	25%
Moderate awareness	35%	28%	14%	38%	35%
High awareness	14%	19%	12%	30%	31%
Total	100%	100%	100%	100%	100%

Figures 16 and 17 confirm that respondents perceive employees in their organizations as lacking a sufficient awareness level about data security compliance and policies. The lowest level of employee awareness appears to exist in France and the United Kingdom. In contrast, respondents in Germany and Japan believe employees have a high level of awareness about data security compliance and related policies.

Figure 16: Employee awareness about data security compliance and policies

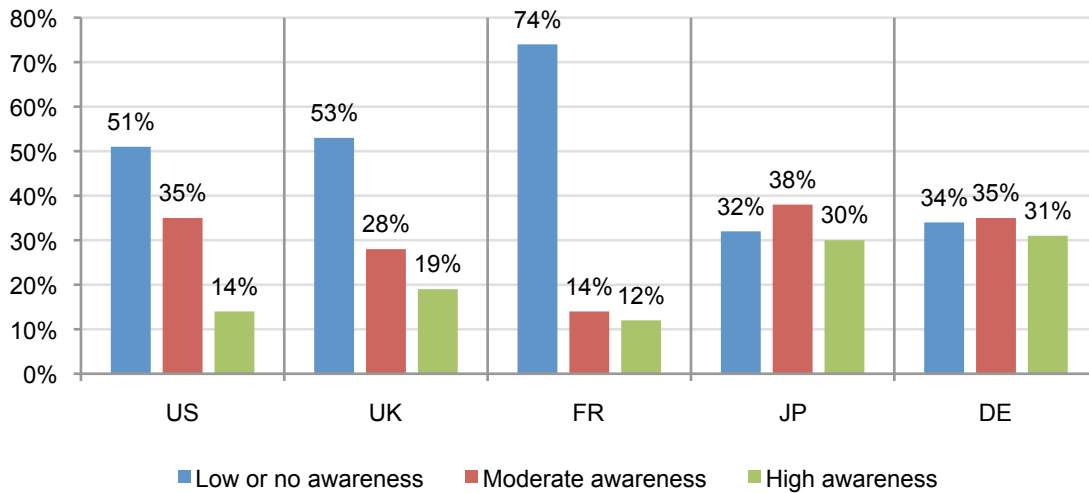
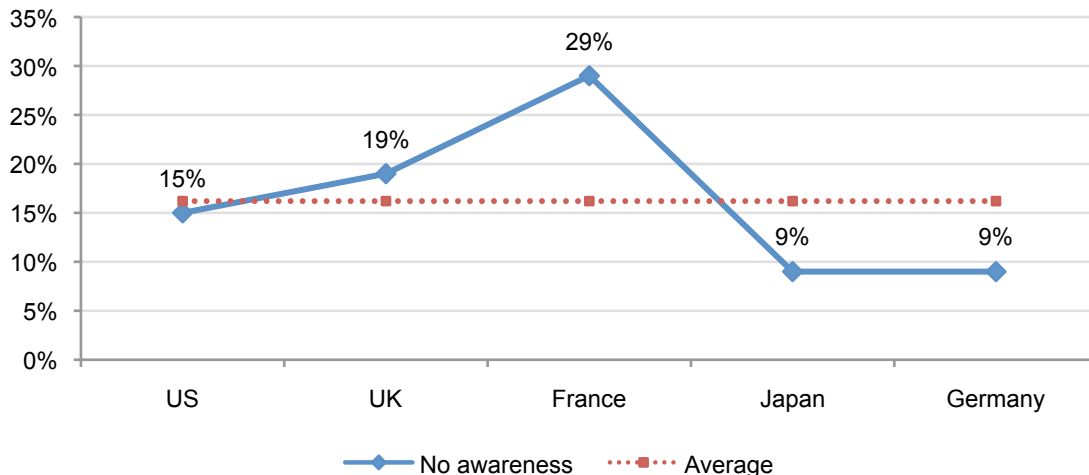


Figure 17: Employees who are not aware of data security compliance and policies



Part 3. Methods

Five national sampling frames consisting of over 51,000 adult-aged individuals who reside in the US, UK, France, Japan and Germany were used to recruit and select participants to this survey. Our omnibus sampling frames were built from several proprietary lists of experienced IT and IT security practitioners. In total, 2,615 respondents completed the survey. Of the returned instruments, 189 surveys failed reliability checks. A total of 2,426 surveys were used as our final Meta sample, which represents a 4.7 percent response rate.

