Business Risk of a Lost Laptop
A Study of U.S. IT Practitioners

Sponsored by

Dell Corporation

Independently conducted by Ponemon Institute LLC

Publication Date: April 2009

Business Risk of a Lost Laptop

A Study of U.S. IT Practitioners

Presented by Dr. Larry Ponemon, April 2009

Executive Summary

When companies provide their employees with laptops for purposes of greater productivity and mobility, they are also handing them the proverbial keys to the corporate information kingdom. Employees, temporary employees and contractors can potentially access and store enormous amounts of confidential data about customers, employees and intellectual property on their laptops anytime and anywhere.

Sponsored by Dell, Ponemon Institute independently conducted this national study entitled, *The Business Risk of a Lost Laptop* to understand the implications to organizations when employees' laptops are missing. The number of laptop computers companies are assigning to employees is increasing and, in the opinion of participants, so is the likelihood that more laptops will be lost or stolen. But it is not the replacement value of the missing laptop that is of most concern to those in our study. According to 51% of respondents it is the confidential information residing on the lost laptop that has them most worried.

We conducted a Web-based survey involving 714 IT and IT security practitioners with an average of almost 7.5 years of domain-specific experience. The overall demographics for respondents are summarized at the conclusion of this report. The most salient findings are presented below.

Why is it important to understand the business risk of lost or missing laptops?

The following findings illustrate some of the reasons why employees' laptops are at risk and why this is a serious issue for most business and governmental organizations.

- The percentage of employees being given laptops is growing. The question is: are organizations taking the necessary steps to make sure the growing number of laptops and the data contained on those laptops are secure?

- The hard disk capacity of these laptops is significant and enables employees, temporary employees and contractors to store a large amount of sensitive and confidential data about customers, employees, temporary employees and contractors.

- Many organizations admit that no one person is accountable for securing laptops. More than 41% believe that accountability should be with the business unit or departmental management.

- More than 31% do not know how many laptops were missing or stolen during the past year. As a result, organizations do not have a clear understanding of the potential risk of a data breach and how to prevent the breach.

- Most respondents (65%) report that the number of lost or stolen laptops has increased from prior years and only 7% say that laptop losses appear to be decreasing.

- Most respondents (75%) are aware of an incident in their organization where confidential or sensitive information was at risk as a result of a lost or stolen laptop computer.

What is the business risk of lost or missing laptops?

According to the findings below, IT practitioners in our study understand the risk of lost or stolen laptops to data security. They seem to be most concerned about how their company's reputation may be adversely affected if the lost laptop results in a data breach requiring public notice to victims.

- More than 41% believe that the risk of having lost or stolen laptops will increase over the next 12 to 24 months, and the main reasons are insufficient resources to enforce compliance and ineffective security leadership.

- More than half (51%), believe the data or information residing on the lost laptop is more valuable than the replacement value of the computer itself. The information that presents the greatest risk when a laptop computer is lost or stolen includes customer information (such as contact lists), employee information and non-financial confidential information.

- Almost one-third of participants (31%) say that they don't know how many laptops were lost or stolen in the past year within their organization. More than 49% of respondents say that their organizations experienced more than 10 lost or stolen laptops over the past year.

- The most vulnerable time to lose a laptop is during travel. Participants report that the most common locations where employees lose their laptops are: hotels, airports, rental cars and at conferences.

- IT practitioners worry most about loss of trust by consumers and other stakeholders followed by negative media and brand damage if a laptop is lost or missing. While important, regulatory action and costly remediation efforts are less of a concern than reputation diminishment.

In addition to lost laptops, what are the most significant threats to data security?

According to participants, lost or stolen laptops are the third greatest threat to data security in their organizations. The first two are business process failures and technology glitches. Cyber crime and malicious employees are also significant threats. The following are more interesting findings:

- About 52% of respondents report their organization had more than 10 cyber crime attacks over the past year that sought to bring economic harm, including the disruption of service. Another 24% were unable to estimate the number of cyber crimes actually encountered.

- About 75% of respondents say more than 30% of their organization's sensitive or confidential information is being accessed at any given time by remote workers, contractors or third parties.

- The greatest threats to their organization's information security are a data breach involving a remote end-user device not protected by the corporate firewall (78%) followed by third parties and contractors with unauthorized access to their network (67%) followed by the inability to properly identify and authenticate users to the organization's multiple systems (56%).

Does the human factor put laptops and data at risk?

Employees are often careless or circumvent security procedures and as a result confidential and sensitive data can be at great risks. The findings below describe how the human factor affects the security of laptops:

- While only 28% believe that it is likely that employees, temporary employees or contractors will lose a laptop, 71% believe that these individuals put an organization’s confidential data at risk very frequently and frequently.

- Physical damage also poses a risk to data. According to IT practitioners in our study, 34% report that employee spilled food or liquids on the laptop and 28% report it is dropping the laptop accidentally that are the two most common damages inflicted by employees. However, only 13% say that physical damage is due to an employee’s anger or frustration.

- More than half (52%) of the IT practitioners in our study admit to losing data because of damage to their computers.

- The greatest threats caused by employees include failing to use proper authentication or passwords, not protecting laptops when traveling and transferring files on USB memory sticks.

- IT practitioners admit to discovering the following content on employees’ laptops that could put the company at risk. These are: inappropriate pictures or videos, links to inappropriate content/websites in browser history and existence of inappropriate interactions with other employees.

- Older employees are more security conscious. According to most of the IT practitioners (67%), employees who are 36 and older are more likely to practice safe security and follow their organization’s security procedures and policies best. The main reason is that this age group believes practicing safe security is an important part of their job.

What can organizations do to reduce the business risk of a lost or missing laptop?

Security features are designed in laptop hardware that can prevent cyber crime or other malicious attacks. More than 61% are aware of the existence of these features. Most of the respondents believe that whole disk encryption is the most effective solution followed by anti-theft technologies such as location tracking and file- or record-level encryption.

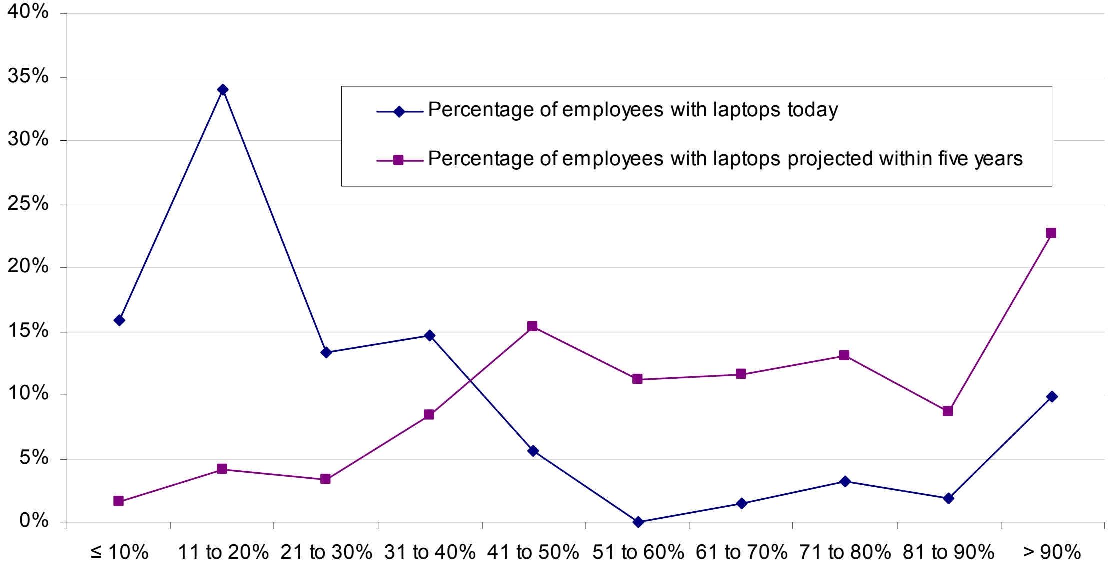
Leading practices that organizations use to reduce the risk of lost or stolen laptops include policies that require the prompt reporting of a lost or missing laptop, training and awareness programs about how to protect the laptop and the data stored on it.,strict authentication and access procedures and whole disk encryption

The next section provides the detail findings of the survey in graphical or bar chart format. This is followed by a summary of key demographics and organizational characteristics for the sample, and survey caveats. Detailed survey results are reported in the Appendix.

