Business Risk of a Lost Laptop

A Study of IT Practitioners in the United States, United Kingdom, Germany, France, Mexico & Brazil

---

Sponsored by

Dell Corporation

Independently conducted by Ponemon Institute LLC

Publication Date: April 15, 2009

Business Risk of a Lost Laptop

IT Practitioners in the United States, United Kingdom, Germany, France, Mexico & Brazil
Presented by Dr. Larry Ponemon, April 15, 2009

Executive Summary

Dell Corporation and Ponemon Institute, LLC are pleased to report the results of the *Business Risk of Lost Laptops in the United States, United Kingdom, Germany, France, Mexico and Brazil.* The study was conducted to understand the risks to organizations' personal and confidential information as the number of lost or stolen employee-assigned laptops increases. We also wanted to learn if there are significant differences in how companies in these different countries are addressing the business risk of lost laptops.

Ponemon Institute conducted a web-based survey of 3,100 information technology (IT) and IT security practitioners located in the United States, United Kingdom, Germany, France, Mexico and Brazil who have significant experience and are employed in the public or private sector. In this report, we provide a high-level comparative analysis of the findings from respondents in these six countries. Demographics of survey respondents are summarized at the conclusion of this report. Individual country-level reports are also available upon request.

The questions sought by this research address the following topics:

- Why is it important to understand the business risk of lost or missing laptops?
- What is the business risk of lost or missing laptops?
- In addition to lost laptops, what are the most significant threats to data security?
- Does the human factor put laptops and data at risk?
- What can organizations do to reduce the business risk of a lost or missing laptop?
- Do IT and IT security practitioners in six countries perceive or respond differently to the business risks associated with a lost or stolen laptop computer?

The next section provides the detail findings of six separate national surveys in bar chart format. The country legend used within bar charts is as follows:

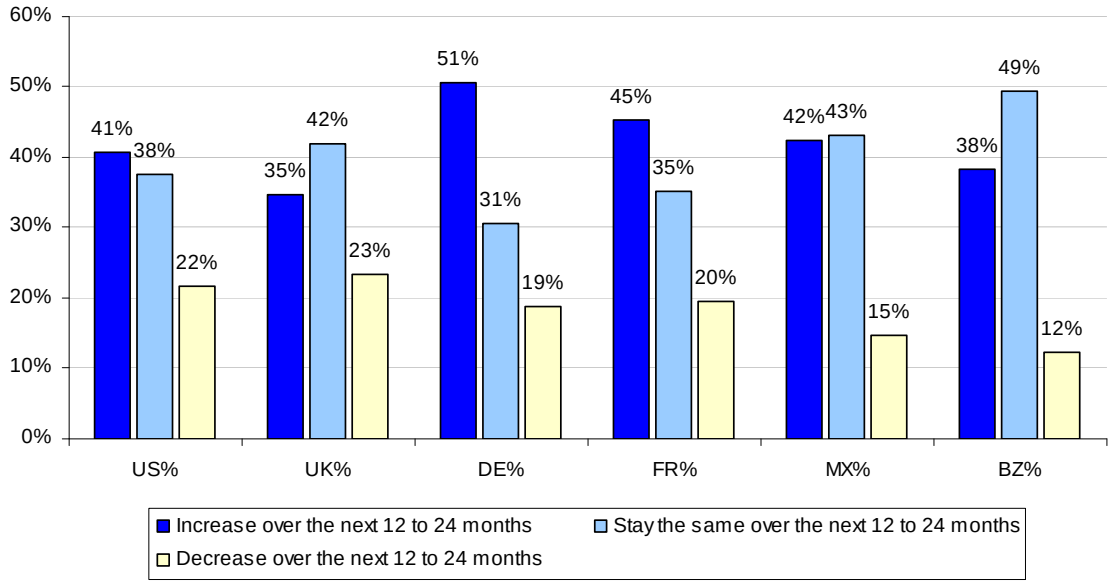
US = United States, UK = United Kingdom, FR = France, DE = Germany, MX = Mexico and BZ = Brazil.

Why organizations are at risk

Anytime and anywhere employees, temporary employees and contractors can access and store enormous amounts of confidential data about customers, employees and their organizations' operations on laptops. When these laptops are lost due to negligence or theft, the data is at risk if the organization has failed to use such safeguards as encryption or anti-theft technologies. At the conclusion of this report, we recommend seven steps that can help prevent the loss and avoid the business risk of a missing laptop.

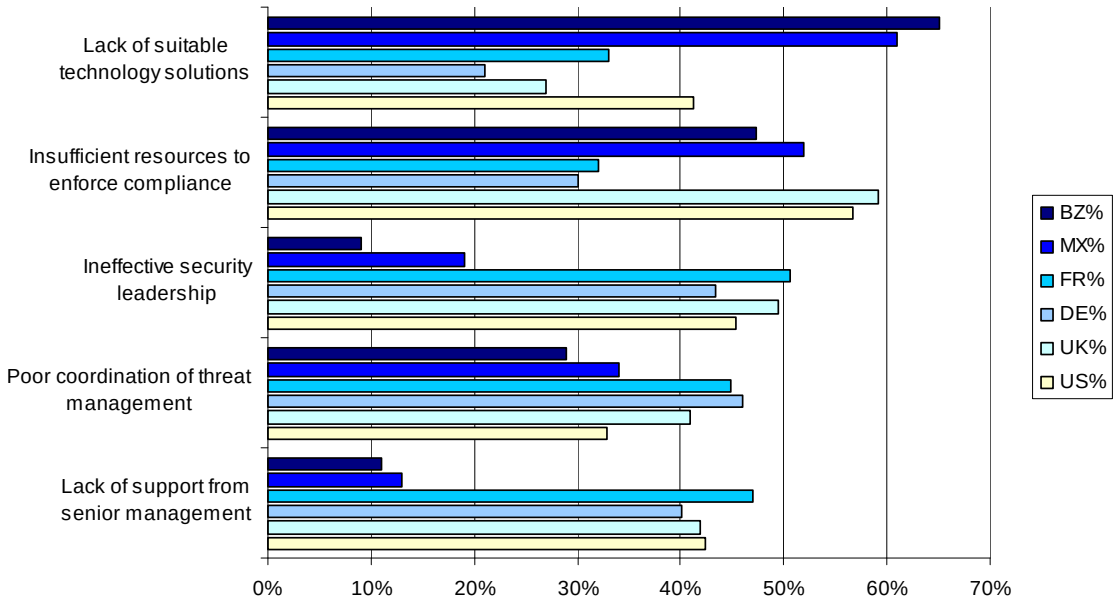
As shown in Bar Chart 1a, a majority of IT professionals in all six countries believe the risk of having lost or stolen laptops will most likely increase or stay the same (i.e., not improve) over the next 12 to 24 months.

Bar Chart 1a
How does the risk of having a lost or stolen laptop change over time?



According to Bar Chart 1b, in the US and UK, the number one reason for the risk is insufficient resources to enforce compliance followed by ineffective security leadership and lack of support from senior management. For Germans, the top reason for increasing laptop loss is poor coordination of threat management and ineffective security management. In France, the top reason is ineffective security leadership and lack of senior management support. Mexico and Brazil blame lack of suitable technology solutions and insufficient resources.

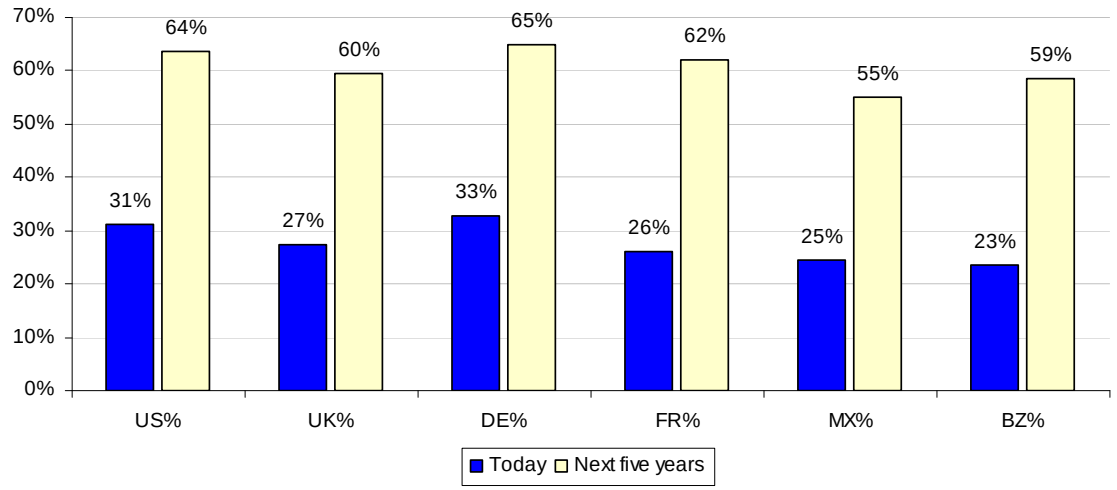
Bar Chart 1b
Why does the risk increase or stay the same?



The business risk of a lost laptop is likely to increase because more employees are expected to have laptop computers in the near future. Accordingly, Bar Chart 2 shows the average percentage of employees who are assigned a laptop as their primary computing device by their organizations. This chart also shows the percentage of employees who are expected to be assigned laptops as their primary computer sometime in the next five years. As can be seen, in all six countries significantly more laptops will be assigned to employees.