Table 11: Sample response	US	UK	France	Japan	Germany
Total sampling frame	13,447	10,902	8,976	5,993	11,908
Total response	609	491	480	392	643
Rejected responses	45	36	38	41	29
Final sample	564	455	442	351	614
Response rate	4.2%	4.2%	4.9%	5.9%	5.2%

Pie Chart 1 reports the primary industry sector of respondents' organizations for all five-country samples combined. As shown, the largest segments include financial services, industrial, government, services, retail, and services.

Pie Chart 1: Industry distribution consolidated for five countries

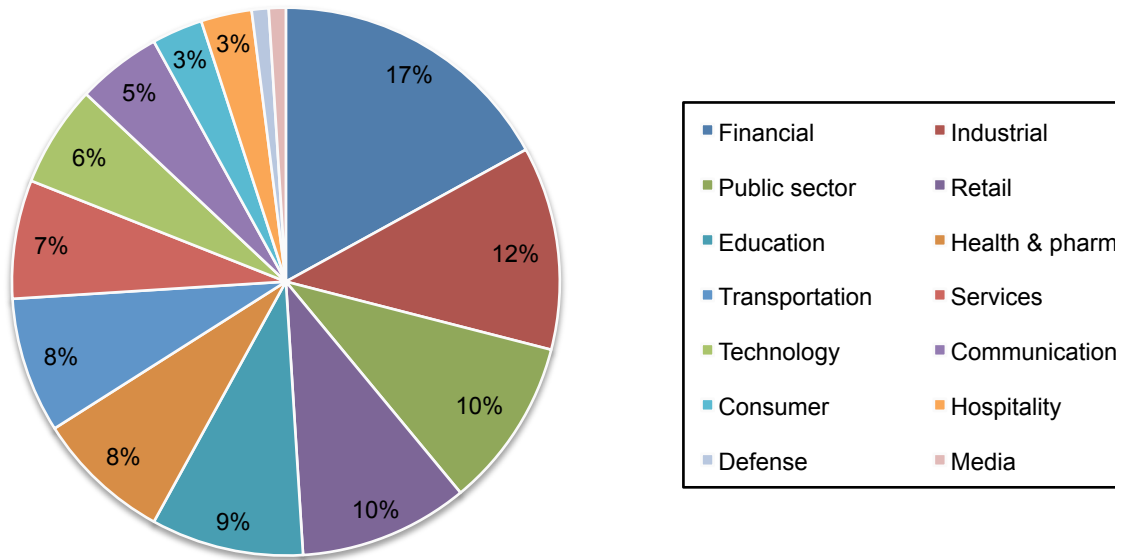


Table 12 reports the respondent organization's global headcount. As shown, 73 percent of respondents work within companies with more than 1,000 employees. More than 42 percent of respondents are located in larger-sized companies with more than 5,000 employees.

Table 12. Worldwide headcount	US	UK	France	Japan	Germany
Less than 500 people	8%	10%	16%	10%	12%
500 to 1,000 people	11%	18%	20%	16%	16%
1,001 to 5,000 people	23%	29%	31%	13%	20%
5,001 to 25,000 people	31%	28%	23%	35%	24%
25,001 to 75,000 people	18%	11%	7%	18%	21%
More than 75,000 people	9%	4%	3%	7%	7%
Total	100%	100%	100%	100%	100%

Table 13 reports the respondent's primary reporting channel. Based on the average of respondents in all five countries, 67 percent of respondents are located in the organization's IT department (led by the company's CIO or CTO).

Table 13. Respondents' reporting channels.	US	UK	France	Japan	Germany
CEO/Executive Committee	1%	2%	5%	0%	2%
Chief Financial Officer (CFO)	4%	5%	4%	2%	2%
General Counsel	3%	6%	6%	3%	0%
Chief Information Officer (CIO)	55%	54%	48%	55%	64%
Chief Information Security Officer (CISO)	17%	10%	9%	8%	15%
Compliance Officer	11%	0%	13%	14%	6%
Human Resources VP	2%	7%	9%	6%	0%
Chief Security Officer (CSO)	3%	5%	2%	10%	2%
Chief Risk Officer	4%	4%	3%	0%	6%
Other	0%	8%	1%	3%	3%
Total	100%	100%	100%	100%	100%

Table 14 reports the respondents' position level. As can be seen, a majority of respondents self-report their positions at or above the supervisory level.