Survey findings

Line Graph 1 shows the percentage of employees who are assigned a laptop as their primary computer by their organizations. It also shows the percentage of employee-assigned laptops as projected by respondents within the next five years. This graph clearly shows a projected trend of significantly more laptops being assigned to employees in the future.

Line Graph 1
What percent of your company's employees are given a laptop computer for business use?
Today and within the next five years?

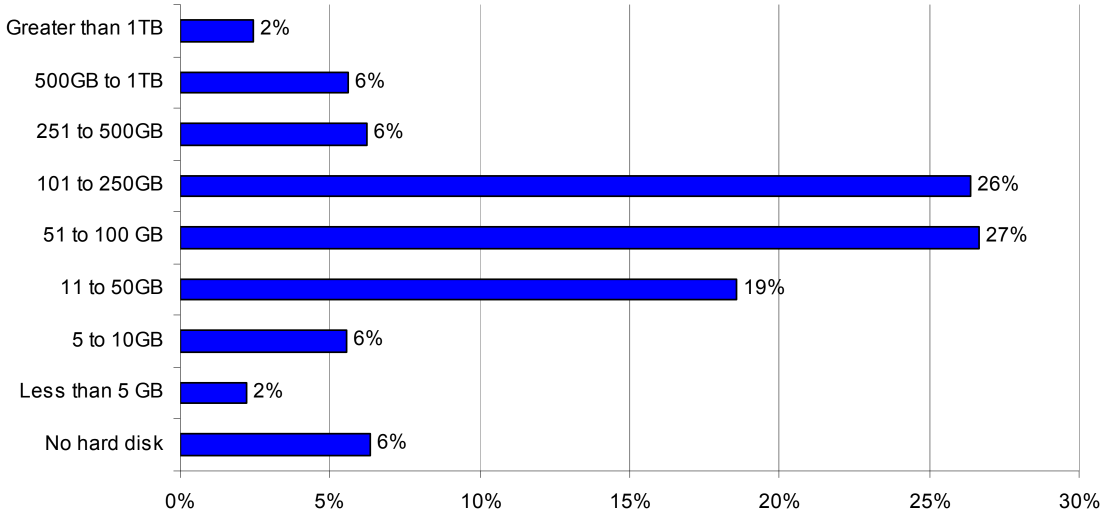


As noted in Table 1, the primary reasons for assigning laptops rather than desktop computers to employees are mobility (73%), productivity (69%) and cost savings (39%). Only 9% believe improved security as a reason for laptops vs. desktop computers.

Table 1 **What are the main reasons for assigning employees a laptop computer for business use?**	**Total%**
Mobility	73%
Productivity	69%
Cost savings	39%
Employee benefits	18%
Security	9%
Other	1%

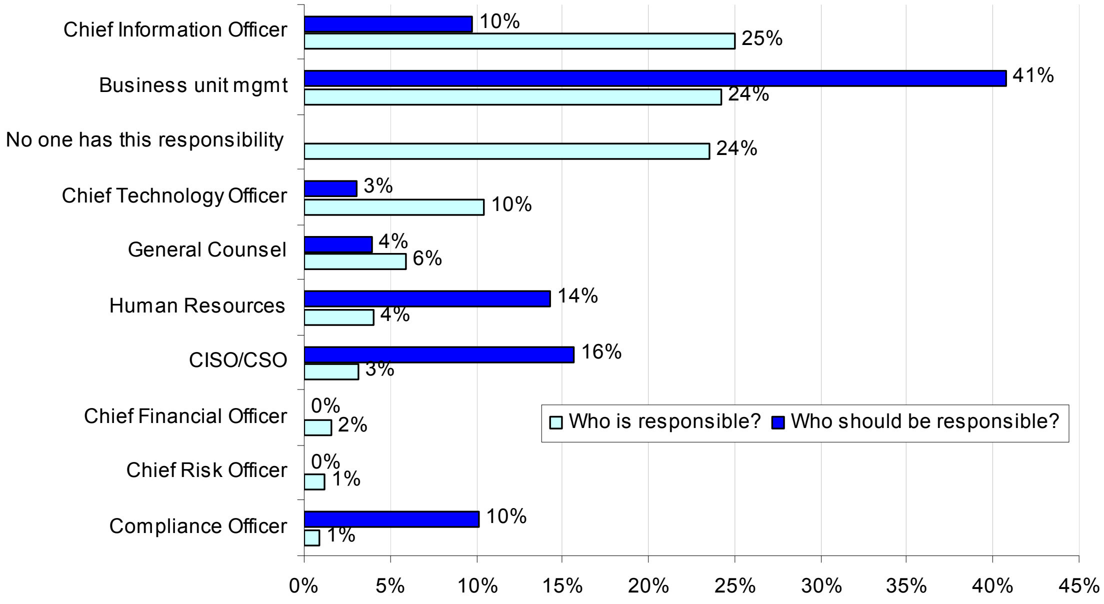
Bar Chart 1 reports the hard disk capacity of employee-assigned laptop computers among respondents' organizations. Less than 6% of laptops are configured without a hard disk (a.k.a. dumb terminal or drone). In contrast, 40% of organizations configure laptops with more than 100 gigabytes (GB). Only 2% of respondents say their organizations normally configure their laptop computers with more than one terabyte (TB).

Bar Chart 1
What is the hard disk capacity or size provided on employee-assigned laptops?



Bar Chart 2 provides a comparison of two survey questions. One question asked respondents to list who they believe is most responsible for ensuring laptop security today. The second question asked respondents to list who *should be* most responsible for securing laptop computers.

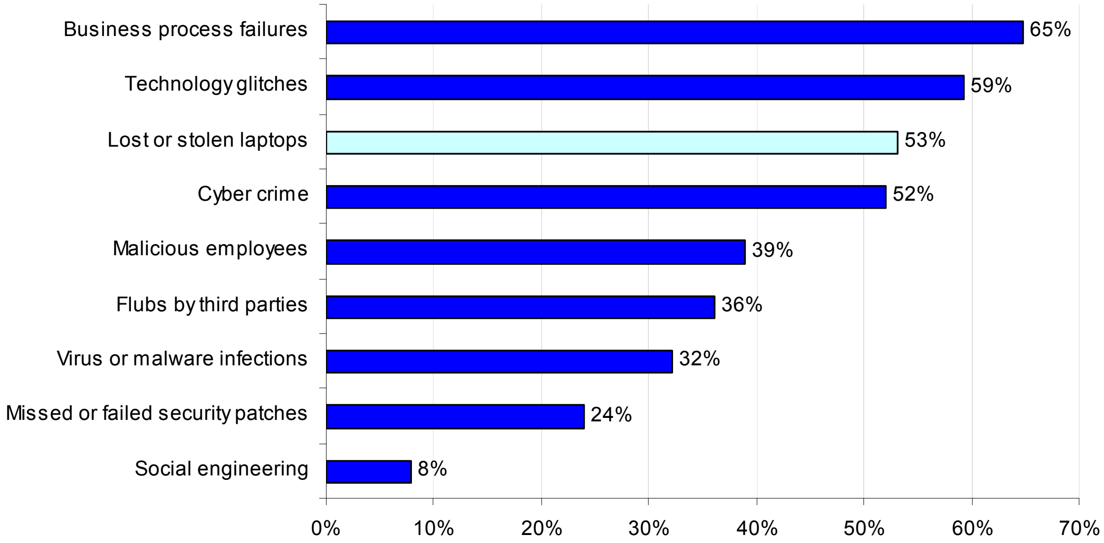
Bar Chart 2
Who is and who should be responsible for ensuring laptop computers are secure?



As shown above, respondents believe that business unit or departmental leaders, CISO/CSOs, human resources and compliance officers need to assume greater responsibility for securing laptops, while CIOs and CTOs should assume less responsibility. It is also interesting to see that 24% of respondents believe no one in their organizations are responsible for ensuring laptop computers are safe and secure.