Bar Chart 2

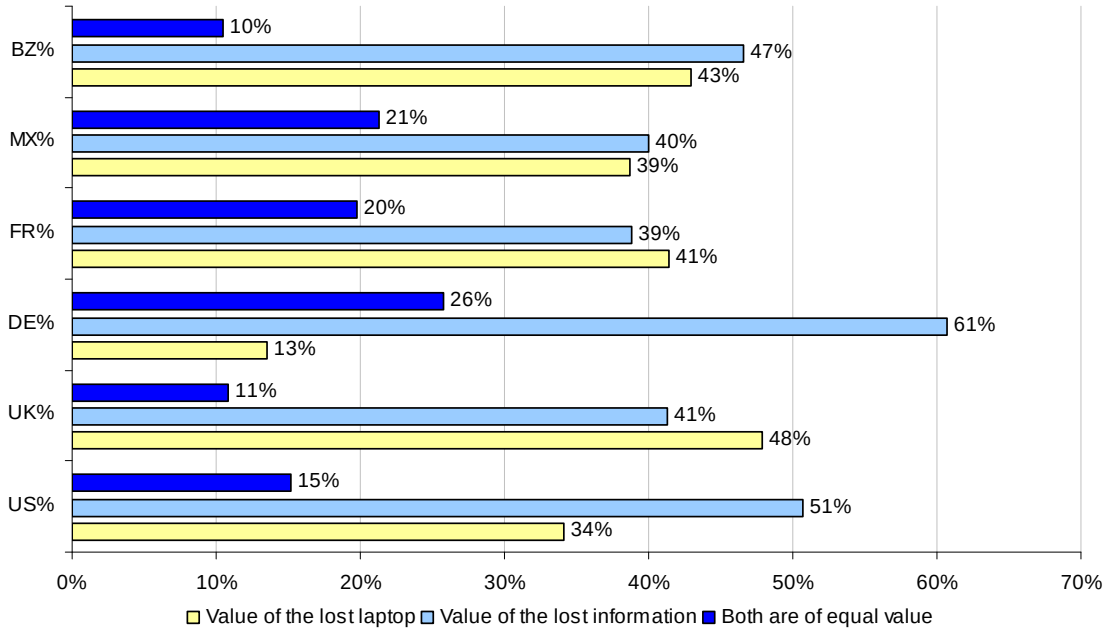
The use of laptop use in business organizations today and in the next five years (expected)



What is most valuable – the lost information or the lost computer? As shown in Bar Chart 3, respondents in all six countries believe the information residing on the lost laptop is more valuable than the replacement cost of the computer equipment. German respondents appear to hold the strongest belief about the value of lost information versus lost equipment.

Bar Chart 3

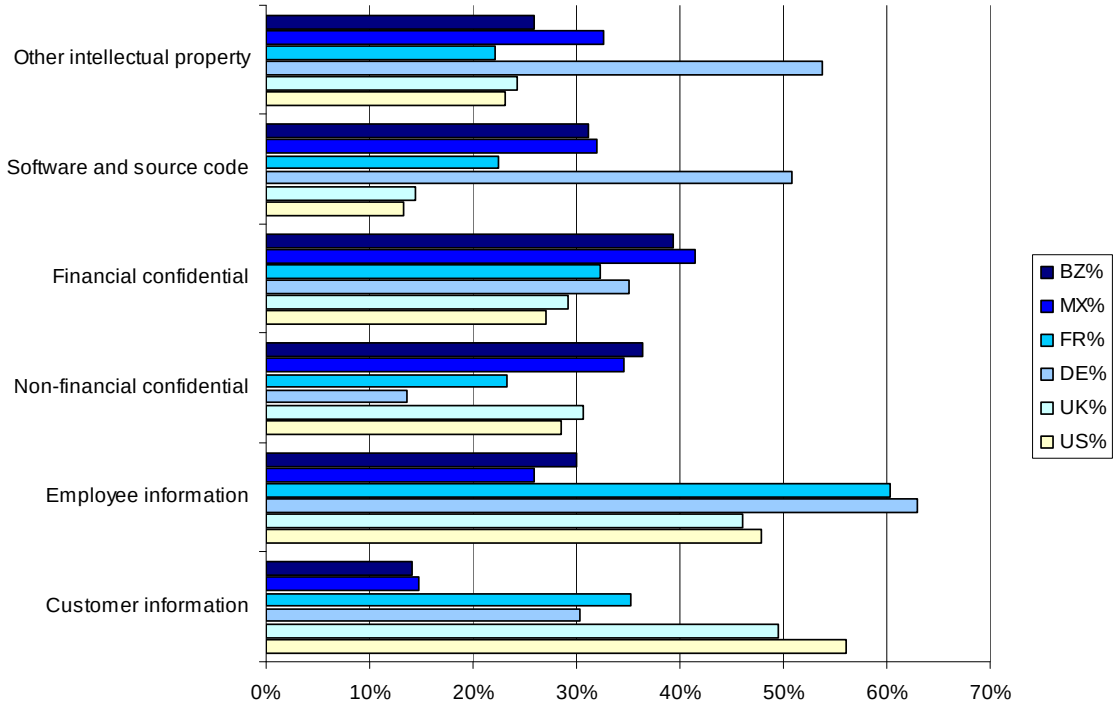
What is most valuable - lost information or the laptop computer?



In Germany and France, employee records pose the greatest business risk when a laptop is lost or stolen. While US respondents say it is customer information (such as contact lists). These differences may be attributable, at least in part, to regional privacy and data protection regulations. In Brazil and Mexico respondents appear to worry most about confidential financial information. It is also interesting to see that German respondents are most likely to attach a high risk value to lost or stolen intellectual property and source code than respondents in other countries.

Bar Chart 4

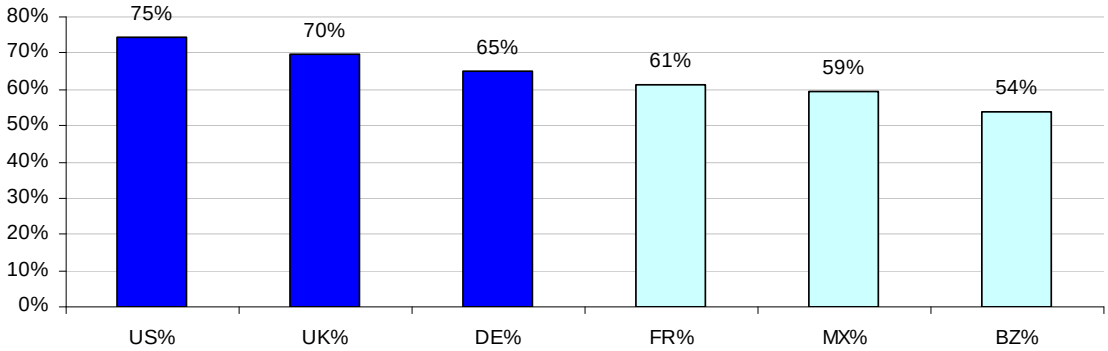
What types of information pose the greatest risk if lost or stolen?



The majority of respondents in every country are aware of an incident in their organizations where confidential or sensitive information was at risk as a result of a lost or stolen laptop computer. As shown in Bar Chart 5, the highest percentage of known incidents involving the loss of sensitive data on a laptop computer is in the US (75%) and the lowest percent is in Brazil (54%).

Bar Chart 5

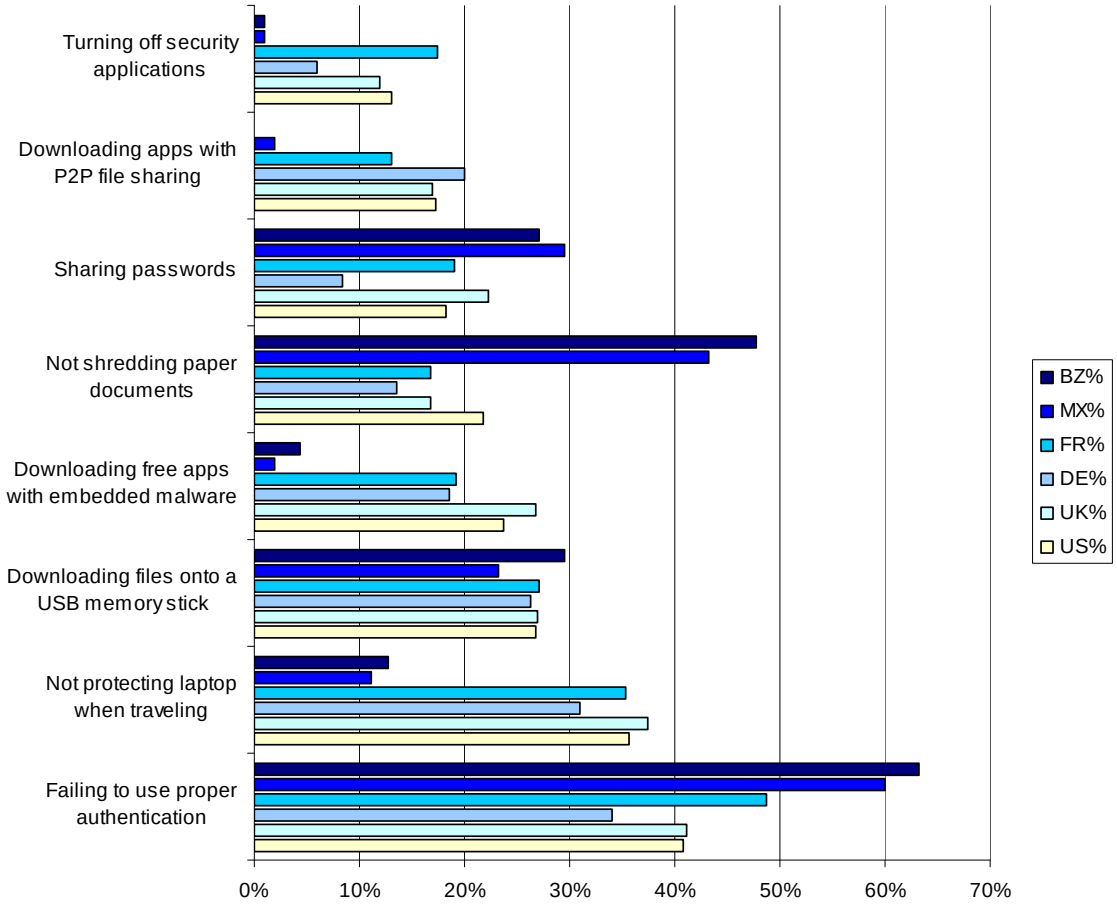
Are you aware of an incident in your organization where sensitive information was at risk because of a laptop computer? Each bar shows the percentage Yes response.