Table 14. Respondents' position level	US	UK	France	Japan	Germany
Senior Executive	1%	1%	5%	2%	2%
Vice President	2%	0%	2%	1%	2%
Director	16%	7%	15%	13%	21%
Manager	21%	20%	21%	28%	12%
Supervisor	19%	17%	16%	12%	17%
Technician	22%	28%	24%	24%	29%
Staff	12%	18%	6%	14%	5%
Contractor	5%	6%	0%	7%	1%
Other	2%	3%	11%	0%	11%
Total	100%	100%	100%	100%	100%

Overall, the sample consisted of individuals who hold full-time employment in the IT or a related field. The median and median years of experience level in IT or IT security for the combined samples are 11.5 and 10.0, respectively. Approximately, 22 percent of respondents are female and 78 percent male. Please note that this skewed result on gender is consistent with other global studies of IT and IT security practitioners. Other facts about this sample are provided in the Appendix to this report.

Part 4. Caveats

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

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used an omnibus collection method, it is possible that responses are biased by other items contained in the Meta survey instrument.
- 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 I: Survey Question Details

Fieldwork concluded on April 16, 2010

Sample response	US	UK	France	Japan	Germany	Average
Total sampling frame	13447	10902	8976	5993	11908	51226
Total response	609	491	480	392	643	2615
Rejected responses	45	36	38	41	29	189
Final sample	564	455	442	351	614	2426
Response rate	4.2%	4.2%	4.9%	5.9%	5.2%	4.7%

Q1. On average, how many different vendors do you use to secure your organization's network?	US	UK	France	Japan	Germany	Average
1 to 2	19%	30%	10%	11%	30%	20%
3 to 6	21%	42%	24%	23%	14%	25%
7 to 10	42%	20%	33%	21%	31%	29%
More than 10	18%	8%	33%	45%	25%	26%
Total	100%	100%	100%	100%	100%	100%
Median	6.96	5.00	7.97	8.40	6.71	7.01

Q2. Please rank the following three obstacles when consolidating the number of vendors (1 = most concern to 3 = least concern)*	US	UK	France	Japan	Germany	Average
Limited availability of integrated solutions	1.99	2.53	2.56	2.96	1.56	2.32
Ensuring optimal performance	2.87	1.19	2.23	2.24	2.01	2.11
Pricing and/or total cost of ownership	1.54	1.41	1.35	1.18	2.57	1.61

*Ranking reversed in the analysis section

Q3. Which of the following is the most significant information security challenge facing your company? Please select only one choice.	US	UK	France	Japan	Germany	Average
Industry and/or government compliance mandates	19%	16%	28%	21%	29%	22%
Managing the complexity of security	33%	35%	35%	24%	36%	33%
Enforcing security policies	15%	7%	7%	24%	12%	13%
Preventing data breaches from outside attackers	12%	14%	14%	14%	7%	12%
Preventing data loss by employees or others	21%	28%	17%	17%	16%	20%
Total	100%	100%	100%	100%	100%	100%

Q4. Please rank the following security priorities for 2011 (1 = highest priority to 7 = lowest priority)*	US	UK	France	Japan	Germany	Average
Meet IT governance, risk and compliance	1.96	1.52	3.87	3.27	3.46	2.82
Increase focus on data protection	3.80	2.93	3.91	4.18	2.65	3.49
Secure and manage Web 2.0 applications	3.12	4.64	3.68	4.36	4.07	3.97
Secure all fixed and mobile endpoints	3.36	2.01	2.11	5.02	1.93	2.89
Protect against attacks and evolving threats	2.45	3.85	3.29	3.75	3.40	3.35
Secure virtualized and cloud environments	4.60	4.64	4.71	2.18	3.29	3.88
Reduce IT security spending	5.35	4.44	2.44	4.56	5.52	4.46