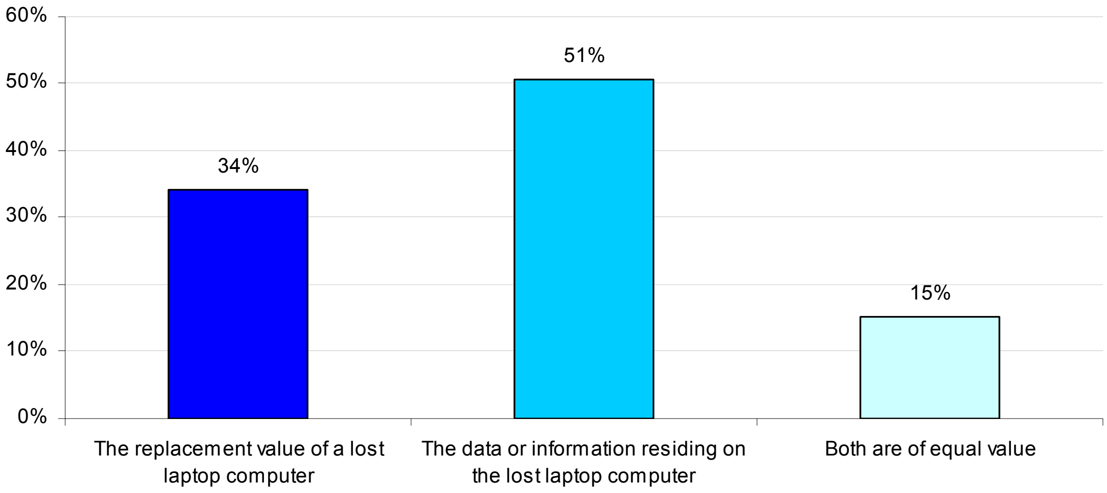
Bar Chart 3 provides a rank order of known security threats. Each bar reflects the percentage of responses that represented the two highest threat levels on a nine-point scale. The chart shows that business process failures, technology glitches and lost or stolen laptops are the top three security threats facing participants' organizations.

Bar Chart 3
Rank order of the threat of a lost or stolen laptop with other known security threats
Each bar defines the percentage of 1+ 2 (highest risk) on a nine-point scale



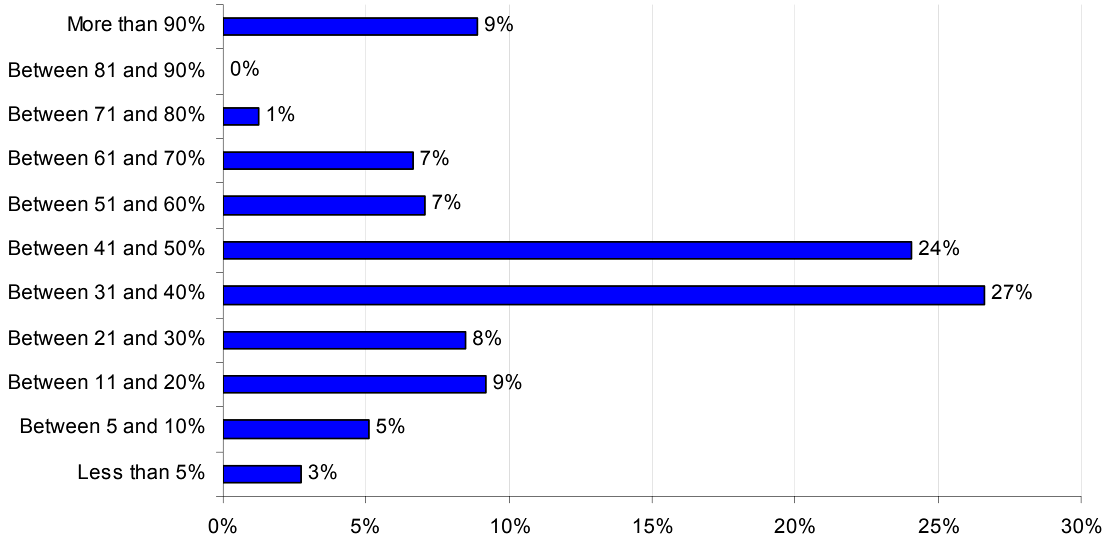
Bar Chart 4 reports the priorities with respect to the value of a lost laptop. In other words, is the replacement value of the equipment most important? Or, is the data stored on the computer more valuable? As shown, 51% of respondents believe the data or information residing on the device is more valuable than the replacement cost of the computer.

Bar Chart 4
In your organization, which is more valuable?



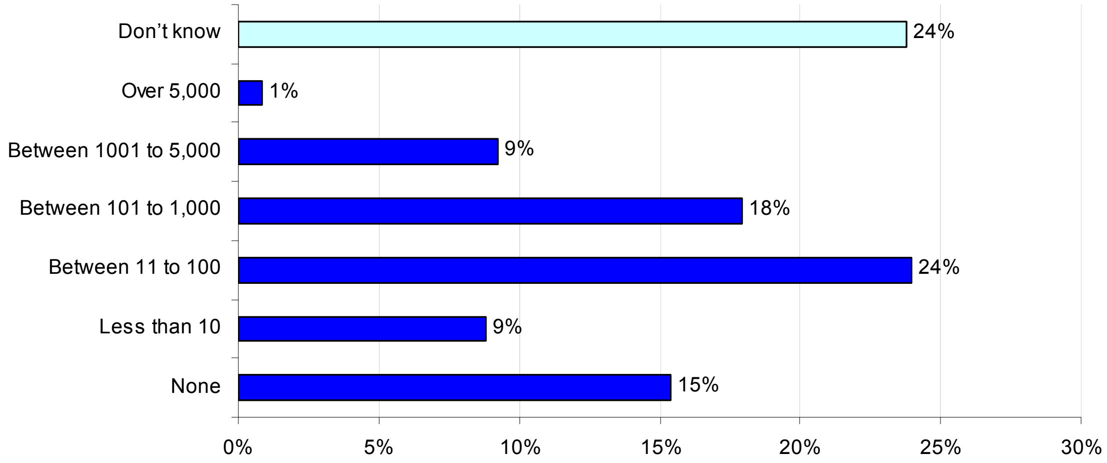
How much sensitive or confidential information is accessible to remote workers, contractors or other third parties? Bar Chart 5 reports availability of information assets. The distribution of responses suggests remote workers, contractors and third parties have significant access to the organization's confidential information.

Bar Chart 5
What percentage of your company's confidential data is accessed at any given time by remote workers, contractors or other third parties?



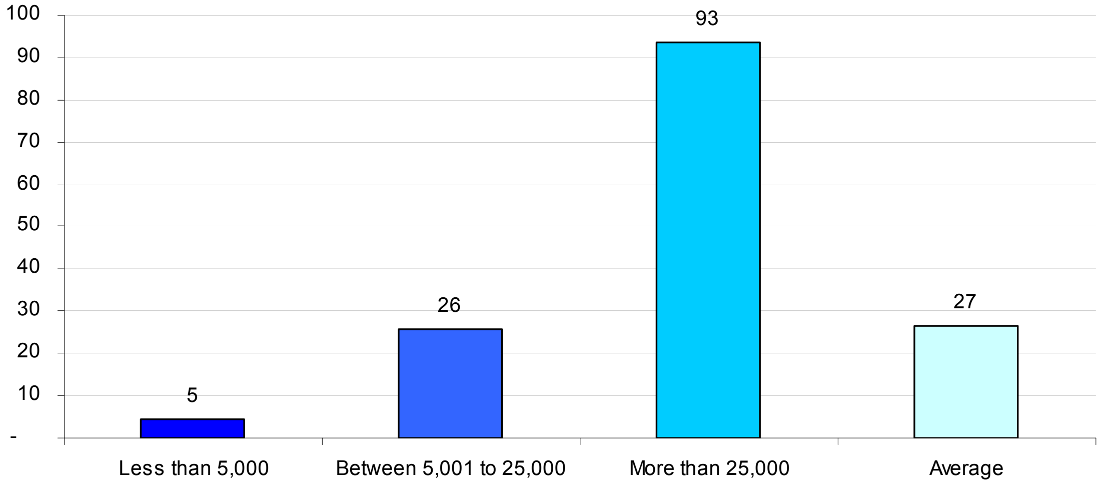
How many cyber crimes did respondents' organizations experience over the past 12 months? As reported in Bar Chart 6, more than 24% of respondents could not answer this question. Another 15% state that the number of cyber attacks is zero. The remaining 61% state that the range of cyber attacks varied from less than 10 to over 5,000 over the past year.