Are organizations taking the necessary steps to secure laptops and the data contained on those laptops? According to Bar Chart 6, the number one threat caused by employees to their organizations' confidential data is the failure to use proper authentication or passwords.

Bar Chart 6

What are the most serious threats caused by employees to a company's confidential data?

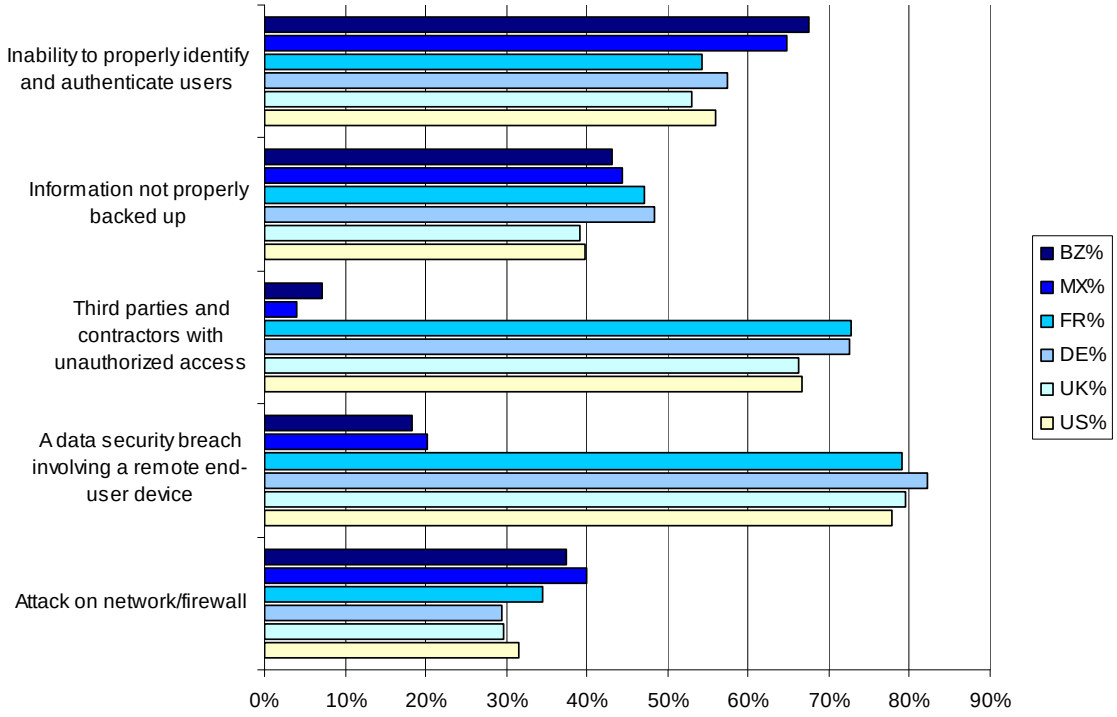


Employees who do not protect laptops when traveling and transferring files on USB memory sticks are also considered serious threats. However, in Mexico and Brazil the number two threat is not shredding paper documents containing confidential information.

As shown in Bar Chart 7, overall there seems to be consistency in how threats to information security are perceived by respondents in all six countries. However, there are some interesting differences. For example, the greatest threat to information security in the US, UK, Germany and France is a data security breach involving a remote end-user device not protected by corporate firewall, followed by third parties and contractors with unauthorized access to their network. However, it is interesting to note that this threat seems to be negligible for IT practitioners in Mexico and Brazil.

Respondents in Mexico and Brazil say the biggest threat is the inability to properly identify and authenticate users to their organizations' multiple systems followed by information not properly backed up and attacks on network/firewall. According to respondents in the US, UK, Germany and France, an attack on the network or firewall is the least concern.

Bar Chart 7
What are the greatest threats to your organization's information security?



How employees put data at risk

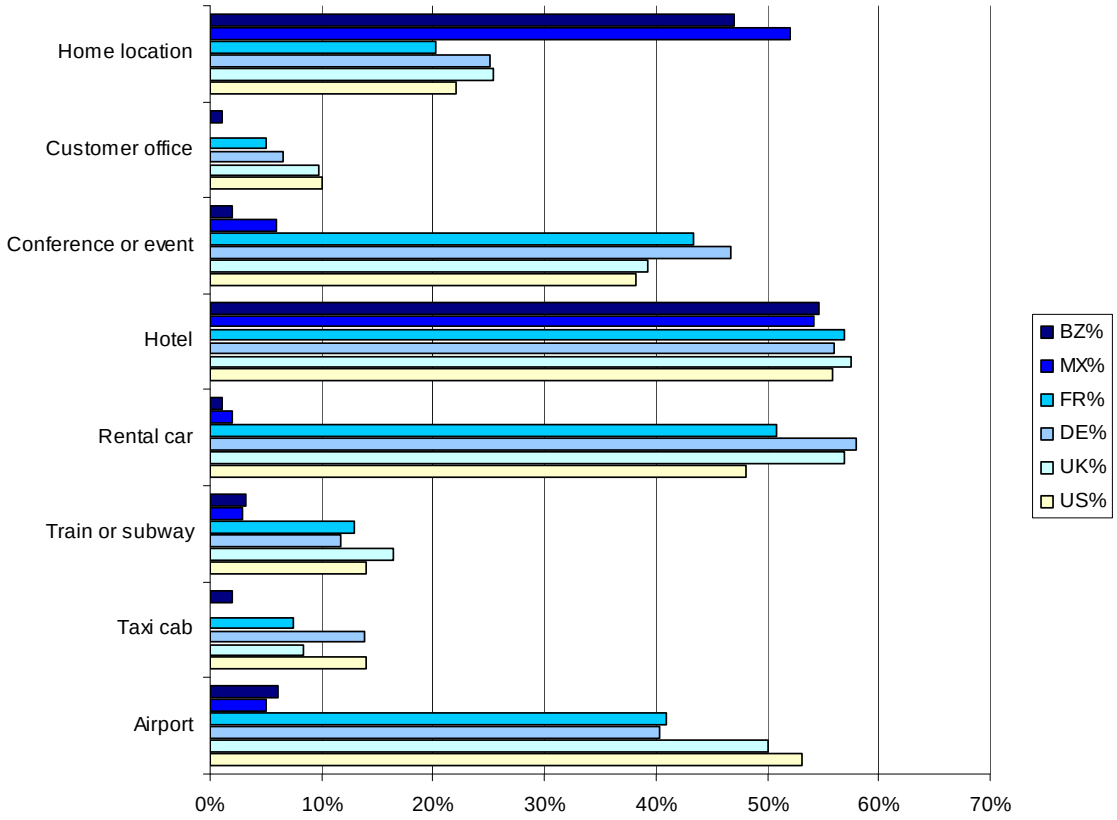
Findings from all six national surveys suggest that employees are often careless or deliberately circumvent security procedures. According to survey results, employees are most likely to lose a laptop computer during travel at such locations as hotels, airports, rental cars and at conference events.

As shown in Bar Chart 8, the number one location where employees lose their laptops is a hotel according to respondents from the US, UK, France, Mexico and Brazil. In Germany, the most likely location is in a rental car. US and UK respondents select airports as one of their top three locations where employees lose laptops. In contrast, only a small number of respondents in Mexico and Brazil cite airports as a frequently encountered location for laptop loss or theft. Instead home locations, which can include personal cars, are likely locations to lose or have a laptop stolen in Mexico and Brazil.

The least likely location for laptop loss or theft in the US, Germany, France, Mexico and Brazil is a client or customer office. In Mexico and Brazil, the least likely place for experiencing the loss or theft of a laptop computer is in a rental car, and in the UK the least likely location for laptop loss is in a taxi.