*Ranking reversed in the analysis section

Q5. Is the ability to manage policies by user, in addition to devices or IP address, a key functionality for your organization today or in the future?	US	UK	France	Japan	Germany	Average
Yes	60%	52%	46%	68%	65%	58%
No	24%	40%	36%	17%	29%	29%
Unsure	16%	8%	18%	15%	6%	13%
Total	100%	100%	100%	100%	100%	100%

Q6. What is your top concern about emerging technology adoption, such as cloud computing, virtualization, mobility, Web 2.0 application and others?	US	UK	France	Japan	Germany	Average
Security uncertainty	17%	23%	13%	35%	16%	21%
Costs/budgets	19%	19%	21%	24%	18%	20%
Staffing/IT resources	31%	28%	13%	29%	32%	27%
Compliance	32%	28%	52%	9%	32%	31%
Other (please specify)	1%	2%	1%	2%	2%	2%
Total	100%	100%	100%	100%	100%	100%

Q7. What percentage of servers does your organization plan to virtualize in the next 18 months?	US	UK	France	Japan	Germany	Average
Less than 25%	15%	29%	51%	15%	15%	25%
25-49%	36%	51%	35%	16%	35%	35%
50-74%	19%	16%	10%	21%	30%	19%
75-90%	16%	2%	2%	17%	8%	9%
Greater than 90%	14%	2%	2%	31%	12%	12%
Total	100%	100%	100%	100%	100%	100%
Median	55%	40%	35%	65%	53%	50%

Q8. If your organization encountered sensitive data loss last year (regardless of intent) what were the causes? Please select all that apply.	US	UK	France	Japan	Germany	Average
Respondents who did not encounter data loss	14%	25%	30%	27%	17%	23%
Lost or stolen equipment	32%	35%	29%	31%	29%	31%
Accidentally sending emails to the wrong recipient	7%	6%	4%	5%	7%	6%
Unencrypted USB or media storage device	22%	19%	5%	7%	13%	13%
Web-based application or file sharing site	27%	22%	17%	16%	23%	21%
Insecure mobile devices	15%	8%	10%	18%	12%	13%
Network was hacked	29%	25%	24%	17%	20%	23%
Other (please specify)	2%	1%	1%	0%	0%	1%
Total	147%	141%	120%	122%	121%	130%

Q9. If your organization encountered data loss last year, what type of information was lost or disclosed? Please check all that apply.	US	UK	France	Japan	Germany	Average
Respondents who did not encounter data loss	14%	25%	30%	27%	17%	23%
Corporate plans and strategies	14%	6%	20%	22%	20%	16%
Information about products or services in progress	12%	12%	16%	21%	3%	13%
Financial or accounting information	6%	3%	5%	5%	3%	4%
Employee information	31%	36%	26%	34%	28%	31%
Customer information	56%	52%	51%	50%	52%	52%
Consumer (targeted customer) information	45%	35%	38%	52%	51%	44%
Other intellectual properties such as source code	33%	36%	41%	28%	29%	33%
Unsure	32%	37%	36%	38%	33%	35%
Other (please specify)	1%	0%	0%	2%	0%	1%
Total	244%	241%	263%	277%	236%	252%

Q10. How would you rate the level of awareness employees in your organization have about data security compliance and policies?	US	UK	France	Japan	Germany	Average
No awareness	15%	19%	29%	9%	9%	16%
Low awareness	36%	34%	45%	23%	25%	33%
Moderate awareness	35%	28%	14%	38%	35%	30%
High awareness	14%	19%	12%	30%	31%	21%
Total	100%	100%	100%	100%	100%	100%

Organizational Characteristics & Demographics

D1. What organizational level best describes your current position?	US	UK	France	Japan	Germany	Average
Senior Executive	1%	1%	5%	2%	2%	2%
Vice President	2%	0%	2%	1%	2%	1%
Director	16%	7%	15%	13%	21%	15%
Manager	21%	20%	21%	28%	12%	20%
Supervisor	19%	17%	16%	12%	17%	16%
Technician	22%	28%	24%	24%	29%	25%
Staff	12%	18%	6%	14%	5%	11%
Contractor	5%	6%	0%	7%	1%	4%
Other	2%	3%	11%	0%	11%	6%
Total	100%	100%	100%	100%	100%	100%