Bar Chart 6
How many cyber crime attacks did your organization have over the past year that resulted in economic loss including the disruption of service?



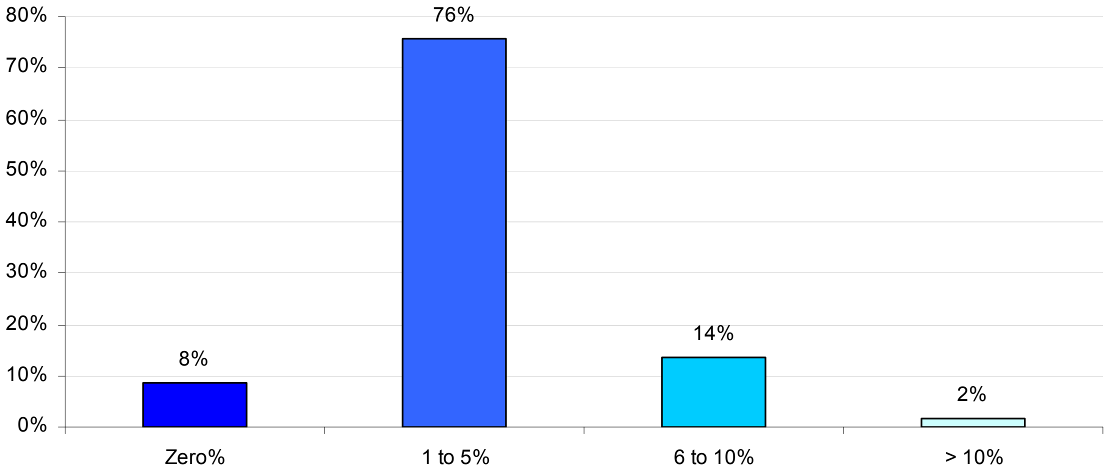
Bar Chart 7 reports the frequency of lost or stolen laptops over the past year according to the size of the respondent's organization (where size is measured by enterprise headcount). As shown, the average number of lost or stolen laptop computers equals 27. For companies with more than 25,000 employees, the average loss frequency increases to 93 laptop computers.

Bar Chart 7
How many laptops were lost or stolen in the past year within your organization
Enterprise size defined by worldwide headcount



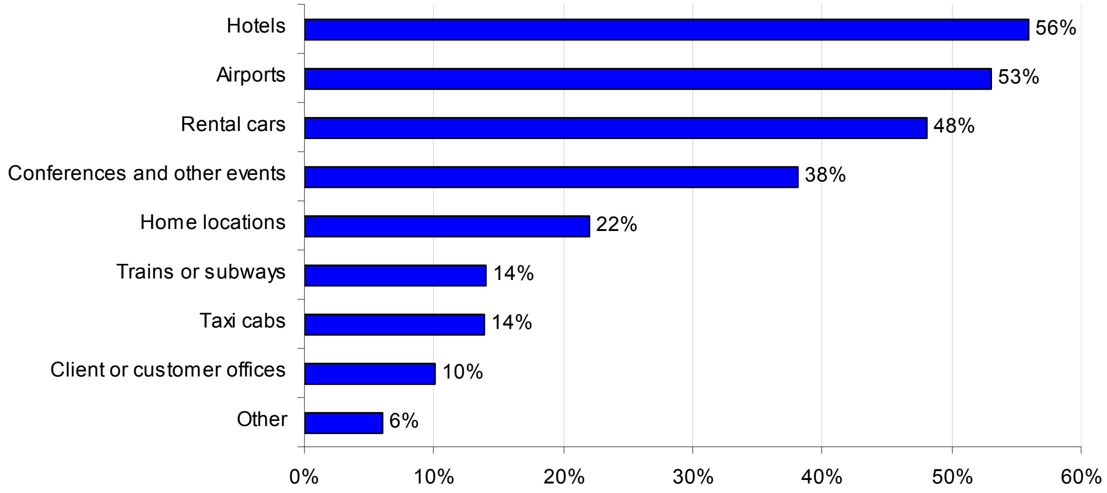
Bar Chart 8 shows the frequency of lost or stolen laptops as a percentage to the total number of laptops in use within respondents' organizations. Only 8% of respondents report a zero loss rate over the past year. More than 76% report a laptop loss rate between 1 to 5% of all laptops use.

Bar Chart 8
How many laptops were lost or stolen in the past year?
The percentage of total laptops in use within your organization



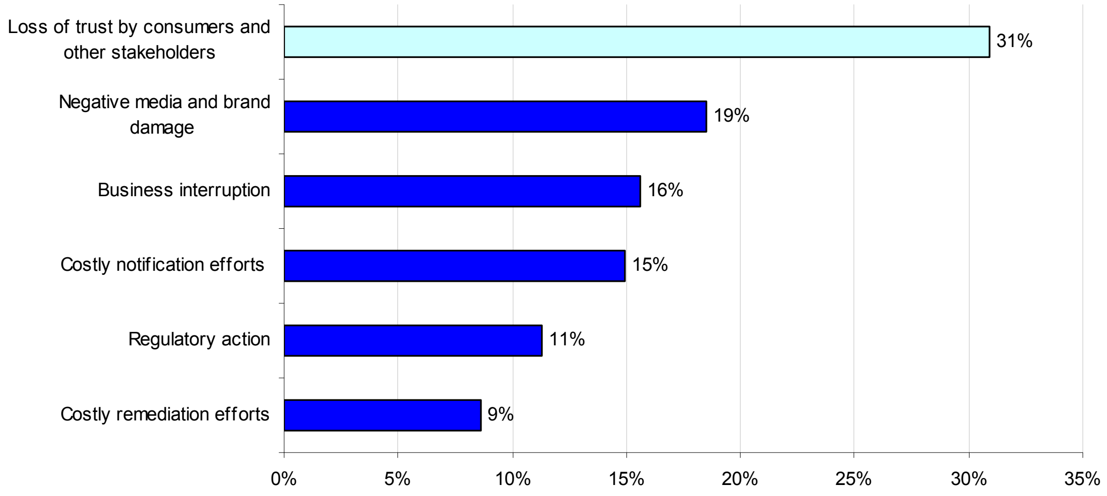
Bar Chart 9 reports the frequency of locations where laptop computers have been lost or stolen. According to respondents, the top three locations include hotels, airports and rental cars. Other common locations include conferences, home, trains or subways, and taxi cabs.

Bar Chart 9
What are the most common locations where employees lose their laptops?
More than one response is permitted



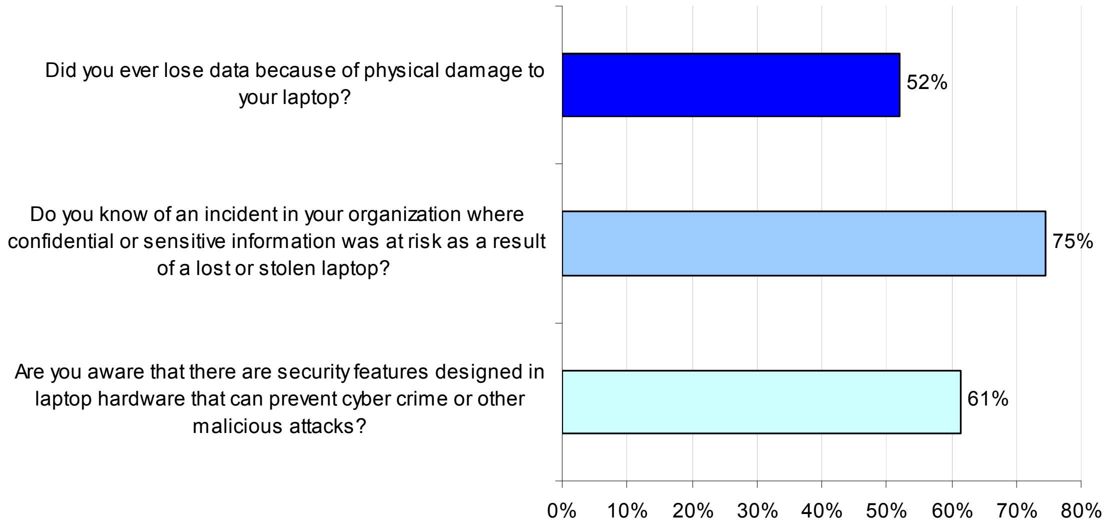
Bar Chart 10 shows the most significant consequences associated with laptop loss or theft. As can be seen, the most severe impact concerns the loss of trust by consumers and other stakeholders – perhaps following a data breach incident requiring notification to victims. The second highest consequence concerns negative media and resulting brand damage.