Bar Chart 8

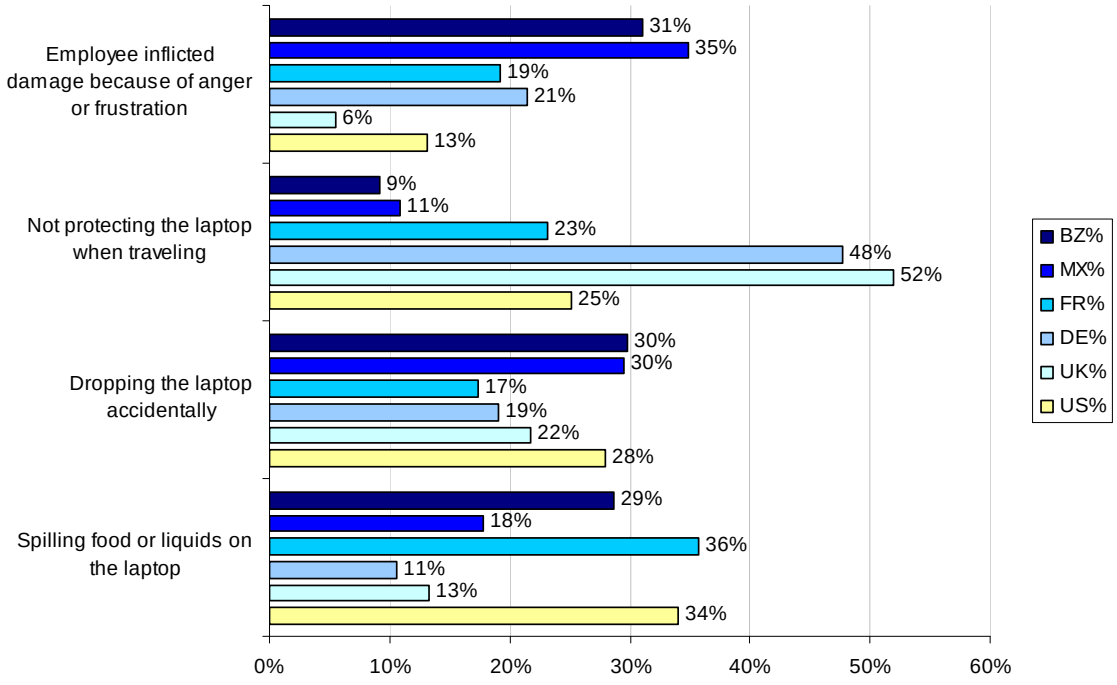
Where are the most common locations where employees lose laptops?



Bar Chart 9 reports the most common causes of physical damage to laptop computers. In the US and France the most common cause of damage involves spilled food or liquids onto the laptop. In contrast, respondents in Mexico and Brazil state that employee inflicted damage because of anger or frustration is the most common cause of laptop damage.

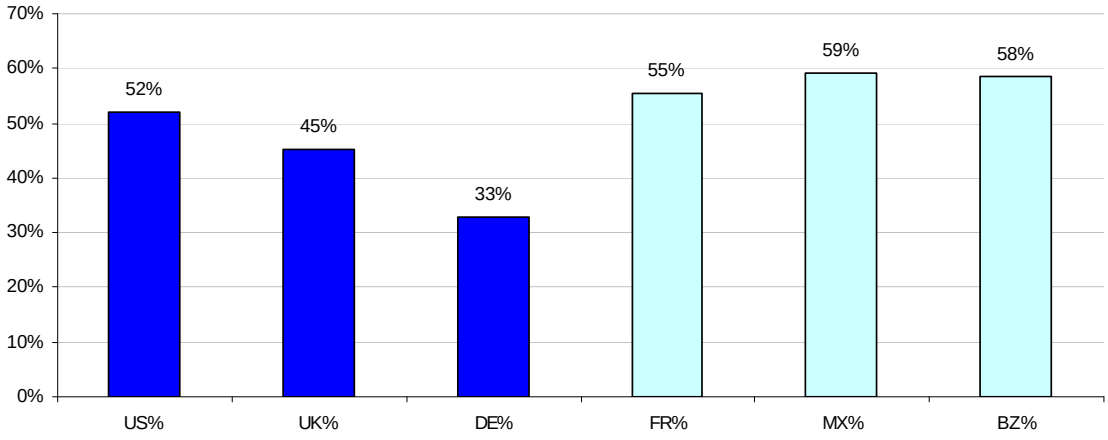
In the UK and Germany, the most common cause of laptop damage is the failure of employees to adequately protect their laptop when traveling. More than 30% of respondents in Mexico and Brazil state that physical damage to laptops occur because of accidental drops or lax handling – in other words, employee incompetence.

Bar Chart 9
What are the most common causes of physical damage to laptops?



According to Bar Chart 10, more than half of respondents in the US (52%), France (55%), Mexico (59%) and Brazil (58%) admit that their company lost sensitive or confidential data because of employee-inflicted physical damage to laptop computers. Only 33% of respondents in Germany state that their companies lost sensitive or confidential data as a result of damage to the laptop.

Bar Chart 10
Did your company ever lose data because of physical damage to a laptop computer? Each bar shows the percentage Yes response.

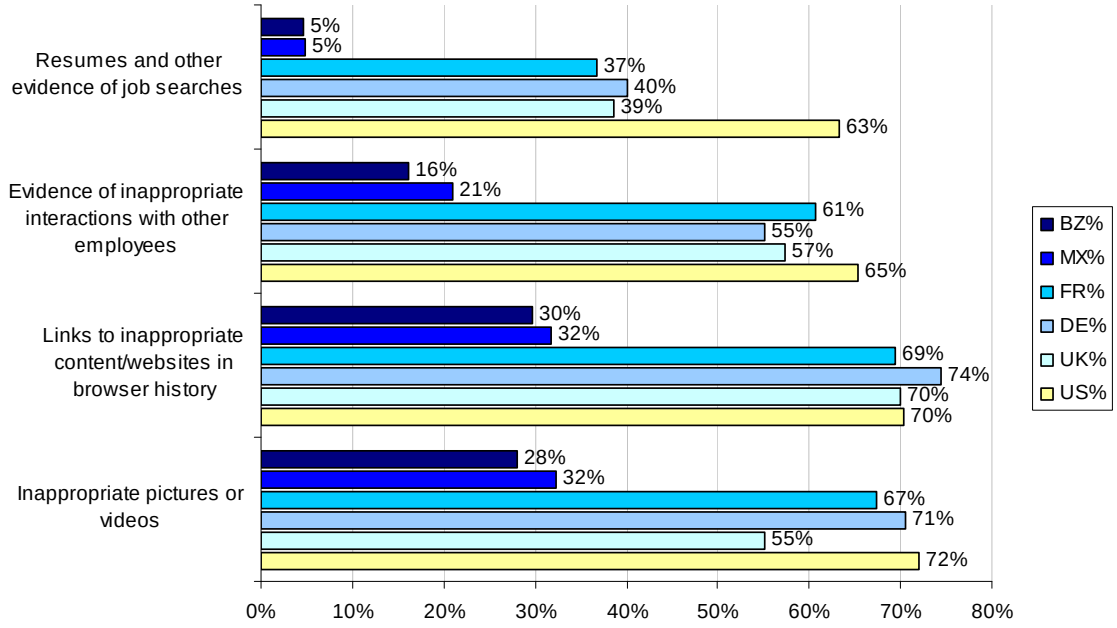


As shown in Bar Chart 11, respondents admit to discovering the following extremely sensitive personal content on employees' laptops that could put their company at risk. These discoveries include inappropriate pictures or videos, links to inappropriate content/websites in browser history and existence of inappropriate interactions with other employees.

In the US and Mexico the number one data discovery concerns inappropriate digital photos, followed by links to inappropriate content/websites in the browser history. In the UK, Germany, France and Brazil, the number one discovery is links to inappropriate content/websites. The UK ranks evidence of inappropriate interactions with other employees as the number two discovery.

Bar Chart 11

Did your company ever discover the following on an employee's laptop? Each bar shows the percentage Yes response.

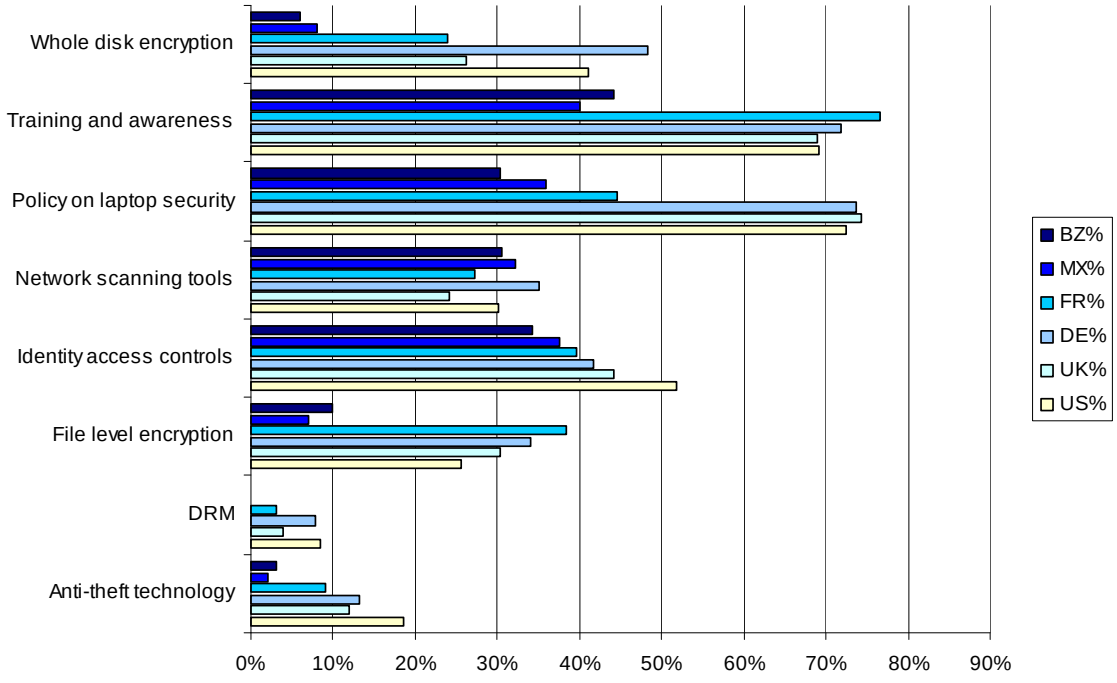


How to reduce the business risk of lost laptops

As shown in Bar Chart 12, respondents in the US, UK and Germany appear to focus on manual control steps including security policies and training and awareness programs for employees. In France, the top control method concerns training and awareness followed by policy. In Mexico, the number one method for reducing laptop loss is identity management and access controls followed by policy. In Brazil it is training followed by identity management and access controls. The most effective method used by their organizations to reduce the risk of lost or stolen laptops is whole disk encryption.