D2. Is this a full time position?	US	UK	France	Japan	Germany	Average
Yes	98%	97%	94%	100%	96%	97%
No	2%	3%	6%	0%	4%	3%
Total	100%	100%	100%	100%	100%	100%

D3. Check the Primary Person you or your IT security leader reports to within the organization.	US	UK	France	Japan	Germany	Average
CEO/Executive Committee	1%	2%	5%	0%	2%	2%
Chief Financial Officer (CFO)	4%	5%	4%	2%	2%	3%
General Counsel	3%	6%	6%	3%	0%	4%
Chief Information Officer (CIO)	55%	54%	48%	55%	64%	55%
Chief Information Security Officer (CISO)	17%	10%	9%	8%	15%	12%
Compliance Officer	11%	0%	13%	14%	6%	9%
Human Resources VP	2%	7%	9%	6%	0%	5%
Chief Security Officer (CSO)	3%	5%	2%	10%	2%	4%
Chief Risk Officer	4%	4%	3%	0%	6%	3%
Other	0%	8%	1%	3%	3%	3%
Total	100%	100%	100%	100%	100%	100%

D4. Experience in IT or IT security	US	UK	France	Japan	Germany	Average
D4a. Total years of experience	11.9	12.2	13.4	9.26	10.8	11.51
D4b. Total years in present position	4.5	6.7	5.2	4.6	6.8	5.56

D5. Gender	US	UK	France	Japan	Germany	Average
Female	24%	22%	26%	19%	20%	22%
Male	76%	78%	74%	81%	80%	78%
Total	100%	100%	100%	100%	100%	100%

D6. What best describes your organization's industry classification	US	UK	France	Japan	Germany	Average
Airlines	1%	1%	4%	5%	1%	2%
Automotive	1%	4%	2%	7%	4%	4%
Brokerage & Investments	3%	2%	2%	1%	1%	2%
Communications	4%	3%	2%	3%	4%	3%
Consumer	5%	3%	1%	6%	0%	3%
Credit Cards	2%	4%	1%	0%	1%	2%
Defense	1%	5%	0%	0%	0%	1%
Education	3%	5%	8%	4%	7%	5%
Energy	2%	2%	0%	4%	0%	2%
Entertainment and Media	1%	1%	2%	2%	1%	1%
Government	8%	10%	14%	8%	12%	10%
Food Service	1%	0%	4%	3%	1%	2%
Healthcare	8%	2%	3%	2%	5%	4%
Hospitality	4%	3%	3%	2%	3%	3%
Industrial	8%	12%	8%	13%	10%	10%
Insurance	1%	2%	1%	0%	0%	1%
Internet & ISPs	1%	0%	3%	3%	5%	2%
Pharmaceuticals	4%	9%	0%	0%	5%	4%
Professional Services	3%	0%	5%	2%	3%	2%
Research	3%	3%	0%	9%	4%	4%
Retailing	8%	6%	10%	9%	5%	8%
Retail Banking	14%	13%	11%	10%	12%	12%
Services	5%	7%	3%	5%	6%	5%
Technology & Software	6%	3%	10%	0%	9%	6%
Transportation	3%	0%	3%	2%	1%	2%
Total	100%	100%	100%	100%	100%	100%

D7. Where are your employees located? Check all that apply.	US	UK	France	Japan	Germany	Average
United States	100%	87%	76%	81%	83%	85%
Canada	92%	77%	56%	79%	62%	73%
Europe	76%	100%	100%	78%	100%	91%
Middle East	50%	51%	65%	46%	57%	54%
Asia-Pacific	72%	56%	60%	100%	67%	71%
Latin America (including Mexico)	88%	47%	39%	49%	43%	53%
Africa	34%	36%	42%	23%	35%	34%

D8. What is the worldwide headcount of your organization?	US	UK	France	Japan	Germany	Average
Less than 500 people	8%	10%	16%	10%	12%	11%
500 to 1,000 people	11%	18%	20%	16%	16%	16%
1,001 to 5,000 people	23%	29%	31%	13%	20%	23%
5,001 to 25,000 people	31%	28%	23%	35%	24%	28%
25,001 to 75,000 people	18%	11%	7%	18%	21%	15%
More than 75,000 people	9%	4%	3%	7%	7%	6%
Total	100%	100%	100%	100%	100%	100%

Ponemon Institute

Advancing Responsible Information Management

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

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