Bar Chart 10
If your organization had a lost or stolen laptop computer, which of the following possible consequences would have the most negative impact?



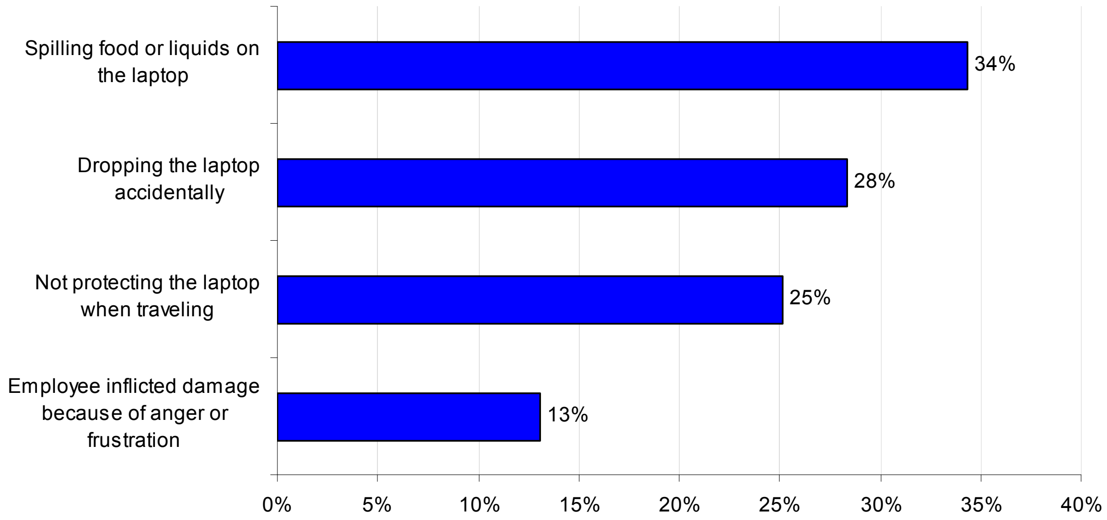
Bar Chart 11 shows a yes response to three important questions in the survey instrument. Accordingly, 52% of respondents said they lost data because of physical damage to their computer. About 75% said they know of one or more incidents where company's confidential information was at risk because of a lost or stolen laptop. Finally, 61% state that they are aware of security features on laptops that prevent or deter cyber crime and other malicious acts.

Bar Chart 11
Each bar defines the percentage Yes response to each question



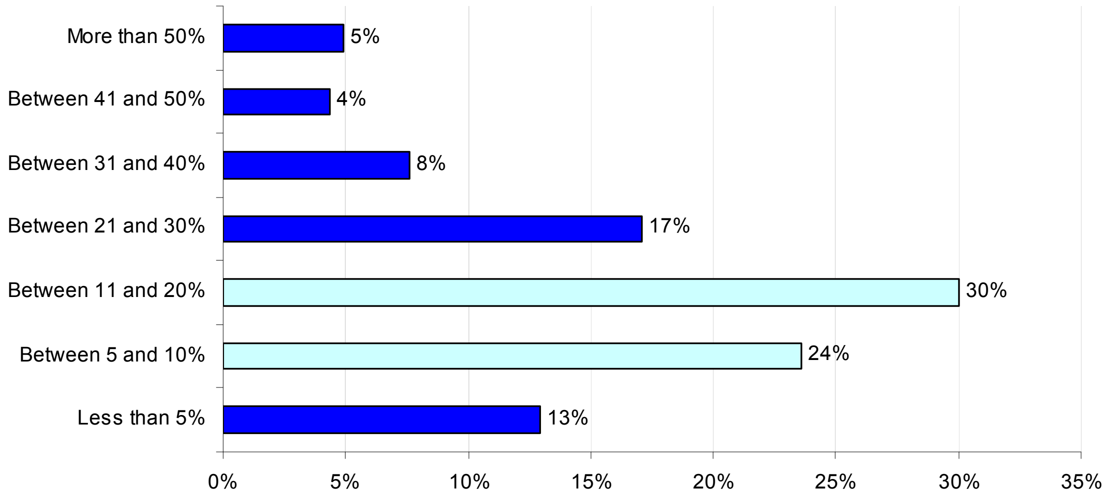
Bar Chart 12 reports common cause of physical damage to laptop computers. As can be seen, spilling food or liquids on the laptop is rated the number one cause followed by dropping the laptop accidentally. It is interesting to see that 13% of respondents report laptop damages caused by employee frustration or anger.

Bar Chart 12
What is the most common cause of physical damage to laptop computers that resulted in data loss within your organization?



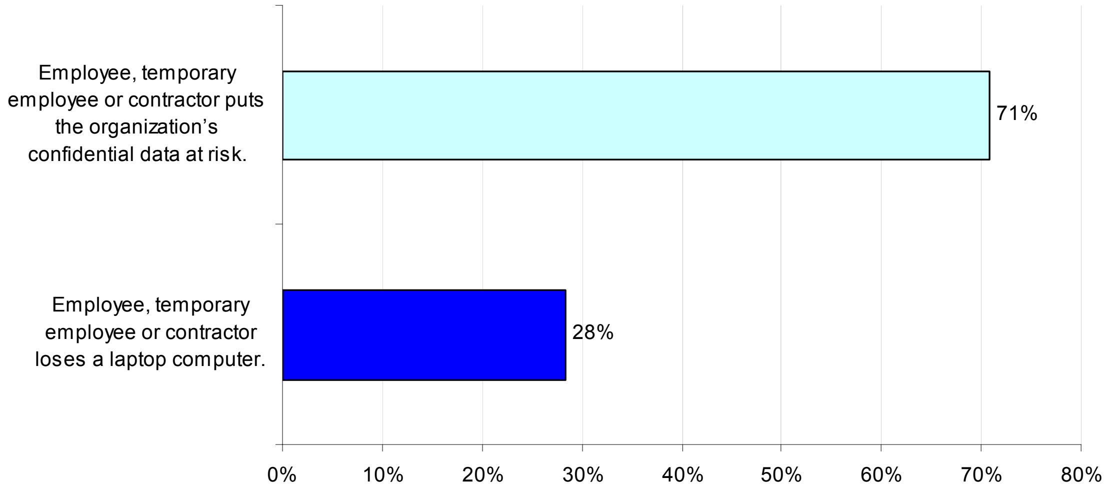
Bar Chart 13 shows the distribution of laptops damaged by employees by virtue of their anger or frustration, such as over technical glitches. More than 54% of respondents state that damaged laptops are the result of employee-inflicted acts 5% to 20% of the time.

Bar Chart 13
What percentage of damaged laptop computers within your organization is due to employee inflicted damage because of anger or frustration over technical issues?