The US and Germany also believe anti-theft technologies are effective. France and the UK believe file or record level encryption is effective. Mexico and Brazil believe identity management and access controls are effective at reducing or mitigating the risk of laptop loss. Considered least effective by respondents in the US, UK, Germany and France are network scanning tools. In Mexico and Brazil it is policy focused on laptop security.

Bar Chart 12
Methods used to reduce the risk of laptop loss



Experts agree, however, that preventing employee-assigned laptops from being lost or stolen in the first place should be a priority. We recommend taking the following seven steps to prevent the business risk of lost laptops:

1. Conduct an audit to determine where laptops are used within the organization.

2. Determine whether specific employees need a laptop to do their jobs.

3. Classify data on the laptop according to organization guidelines.

4. Determine if data residing on each laptop is necessary for employees to complete their job.

5. Conduct a risk assessment to determine possible theft scenarios for the data stored, processed, or transmitted by laptop. Devise appropriate security measures to protect both the data and the laptop.

6. Implement the required protection strategies.

7. Create a lost response team to monitor laptops and data.

It is difficult to protect a laptop and its data. However, training employees on the importance of safeguarding their laptops, putting physical and electronic security measures in place and having a data recovery team available can do much to reduce the business risk of a lost laptop.

The data at risk

Table 1 shows an estimated amount of hard disk storage space occupied by data on the average laptop that is lost or stolen by companies in six countries. Accordingly, respondents in Germany report the highest percentage of occupied hard disk space (36.52 gigabytes) on lost laptops, followed by the United States (32.63 gigabytes). Respondents in Mexico report the lowest percentage of occupied hard disk space (7.99 gigabytes), followed by Brazil (10.82 gigabytes).

Table 1: Extrapolated value of data at risk	Average gigabytes of occupied space	Average number of lost laptops per company per year	Average number of companies in country	Extrapolated Terabytes of lost data
United States	32.63	27	28173	24,818
United Kingdom	29.44	14	13798	5,688
Germany	36.52	12	9712	4,256
France	25.64	19	11985	5,839
Mexico	7.99	8	8132	520
Brazil	10.82	13	8489	1,194
			Total	42,315

The average number of lost or stolen laptops for each company ranges from a high of 27 per year in the United Stage to a low of 8 laptops per year in Mexico. The adjacent column provides the approximate number of companies with more than 100 employees (as determined from national census statistics). Drawing upon national values, we extrapolate the terabytes (gigabytes X 1,000) of lost data as a consequence of lost or missing laptops. As shown, the total number of terabytes of lost data is 42,315 terabytes (or 42,314,640 gigabytes) for six countries each year.

Methods

Six national sampling frames involving more than 68,000 adult-aged individuals were used to recruit participants to this web survey.[1] Our randomly selected sampling frame was selected from panels containing contact information for practitioners who are employed in the information technology, data security, data protection or compliance fields, respectively. Table 2 summaries response rates for six separate national surveys – ranging from a high of 5.8% in Mexico to a low of 3.7% in Germany.

Table 2: Sample description	U.S.	U.K.	Germany	France	Mexico	Brazil
Total sampling frame	15993	11,302	14,950	8,901	8,186	9,095
Bounce-back	4025	2,082	1,387	1,034	1,987	1,995
Total returns	816	561	579	413	529	560
Rejected surveys	102	55	31	64	56	50
Final sample	714	506	548	349	473	510
Response rate	4.5%	4.5%	3.7%	3.9%	5.8%	5.6%

A total of 3,100 respondents successfully completed the survey results over a two week research ending in March 2009. Of returned instruments, 358 were rejected because of reliability tests. The margin of error on all adjective scale responses is $\leq$ 3 percent for all national samples.

Pie Chart 1 shows the distribution of respondents for all six countries combined by primary industry classifications. As shown, financial services and government represent the two largest industry segments (both at 13%).

[1] Respondents were given an identical survey instrument translated into the language of the respondent.

Pie Chart 1
Industry distribution of respondents for six countries combined

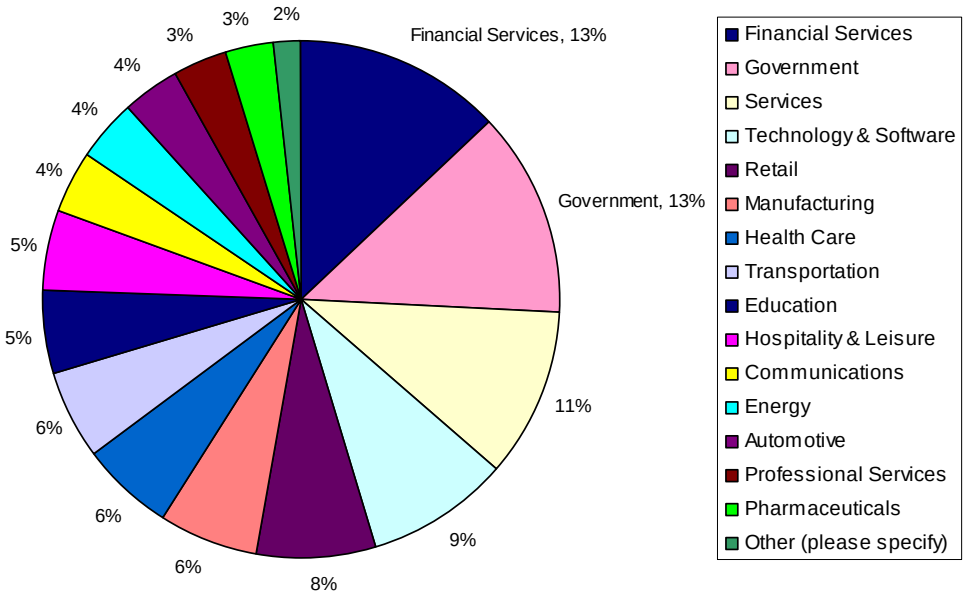


Table 3 reports the average experience levels of respondents in all six countries. Combining all national samples, respondents have an average of 9.8 years of overall experience and 7.8 in the IT, security or related fields. About 74% of respondents are males and 16% are females. While results are skewed on the gender variable (more male than female respondents), this result is consistent with known demographics about the IT field all six countries. The average time to complete the survey instrument was 14.9 minutes, and more than 95% of respondents completed the survey within 20 minutes.

Table 3: Mean experience levels	US	UK	DE	FR	MX	BZ
Overall business experience	9.55	10.10	9.99	11.66	8.74	8.88
In the IT or security field	7.48	7.49	9.63	8.28	8.41	7.75
In current position	3.09	5.82	2.81	7.30	3.53	2.47

Table 4 summarizes the self-reported organizational level of respondents in all six countries. The majority of respondents are at the manager (14%), supervisor (18%), associate/staff (18%) or technician (31%) levels, respectfully. Over 8% are at or above the director level.

Table 4: Organizational levels	US%	UK%	DE%	FR%	MX%	BZ%
Senior Executive	0%	0%	0%	0%	0%	0%
Vice President	1%	0%	1%	1%	0%	0%
Director	9%	3%	8%	4%	10%	9%
Manager	20%	12%	11%	10%	15%	20%
Supervisor	19%	20%	19%	15%	19%	17%
Associate/Staff	19%	16%	19%	17%	22%	19%
Technician	26%	37%	28%	44%	26%	24%
Consultant	4%	4%	5%	5%	4%	4%
Other	2%	9%	8%	3%	5%	7%
Total	100%	100%	100%	100%	100%	100%

Table 5 provides the approximate headcounts of participating organizations. As can be seen, a majority of respondents work for larger-sized companies with more than 1,000 employees. Over 8% of US respondents work in the largest-sized organizations (more than 75,000 employees).

Table 5 Approximate worldwide headcount for participants' organizations	US%	UK%	DE%	FR%	MX%	BZ%
Less than 500 people	13%	21%	13%	22%	15%	13%
500 to 1,000 people	12%	12%	12%	12%	12%	11%
1,001 to 5,000 people	15%	11%	11%	12%	26%	26%
5,001 to 10,000 people	17%	15%	28%	19%	17%	16%
10,001 to 25,000 people	20%	20%	19%	17%	12%	19%
25,001 to 50,000 people	10%	12%	10%	10%	11%	9%
50,001 to 75,000 people	5%	7%	5%	5%	8%	5%
More than 75,000 people	8%	2%	2%	3%	0%	1%
Total	100%	100%	100%	100%	100%	100%

Caveats to this survey

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 information technology 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.

The following Appendix provides all survey results in percentage frequency tables.

Appendix: Response to Survey Items

Survey fieldwork completed on March 19, 2009

Following are the percentage frequency responses to all survey items in six countries. The country legend is defined as: US = United States, UK = United Kingdom, FR = France, DE = Germany, MX = Mexico and BZ = Brazil.

Q1. Current Title (Top 5 choices)	US%	UK%	DE%	FR%	MX%	BZ%
Information security	24%	17%	25%	13%	10%	11%
Operations	21%	41%	39%	38%	48%	41%
Network management	18%	8%	10%	11%	8%	8%
Application development	10%	7%	9%	14%	8%	12%
Data protection	8%	6%	4%	5%	7%	7%
Data quality & compliance	8%	8%	11%	6%	7%	9%
Other	11%	13%	3%	12%	13%	12%
Total	100%	100%	100%	100%	100%	100%

Q2. What organizational level best describes your current position?	US%	UK%	DE%	FR%	MX%	BZ%
Senior Executive	0%	0%	0%	0%	0%	0%
Vice President	1%	0%	1%	1%	0%	0%
Director	9%	3%	8%	4%	10%	9%
Manager	20%	12%	11%	10%	15%	20%
Supervisor	19%	20%	19%	15%	19%	17%
Associate/Staff	19%	16%	19%	17%	22%	19%
Technician	26%	37%	28%	44%	26%	24%
Consultant	4%	4%	5%	5%	4%	4%
Other	2%	9%	8%	3%	5%	7%
Total	100%	100%	100%	100%	100%	100%

Q3. Check the **Primary Person** you or your manager reports to within your organization.	US%	UK%	DE%	FR%	MX%	BZ%
CEO/Executive Committee	0%	0%	0%	0%	0%	0%
Chief Financial Officer	4%	4%	5%	6%	6%	3%
Chief Information Officer	41%	41%	47%	51%	46%	42%
Chief Technology Officer	14%	14%	15%	14%	14%	17%
Chief Risk Officer	5%	7%	2%	0%	2%	5%
Chief Security Officer	6%	4%	5%	2%	5%	6%
Compliance Officer	10%	9%	4%	9%	6%	6%
General Counsel	3%	3%	2%	1%	4%	1%
Human Resources	2%	4%	2%	3%	2%	2%
Director of IT Security	13%	13%	13%	11%	10%	9%
Other	2%	1%	6%	3%	6%	10%
Total	100%	100%	100%	100%	100%	100%

Q4. Check the **Secondary Person** you or your manager reports to within your organization. Leave blank if not applicable.	US%	UK%	DE%	FR%	MX%	BZ%
CEO/Executive Committee	0%	0%	0%	0%	0%	0%
Chief Financial Officer	6%	6%	9%	6%	7%	7%
Chief Information Officer	24%	23%	24%	29%	32%	33%
Chief Technology Officer	18%	14%	11%	15%	17%	16%
Chief Risk Officer	1%	0%	0%	1%	0%	1%
Chief Security Officer	4%	8%	6%	2%	6%	7%
Compliance Officer	14%	8%	4%	5%	10%	13%
General Counsel	0%	0%	0%	1%	3%	2%
Human Resources	0%	0%	0%	2%	8%	7%
Director of IT Security	23%	21%	12%	8%	6%	6%
Other	10%	20%	34%	30%	11%	8%
Total	100%	100%	100%	100%	100%	100%
Blank	509	303	289	250	295	381
Percent blank (no secondary reporting relationship)	71%	60%	53%	72%	62%	75%

Experience level	US	UK	DE	FR	MX	BZ
Q5a. Years of business experience	9.55	10.10	9.99	11.66	8.74	8.88
Q5b. Years in the IT or security field	7.48	7.49	9.63	8.28	8.41	7.75
Q5c. Years in current position	3.09	5.82	2.81	7.30	3.53	2.47

Q6. Gender	US%	UK%	DE%	FR%	MX%	BZ%
Female	38%	28%	34%	25%	12%	16%
Male	62%	72%	66%	75%	88%	84%
Total	100%	100%	100%	100%	100%	100%

Q7. Do you occupy a full time position?	US%	UK%	DE%	FR%	MX%	BZ%
Yes	88%	91%	94%	86%	87%	83%
No	12%	9%	6%	14%	13%	17%
Total	100%	100%	100%	100%	100%	100%

Q8. In which regions does your organization operate? Please check all that apply.	US%	UK%	DE%	FR%	MX%	BZ%
United States	98%	62%	72%	62%	83%	66%
Canada	53%	56%	59%	42%	40%	21%
Europe	57%	100%	100%	100%	21%	50%
Middle East	18%	40%	33%	58%	28%	28%
Latin America (including Mexico)	35%	14%	9%	13%	100%	100%
Asia	44%	48%	50%	38%	26%	34%
Africa	6%	18%	16%	17%	3%	4%
Australia & New Zealand	25%	26%	7%	11%	3%	1%

Q9. What is the industry or business group that best defines your organization? If your organization contains multiple industry sectors or sub-sectors, please check all that apply (or write-in the space for other).	US%	UK%	DE%	FR%	MX%	BZ%
Automotive	2%	1%	7%	5%	2%	4%
Education	4%	5%	9%	8%	2%	4%
Financial Services	18%	18%	12%	12%	8%	10%
Government	14%	17%	15%	13%	9%	10%
Health Care	7%	4%	5%	6%	8%	6%
Hospitality & Leisure	4%	2%	5%	2%	7%	9%
Manufacturing	5%	5%	6%	8%	7%	5%
Transportation	5%	5%	5%	2%	8%	9%
Pharmaceuticals	1%	4%	4%	4%	3%	3%
Professional Services	3%	2%	6%	3%	3%	3%
Retail	8%	7%	8%	11%	5%	6%
Services	11%	9%	6%	11%	14%	12%
Communications	4%	4%	7%	5%	3%	1%
Technology & Software	12%	11%	5%	7%	9%	8%
Energy	1%	5%	1%	4%	8%	5%
Other (please specify)	1%	0%	1%	0%	5%	4%
Total	100%	100%	100%	100%	100%	100%

Q10. What is the headcount of your IT organization?	US%	UK%	DE%	FR%	MX%	BZ%
Less than 100 people	13%	22%	12%	20%	22%	23%
101 to 500 people	9%	10%	9%	9%	8%	10%
501 to 1,000 people	22%	31%	26%	24%	30%	32%
1,001 to 5,000 people	24%	20%	21%	30%	24%	25%
5,001 to 10,000 people	25%	17%	24%	17%	12%	10%
More than 10,000 people	6%	0%	7%	2%	4%	1%
Total	100%	100%	100%	100%	100%	100%

Q11. What is the worldwide headcount of your organization?	US%	UK%	DE%	FR%	MX%	BZ%
Less than 500 people	13%	21%	13%	22%	15%	13%
500 to 1,000 people	12%	12%	12%	12%	12%	11%
1,001 to 5,000 people	15%	11%	11%	12%	26%	26%
5,001 to 10,000 people	17%	15%	28%	19%	17%	16%
10,001 to 25,000 people	20%	20%	19%	17%	12%	19%
25,001 to 50,000 people	10%	12%	10%	10%	11%	9%
50,001 to 75,000 people	5%	7%	5%	5%	8%	5%
More than 75,000 people	8%	2%	2%	3%	0%	1%
Total	100%	100%	100%	100%	100%	100%

Q12. What percentage of your company's employees are given a laptop computer for business use?	US%	UK%	DE%	FR%	MX%	BZ%
Less than 10%	16%	15%	15%	17%	22%	21%
11 to 20%	34%	40%	35%	39%	34%	38%
21 to 30%	13%	14%	12%	14%	13%	12%
31 to 40%	15%	14%	15%	14%	14%	14%
41 to 50%	6%	5%	6%	5%	7%	7%
51 to 60%	0%	1%	0%	0%	2%	0%
61 to 70%	1%	1%	2%	2%	3%	2%
71 to 80%	3%	4%	2%	3%	3%	3%
81 to 90%	2%	2%	1%	2%	2%	2%
More than 90%	10%	5%	13%	3%	0%	0%
Total	100%	100%	100%	100%	100%	100%
Average percentage	31%	27%	33%	26%	25%	23%

Q13. Five years from now, approximately what percentage of your company's employees will be given a laptop computer for business use?	US%	UK%	DE%	FR%	MX%	BZ%
Less than 10%	2%	4%	2%	3%	6%	2%
11 to 20%	4%	7%	5%	4%	11%	10%
21 to 30%	3%	2%	2%	5%	3%	3%
31 to 40%	8%	10%	8%	8%	8%	9%
41 to 50%	15%	16%	15%	16%	16%	16%
51 to 60%	11%	11%	11%	11%	10%	11%
61 to 70%	12%	13%	12%	10%	13%	10%
71 to 80%	13%	13%	13%	12%	12%	15%
81 to 90%	9%	10%	10%	8%	8%	10%
More than 90%	23%	16%	24%	23%	13%	15%
Total	100%	100%	100%	100%	100%	100%
Average percentage	64%	60%	65%	62%	55%	59%

Q14.On average, what is the hard disk capacity or size provided on employee-assigned laptops?	US%	UK%	DE%	FR%	MX%	BZ%
No hard disk (dumb terminals)	6%	3%	0%	2%	8%	6%
Less than 5 GB	2%	0%	1%	3%	13%	14%
5 to 10GB	6%	8%	7%	8%	33%	27%
11 to 50GB	19%	32%	24%	33%	30%	40%
51 to 100 GB	27%	27%	34%	26%	9%	6%
101 to 250GB	26%	15%	17%	16%	5%	3%
251 to 500GB	6%	7%	6%	6%	0%	1%
500GB to 1TB	6%	7%	5%	6%	1%	2%
Greater than 1TB	2%	1%	5%	0%	0%	0%
Total	100%	100%	100%	100%	100%	100%
Average hard disk storage size (GB)	165	144	179	126	37	48

Q15. What are the main reasons for assigning employees a laptop computer for business use? Please check all that apply.	US%	UK%	DE%	FR%	MX%	BZ%
Cost savings	39%	19%	19%	14%	24%	29%
Productivity	69%	57%	47%	64%	77%	79%
Mobility	73%	63%	84%	74%	84%	86%
Employee benefits	18%	10%	2%	9%	20%	21%
Security	9%	7%	49%	18%	10%	10%
Other	1%	2%	0%	1%	1%	1%
Total	208%	158%	201%	181%	216%	226%