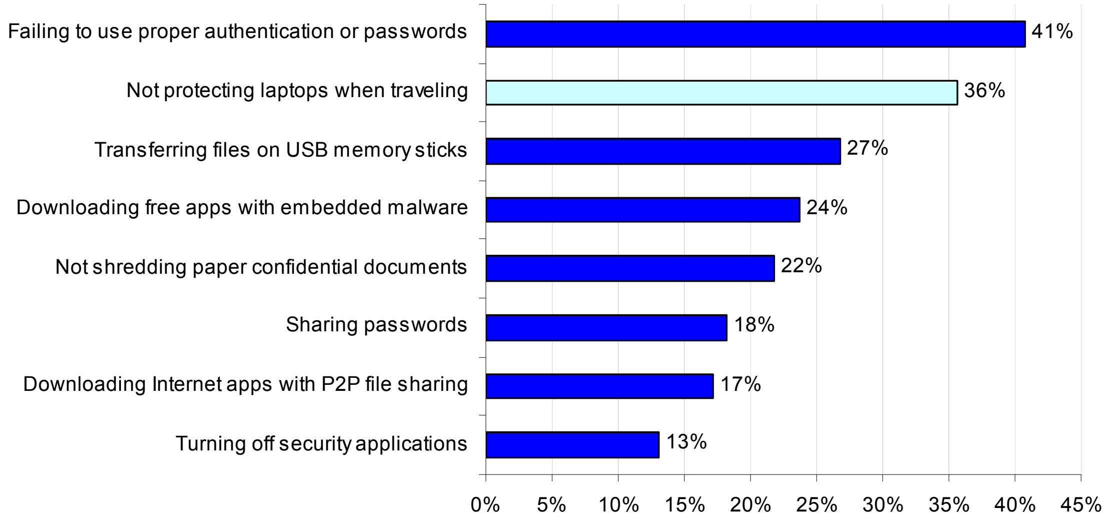
Bar Chart 14 reports data risks caused by employees, temporary employees or contractors. As shown, 71% state that employees, temporary employees and contractors frequently or very frequently put the organization’s confidential data at risk. More than 28% of respondents say that incidents involving lost or stolen laptops by employees, temporary employees and contractors are frequent or very frequent events.

Bar Chart 14
Data at risk: Each bar defines very frequently and frequently responses combined for two survey questions



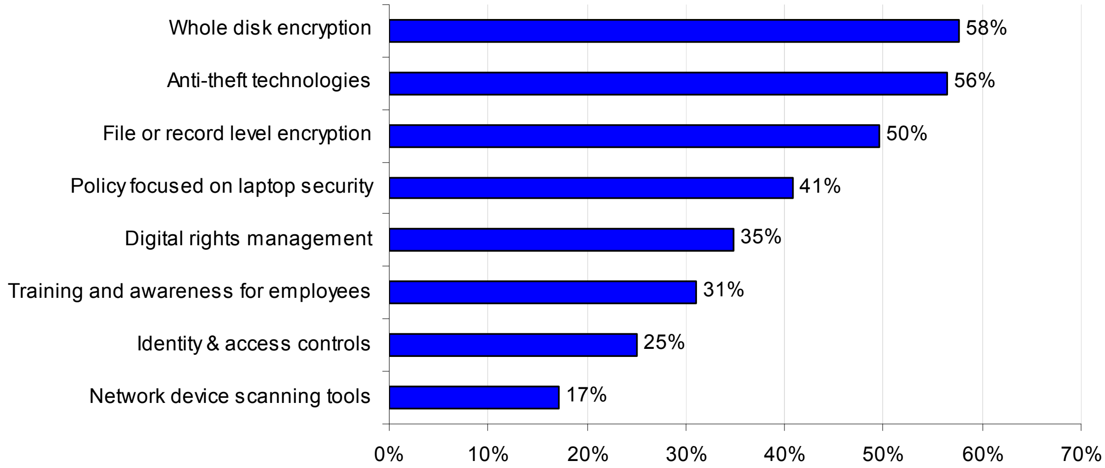
Bar Chart 15 shows the most salient data threats caused by insiders. As reported, the number one threat concerns improper authentication. The number two most serious threat concerns the failure to protect or secure laptops by employees when traveling outside office locations. The third most serious threat concerns the transfer of confidential information onto USB memory sticks.

Bar Chart 15
What are the greatest threats caused by employees to your organization?
More than one response is permitted



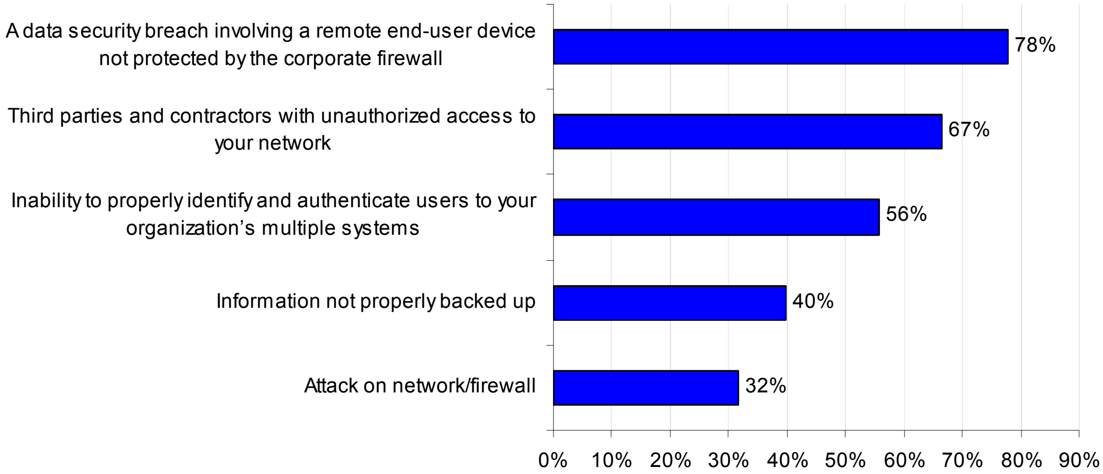
Bar Chart 16 reports the control methods used to reduce or mitigate the risk of lost or stolen laptop computers. Whole disk encryption, anti-theft technologies and file or record level encryption are the top three methods according to respondents. Other notable controls include laptop security policies, digital rights management and employee training.

Bar Chart 16
Rank order the control methods used to reduce the risk of lost or stolen laptops.
Each bar defines the percentage of 1+ 2 (most effective) on a five-point scale



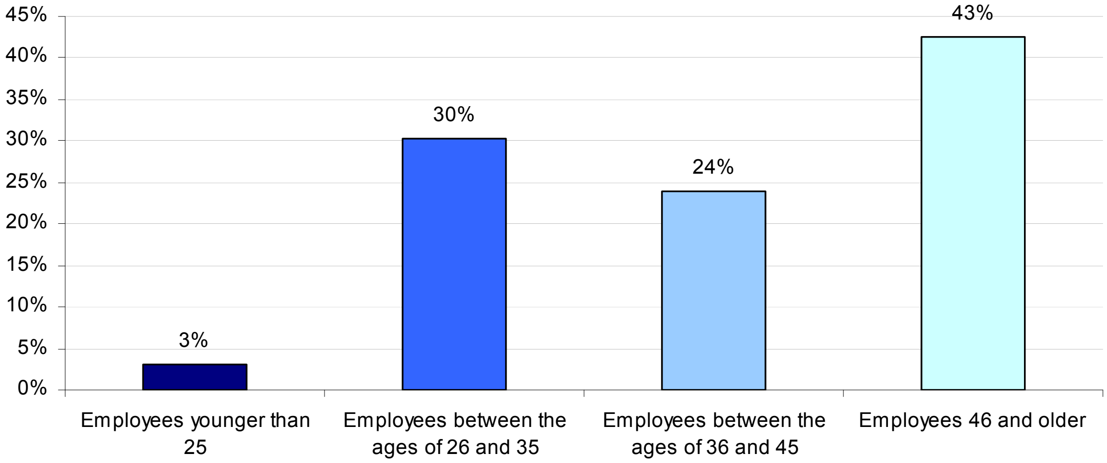
Bar Chart 17 reports the most salient information security threats according to participants. The number one security threat concerns a data breach event involving a remote user device not protected by the corporate firewall (perhaps as a result of cloud computing applications). The second most serious information security threat concerns third party or contractors with unauthorized access to corporate networks.