Q16a. In your organization, **who is** responsible for ensuring laptop computers are safe and secure? Please check only one.	US%	UK%	DE%	FR%	MX%	BZ%
No one person has this responsibility	24%	13%	4%	11%	9%	4%
Business unit or departmental management	24%	27%	18%	19%	10%	11%
CISO/CSO	3%	2%	3%	4%	5%	4%
Chief Risk Officer	1%	2%	1%	2%	0%	0%
Chief Financial Officer	2%	2%	3%	2%	1%	0%
Chief Information Officer	25%	35%	41%	39%	54%	61%
Chief Technology Officer	10%	10%	14%	9%	13%	15%
Chief Privacy Officer	0%	0%	0%	0%	0%	0%
Compliance Officer	1%	2%	5%	5%	0%	1%
General Counsel	6%	5%	1%	2%	1%	0%
Human Resources	4%	2%	10%	1%	2%	1%
Other (please specify)	0%	0%	0%	6%	5%	3%
Total	100%	100%	100%	100%	100%	100%

Q16b. In your organization, **who should be** responsible for ensuring laptop computers are safe and secure? Please check the one best choice.	US%	UK%	DE%	FR%	MX%	BZ%
Business unit or departmental management	41%	31%	32%	15%	35%	32%
CISO/CSO	16%	13%	12%	14%	9%	11%
Chief Risk Officer	0%	1%	1%	0%	0%	0%
Chief Financial Officer	0%	4%	12%	9%	12%	11%
Chief Information Officer	10%	11%	14%	17%	16%	20%
Chief Technology Officer	3%	10%	9%	9%	8%	8%
Chief Privacy Officer	3%	1%	1%	0%	0%	0%
Compliance Officer	10%	15%	4%	19%	3%	3%
General Counsel	4%	1%	1%	0%	0%	0%
Human Resources	14%	13%	14%	14%	16%	15%
Other (please specify)	0%	0%	0%	2%	1%	0%
Total	100%	100%	100%	100%	100%	100%

Q17. Please rank the threat of a lost or stolen laptop with other known IT security threats that may be present within your organization. Place a 1 to denote the highest risk level and 9 to denote the lowest risk level. **The combined percentage of 1 and 2 (highest risk levels.**	US%	UK%	DE%	FR%	MX%	BZ%
Business process failures	65%	63%	47%	47%	35%	34%
Technology glitches	59%	48%	50%	55%	54%	48%
Lost or stolen laptops	53%	43%	33%	35%	35%	36%
Cyber crime	52%	48%	55%	42%	48%	51%
Malicious employees	39%	23%	17%	14%	63%	69%
Outsourcing to undependable vendors	36%	26%	31%	9%	5%	5%
Virus or malware infections	32%	32%	46%	28%	59%	54%
Missed or failed security patches	24%	24%	7%	21%	31%	39%
Social engineering	8%	4%	3%	7%	4%	1%
Average	41%	35%	32%	29%	37%	37%

Q18. In your organization, which is more valuable?	US%	UK%	DE%	FR%	MX%	BZ%
The replacement value of a lost laptop computer	34%	48%	13%	41%	39%	43%
The data or information residing on the lost laptop computer	51%	41%	61%	39%	40%	47%
Both are of equal value	15%	11%	26%	20%	21%	10%
Total	100%	100%	100%	100%	100%	100%

Q19. Which types of information present the greatest risk when a laptop computer is lost or stolen? Please select only two choices.	US%	UK%	DE%	FR%	MX%	BZ%
Customer information (such as contact lists)	56%	50%	30%	35%	15%	14%
Employee information	48%	46%	63%	60%	26%	30%
Non-financial confidential information	29%	31%	14%	23%	35%	36%
Financial confidential information	27%	29%	35%	32%	41%	39%
Software programs, tools, applications and source code	13%	14%	51%	23%	32%	31%
Other intellectual properties	23%	24%	54%	22%	33%	26%
Total	196%	194%	247%	196%	181%	177%

Q20. What percentage of your company's confidential data is accessed at any given time by remote workers, contractors or other third parties?	US%	UK%	DE%	FR%	MX%	BZ%
Less than 5%	3%	1%	4%	2%	1%	1%
Between 5 and 10%	5%	17%	18%	5%	3%	2%
Between 11 and 20%	9%	23%	27%	10%	4%	2%
Between 21 and 30%	8%	18%	21%	10%	3%	4%
Between 31 and 40%	27%	13%	8%	29%	10%	7%
Between 41 and 50%	24%	12%	6%	23%	16%	14%
Between 51 and 60%	7%	8%	7%	7%	46%	41%
Between 61 and 70%	7%	5%	8%	6%	5%	6%
Between 71 and 80%	1%	0%	0%	0%	0%	1%
Between 81 and 90%	0%	2%	0%	0%	0%	0%
More than 90%	9%	0%	1%	8%	12%	22%
Total	100%	100%	100%	100%	100%	100%

Q21. Approximately, how many cyber crime attacks did your organization have over the past year that resulted in economic loss including the disruption of service?	US%	UK%	DE%	FR%	MX%	BZ%
None	15%	19%	9%	11%	13%	12%
Less than 10	9%	24%	18%	38%	15%	18%
Between 11 to 100	24%	15%	18%	7%	12%	8%
Between 101 to 1,000	18%	15%	35%	2%	10%	13%
Between 1001 to 5,000	9%	4%	14%	2%	3%	2%
Over 5,000	1%	2%	2%	8%	5%	4%
Don't know	24%	22%	4%	31%	42%	43%
Total	100%	100%	100%	100%	100%	100%

22a. Approximately, how many laptops were lost or stolen in the past year within your organization (entire enterprise),:	US%	UK%	DE%	FR%	MX%	BZ%
None	8%	16%	20%	10%	9%	11%
Less than 10	11%	16%	23%	16%	11%	7%
Between 11 to 20	23%	14%	28%	21%	18%	18%
Between 21 to 50	16%	18%	13%	13%	17%	22%
Between 51 to 100	6%	2%	11%	3%	0%	1%
Between 101 to 200	2%	0%	2%	1%	0%	0%
Between 201 to 500	1%	1%	0%	0%	1%	0%
More than 500	1%	0%	0%	0%	0%	0%
Don't know	31%	34%	3%	36%	44%	41%
Total	100%	100%	100%	100%	100%	100%

22b. Approximately, how many laptops were lost or stolen in the past year as the **percentage** of total laptops in use within your organization:	US%	UK%	DE%	FR%	MX%	BZ%
Zero%	8%	16%	21%	9%	9%	10%
1 to 5%	76%	83%	73%	84%	71%	70%
6 to 10%	14%	1%	6%	7%	10%	17%
11 to 20%	2%	0%	0%	0%	1%	2%
21 to 30%	0%	0%	0%	0%	0%	1%
31 to 40%	0%	0%	0%	0%	0%	0%
41 to 50%	0%	0%	0%	0%	0%	0%
More than 50%	0%	0%	0%	0%	10%	0%
Total	100%	100%	100%	100%	100%	100%

Q23. Are you aware that there are security features designed in laptop hardware that can prevent cyber crime or other malicious attacks?	US%	UK%	DE%	FR%	MX%	BZ%
Yes	61%	54%	78%	60%	39%	52%
No	39%	46%	22%	40%	61%	48%
Total	100%	100%	100%	100%	100%	100%

Q24. How has the number of laptop losses changed from prior years?	US%	UK%	DE%	FR%	MX%	BZ%
Increasing	65%	68%	64%	56%	63%	69%
Staying the same	21%	22%	26%	37%	23%	26%
Decreasing	7%	3%	11%	3%	10%	2%
Unsure	7%	6%	0%	4%	4%	3%
Total	100%	100%	100%	100%	100%	100%

Q25. What are the most common locations where employees lose their laptop computers? Please check the top three choices.	US%	UK%	DE%	FR%	MX%	BZ%
Airports	53%	50%	40%	41%	5%	6%
Taxi cabs	14%	8%	14%	7%	0%	2%
Trains or subways	14%	16%	12%	13%	3%	3%
Rental cars	48%	57%	58%	51%	2%	1%
Hotels	56%	58%	56%	57%	54%	55%
Conferences and other events	38%	39%	47%	43%	6%	2%
Client or customer offices	10%	10%	7%	5%	0%	1%
Home locations	22%	25%	25%	20%	52%	47%
Other (please specify)	6%	10%	11%	12%	11%	10%
Total	261%	274%	269%	250%	133%	127%

Q26. If your organization had a lost or stolen laptop computer, which of the following possible consequences would have the most negative impact? Please check one.	US%	UK%	DE%	FR%	MX%	BZ%
Regulatory action	11%	21%	10%	19%	1%	4%
Negative media and brand damage	19%	17%	18%	18%	16%	17%
Business interruption	16%	14%	25%	21%	40%	32%
Costly remediation efforts	9%	9%	8%	8%	9%	9%
Costly notification efforts	15%	6%	7%	1%	0%	1%
Loss of trust by consumers and other stakeholders	31%	32%	32%	32%	33%	34%
Other (please specify)	0%	0%	0%	1%	0%	3%
Total	100%	100%	100%	100%	100%	100%

Q27. Do you know of an incident in your organization where confidential or sensitive information was at risk as a result of a lost or stolen laptop computer?	US%	UK%	DE%	FR%	MX%	BZ%
Yes	75%	70%	65%	61%	59%	54%
No	25%	30%	35%	39%	41%	46%
Total	100%	100%	100%	100%	100%	100%