Bar Chart 17
What are the greatest threats to your organization's information security?
More than one response is permitted



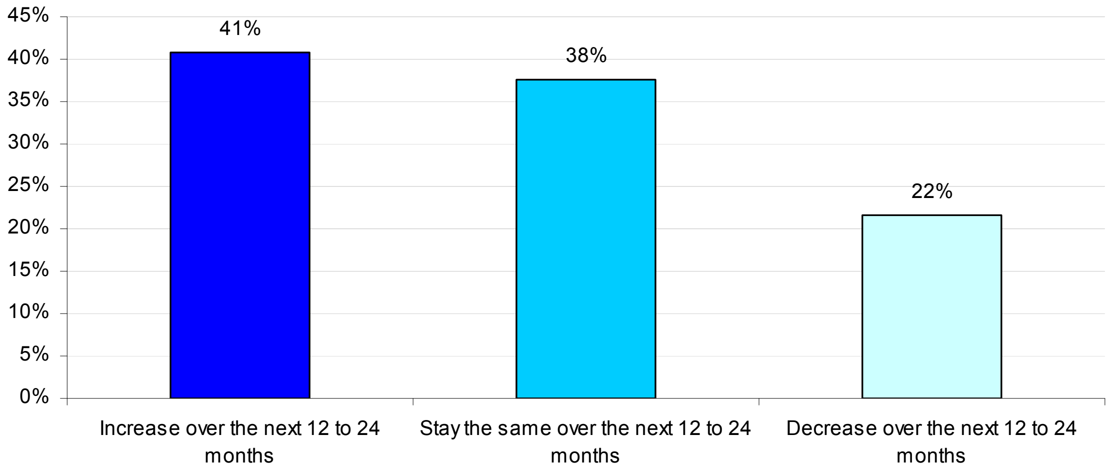
Bar Chart 18 reports respondents' perception about the affect of end-user's age on their data security efforts, including laptop protection efforts. It is interesting to see only 3% of respondents believe that younger employees (less than 25 years) are most likely to practice safe data security. In contrast, over 43% of respondents say end-users who are 46+ are the most safety-oriented age group.

Bar Chart 18
Which age group is best at practicing safe data security?



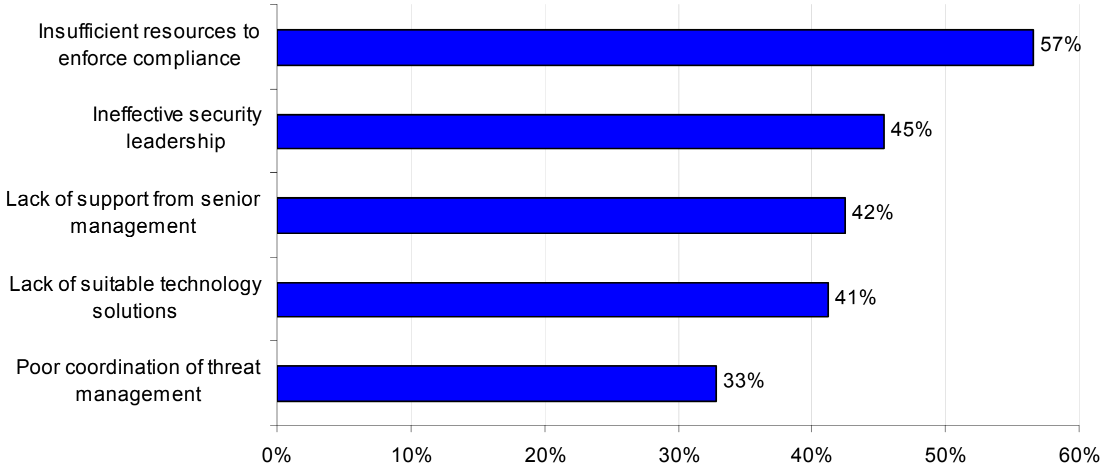
Bar Chart 19 provides the respondents' outlook on lost laptop risk over the next one to two years. Over 41% of respondents believe the risk of lost or stolen laptops will increase within their organizations over the next 12 to 24 months. Another 38% believe that this risk will stay at about the same level, and 22% believe the risk will decrease over the next 12 to 24 months.

Bar Chart 19
How will the risk of having lost or stolen laptop computers change?



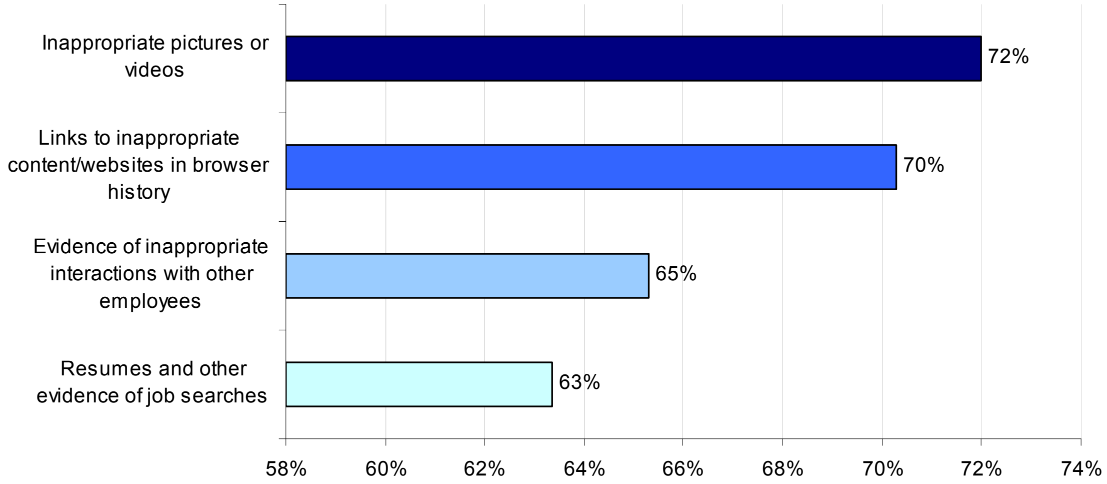
Bar Chart 20 reports the reasons why data risk is expected to increase or stay the same over the next two years. The number one reason concerns insufficient resources within the organization to strictly enforce compliance. Ineffective security leadership and the lack of support from senior management are the second and third reasons, respectively.

Bar Chart 20
If the risk increases or stays the same, why?
More than one response is permitted



Bar Chart 21 reports the types of inappropriate data discovered on employee's laptop computers, perhaps after missing laptops are found. As can be seen, the most common types of data include inappropriate pictures or videos, links to inappropriate websites (such as adult content or gambling sites), evidence of inappropriate interactions with other employees and resumes and other evidence to job search activities.

Bar Chart 21
Did you ever discover the following on an employee's laptop?
More than one response is permitted



Methods

A random sampling frame of 15,993 adult-aged individuals who reside within the United States was used to recruit participants to this web survey.[1] Our randomly selected sampling frame was selected from three national mailing lists of professionals employed in the IT and data security fields.