Q28a. What is the most common cause of physical damage to laptop computers that resulted in data loss within your organization? Please select only one.	US%	UK%	DE%	FR%	MX%	BZ%
Spilling food or liquids on the laptop	34%	13%	11%	36%	18%	29%
Dropping the laptop accidentally	28%	22%	19%	17%	30%	30%
Not protecting the laptop when traveling	25%	52%	48%	23%	11%	9%
Employee inflicted damage because of anger or frustration	13%	6%	21%	19%	35%	31%
Other (please specify)	0%	8%	1%	5%	7%	1%
Total	100%	100%	100%	100%	100%	100%

Q28b. Did you ever lose data because of physical damage to your computer?	US%	UK%	DE%	FR%	MX%	BZ%
Yes	52%	45%	33%	55%	59%	58%
No	48%	55%	67%	45%	41%	42%
Total	100%	100%	100%	100%	100%	100%

Q28c. Approximately what percentage of damaged laptop computers within your organization is due to employee inflicted damage because of anger or frustration over technical issues?	US%	UK%	DE%	FR%	MX%	BZ%
Less than 5%	13%	22%	13%	17%	5%	3%
Between 5 and 10%	24%	33%	21%	20%	23%	19%
Between 11 and 20%	30%	28%	21%	30%	22%	29%
Between 21 and 30%	17%	7%	16%	11%	28%	29%
Between 31 and 40%	8%	11%	22%	16%	21%	17%
Between 41 and 50%	4%	0%	7%	7%	2%	2%
Between 51 and 60%	5%	0%	0%	0%	0%	0%
Between 61 and 70%	0%	0%	0%	0%	0%	0%
Between 71 and 80%	0%	0%	0%	0%	0%	0%
Between 81 and 90%	0%	0%	0%	0%	0%	0%
More than 90%	0%	0%	0%	0%	0%	0%
Total	100%	100%	100%	100%	100%	100%

How likely would it be for the following situations to occur in your organization?

Q29a. Employee, temporary employee or contractor loses a laptop computer.	US%	UK%	DE%	FR%	MX%	BZ%
Very frequent	8%	4%	2%	6%	2%	2%
Frequent	20%	21%	20%	19%	16%	14%
Not frequent	50%	50%	53%	52%	49%	44%
Rarely	14%	10%	20%	16%	16%	16%
Never happens	7%	15%	5%	7%	17%	25%
Total	100%	100%	100%	100%	100%	100%

Q29b. Employee, temporary employee or contractor puts the organization's confidential data at risk?	US%	UK%	DE%	FR%	MX%	BZ%
Very frequent	17%	24%	21%	18%	20%	23%
Frequent	54%	48%	40%	35%	21%	23%
Not frequent	19%	17%	17%	15%	14%	13%
Rarely	9%	3%	19%	18%	34%	35%
Never happens	1%	8%	2%	14%	10%	5%
Total	100%	100%	100%	100%	100%	100%

Q30. What are the greatest threats caused by employees to your organization's confidential data? Please select the top two threats.	US%	UK%	DE%	FR%	MX%	BZ%
Failing to use proper authentication or passwords	41%	41%	34%	49%	60%	63%
Not protecting laptops when traveling	36%	37%	31%	35%	11%	13%
Transferring files on USB memory sticks	27%	27%	26%	27%	23%	29%
Downloading free apps or widgets with embedded malware	24%	27%	19%	19%	2%	4%
Not shredding paper documents containing confidential information	22%	17%	14%	17%	43%	48%
Sharing passwords	18%	22%	8%	19%	30%	27%
Downloading Internet apps with P2P file sharing	17%	17%	20%	13%	2%	0%
Turning off security applications	13%	12%	6%	17%	1%	1%
Other (please specify)	1%	4%	1%	2%	1%	0%
Total	198%	204%	159%	199%	173%	186%

Q31.What method does your organization use to reduce the risk of lost or stolen laptop computers? Please check all methods deployed today.	US%	UK%	DE%	FR%	MX%	BZ%
Policy focused on laptop security	72%	74%	74%	45%	36%	30%
Training and awareness for employees focused on laptop security	69%	69%	72%	77%	40%	44%
Identity management and access controls	52%	44%	42%	40%	38%	34%
Whole disk encryption	41%	26%	48%	24%	8%	6%
Network device scanning tools	30%	24%	35%	27%	32%	31%
File or record level encryption	26%	30%	34%	38%	7%	10%
Anti-theft technologies such as location tracking	19%	12%	13%	9%	2%	3%
Digital rights management	9%	4%	8%	3%	0%	0%
Total	317%	306%	304%	306%	293%	281%

Q32. Please rate the effectiveness of the methods used by your organization to reduce the risk of lost or stolen laptop computers. Please use the following scale for each item selected in Q31 above. 1= Very effective, 2= Effective, 3= Sometimes effective, 4 = Rarely effective, 5 = Not effective. **The combined percentage of very effective (1) + effective (2)**	US%	UK%	DE%	FR%	MX%	BZ%
Anti-theft technologies such as location tracking	56%	31%	54%	26%	15%	20%
Whole disk encryption	58%	56%	60%	59%	58%	57%
File or record level encryption	50%	47%	47%	46%	25%	24%
Digital rights management	35%	29%	24%	20%	0%	0%
Network device scanning tools	17%	12%	17%	14%	15%	14%
Identity management and access controls	25%	17%	29%	22%	41%	43%
Training and awareness for employees focused on laptop security	31%	35%	29%	24%	25%	16%
Policy focused on laptop security	41%	38%	41%	32%	2%	6%
Average	39%	33%	37%	30%	23%	23%

Q33a. In your opinion, the risk of having lost or stolen laptop computers will:	US%	UK%	DE%	FR%	MX%	BZ%
Increase over the next 12 to 24 months	41%	35%	51%	45%	42%	38%
Stay the same over the next 12 to 24 months	38%	42%	31%	35%	43%	49%
Decrease over the next 12 to 24 months	22%	23%	19%	20%	15%	12%
Total	100%	100%	100%	100%	100%	100%

Q33b. If the risk **increases or stays the same**, why? Check all that apply.	US%	UK%	DE%	FR%	MX%	BZ%
Lack of support from senior management	42%	42%	40%	47%	13%	11%
Poor coordination of threat management	33%	41%	46%	45%	34%	29%
Ineffective security leadership	45%	49%	43%	51%	19%	9%
Insufficient resources to enforce compliance	57%	59%	30%	32%	52%	47%
Lack of suitable technology solutions	41%	27%	21%	33%	61%	65%
Other (please specify)	2%	0%	0%	2%	1%	1%
Total	221%	218%	181%	209%	180%	162%

Q33c. If the risk **decreases**, why? Check all that apply.	US%	UK%	DE%	FR%	MX%	BZ%
Support from senior management	8%	11%	9%	5%	7%	5%
Coordination of threat management	42%	40%	41%	39%	34%	35%
Effective security leadership	50%	48%	46%	46%	51%	51%
Sufficient resources to enforce compliance	66%	72%	72%	62%	68%	71%
Suitable technology solutions	61%	57%	40%	46%	81%	77%
Other (please specify)	0%	0%	0%	1%	0%	0%
Total	228%	229%	209%	199%	241%	240%

Q35. Did you ever discover the following on an employee's laptop?	US% = Yes	UK% = Yes	DE% = Yes	FR% = Yes	MX% = Yes	BZ% = Yes
Inappropriate pictures or videos	72%	55%	71%	67%	32%	28%
Links to inappropriate content/websites in browser history	70%	70%	74%	69%	32%	30%
Evidence of inappropriate interactions with other employees	65%	57%	55%	61%	21%	16%
Resumes and other evidence of job searches	63%	39%	40%	37%	5%	5%
Average	68%	55%	60%	59%	22%	20%

Q36. In general, what are the greatest threats to your organization's information security? Please select the top three.	US%	UK%	DE%	FR%	MX%	BZ%
Attack on network/firewall	32%	30%	30%	35%	40%	37%
A data security breach involving a remote end-user device not protected by the corporate firewall	78%	79%	82%	79%	20%	18%
Third parties and contractors with unauthorized access to your network	67%	66%	73%	73%	4%	7%
Information not properly backed up	40%	39%	48%	47%	44%	43%
Inability to properly identify and authenticate users to your organization's multiple systems	56%	53%	57%	54%	65%	67%
Total	272%	267%	290%	288%	293%	288%

Q37a. In your opinion, which age group is **more likely** to practice safe security and follow your organization's data security policies and procedures the best?	US%	UK%	DE%	FR%	MX%	BZ%
Employees younger than 25	3%	2%	12%	2%	31%	34%
Employees between the ages of 26 and 35	30%	29%	22%	14%	35%	33%
Employees between the ages of 36 and 45	24%	36%	32%	41%	21%	27%
Employees 46 and older	43%	34%	34%	44%	13%	6%
Total	100%	100%	100%	100%	100%	100%

Q37b. Which of the following is the primary reason this age group is best at practicing safe data security? Please select the top two reasons.	US%	UK%	DE%	FR%	MX%	BZ%
This age group is more knowledgeable about how to protect their organization's information security	22%	16%	19%	22%	54%	62%
This age group understands best how a data breach can adversely affect their organization	43%	41%	34%	31%	36%	34%
This age group believes practicing safe security is an important part of their job	60%	60%	66%	68%	37%	35%
They do not understand how to circumvent data security procedures	33%	36%	67%	52%	3%	3%
Total	158%	152%	185%	173%	131%	134%

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49686
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.