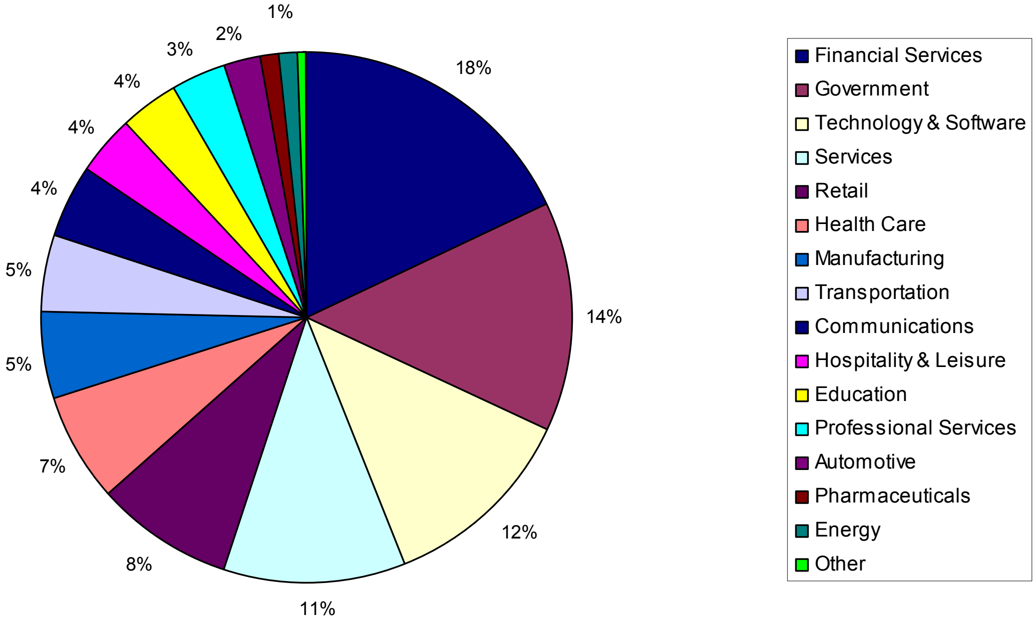
Table 2: Sample description	Freq.
Total sampling frame	15,993
Bounce-back	4,025
Total returns	816
Rejected surveys	102
Final sample	714
Response rate	4.5%

Table 2 shows that 816 respondents elected to complete the survey results during within an eight-day research period. Of returned instruments, 102 were rejected because of reliability tests. A total of 714 surveys were used as our final sample. This sample represents a 4.5% response rate. The margin of error on all adjective scale responses is ≤ 3.5 percent.

Pie Chart 1 shows the distribution of respondents by their organization's primary industry classification. As shown, financial services, government, technology & software, services and retailers represent the largest industry segments in the final sample.

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

Pie Chart 1: Distribution of respondents by industry classification



Over 96% of respondents completed all survey items within 20 minutes. Respondents, on average, have 9.6 years of overall experience and 7.4 in the IT or security fields. About 62% of respondents were males and 38% females. While results are skewed on the gender variable (more male than female respondents), this result is consistent with known demographics about the corporate IT fields in North America.

Table 3a reports the most frequently cited functional areas of respondents. Table 3b provides the self-reported organizational level of respondents. As can be seen, the majority of respondents are at the manager (20%), supervisor (19%) or technician (26%) levels. Over 10% are at or above the director level.

Table 3a: Top functional areas	Pct%
Information security	24%
Operations	21%
Network management	18%
Application development	10%
Data protection	8%
Data quality & compliance	8%
Other	11%

Table 3b: Organizational levels	Pct%
Vice President	1%
Director	9%
Manager	20%
Supervisor	19%
Associate/Staff	19%
Technician	26%
Consultant	4%
Other	2%

Table 4a reports the organization’s geographic footprint outside the United States, showing that the majority of respondents’ organizations have operations in Canada and Europe. Table 4b provides the approximate headcounts of participating organizations. As can be seen, 60% of respondents are employed by large organizations with more than 5,000 employees.

Table 4a The organization’s geographic footprint	Pct%
United States	98%
Canada	53%
Europe	57%
Middle East	18%
Latin America	35%
Asia	44%
Africa	6%
Australia & New Zealand	25%

Table 4b Organizational size based on global headcount?	Pct%
Less than 500 people	13%
500 to 1,000 people	12%
1,001 to 5,000 people	15%
5,001 to 10,000 people	17%
10,001 to 25,000 people	20%
25,001 to 50,000 people	10%
50,001 to 75,000 people	5%
More than 75,000 people	8%

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 frequency and percentage frequency tables.

Appendix 1: Detailed survey results

Following are the audited results of a web-based survey involving 714 IT and IT security practitioners from organizations located in the United States. These results are presented in a percentage frequency format. Pct% = only one choice permitted. Total% = two or more choices are permitted.

Sample description	Freq.
Total sampling frame	15993
Bounce-back	4025
Total returns	816
Rejected surveys	102
Final sample	714
Response rate	4.5%

Q1. Current Title (Top 5 choices)	Pct%
Information security	24%
Operations	21%
Network management	18%
Application development	10%
Data protection	8%
Data quality & compliance	8%
Other	11%
Total	100%

Q2. What organizational level best describes your current position?	Pct%
Vice President	1%
Director	9%
Manager	20%
Supervisor	19%
Associate/Staff	19%
Technician	26%
Consultant	4%
Other	2%
Total	100%

Q3. Check the **Primary Person** you or your manager reports to within your organization.	Pct%
CEO/Executive Committee	0%
Chief Financial Officer	4%
Chief Information Officer	41%
Chief Technology Officer	14%
Chief Risk Officer	5%
Chief Security Officer	6%
Compliance Officer	10%
General Counsel	3%
Human Resources	2%
Director of IT Security	13%
Other	2%
Total	100%

Q4. Check the **Secondary Person** you or your manager reports to within your organization. Leave blank if not applicable.	Pct%
CEO/Executive Committee	0%
Chief Financial Officer	6%
Chief Information Officer	24%
Chief Technology Officer	18%
Chief Risk Officer	1%
Chief Security Officer	4%
Compliance Officer	14%
General Counsel	0%
Human Resources	0%
Director of IT Security	23%
Other	10%
Total	100%
Blank = 509 responses (71%)	

Q5a. Years of business experience	9.55
Q5b. Years in the IT or security field	7.48
Q5c. Years in current position	3.09

Q6. Gender	Pct%
Female	38%
Male	62%
Total	100%

Q7. Do you occupy a full time position?	Pct%
Yes	88%
No	12%
Total	100%

Q8. In which regions does your organization operate? Please check all that apply.	Pct%
United States	98%
Canada	53%
Europe	57%
Middle East	18%
Latin America (including Mexico)	35%
Asia	44%
Africa	6%
Australia & New Zealand	25%

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).	Pct%
Automotive	2%
Education	4%
Financial Services	18%
Government	14%
Health Care	7%
Hospitality & Leisure	4%
Manufacturing	5%
Transportation	5%
Pharmaceuticals	1%
Professional Services	3%
Retail	8%
Services	11%
Communications	4%
Technology & Software	12%
Energy	1%
Other (please specify)	1%
Total	100%

Q10. What is the headcount of your IT organization?	Pct%
Less than 100 people	13%
101 to 500 people	9%
501 to 1,000 people	22%
1,001 to 5,000 people	24%
5,001 to 10,000 people	25%
More than 10,000 people	6%
Total	100%

Q11. What is the worldwide headcount of your organization?	Pct%
Less than 500 people	13%
500 to 1,000 people	12%
1,001 to 5,000 people	15%
5,001 to 10,000 people	17%
10,001 to 25,000 people	20%
25,001 to 50,000 people	10%
50,001 to 75,000 people	5%
More than 75,000 people	8%
Total	100%

Q12. What percentage of your company's employees is given a laptop computer for business use?	Pct%
Less than 10%	16%
11 to 20%	34%
21 to 30%	13%
31 to 40%	15%
41 to 50%	6%
51 to 60%	0%
61 to 70%	1%
71 to 80%	3%
81 to 90%	2%
More than 90%	10%
Total	100%

Q13. Five years from now, approximately what percentage of your company's employees will be given a laptop computer for business use?	Pct%
Less than 10%	2%
11 to 20%	4%
21 to 30%	3%
31 to 40%	8%
41 to 50%	15%
51 to 60%	11%
61 to 70%	12%
71 to 80%	13%
81 to 90%	9%
More than 90%	23%
Total	100%

Q14. On average, what is the hard disk capacity or size provided on employee-assigned laptops?	Pct%
No hard disk (dumb terminals)	6%
Less than 5 GB	2%
5 to 10GB	6%
11 to 50GB	19%
51 to 100 GB	27%
101 to 250GB	26%
251 to 500GB	6%
500GB to 1TB	6%
Greater than 1TB	2%
Total	100%

Q15. What are the main reasons for assigning employees a laptop computer for business use? Please check all that apply.	Total%
Cost savings	39%
Productivity	69%
Mobility	73%
Employee benefits	18%
Security	9%
Other	1%
Total	208%

Q16a. In your organization, **who is** responsible for ensuring laptop computers are safe and secure? Please check only one.	Pct%
No one person has this responsibility	24%
Business unit or departmental management	24%
CISO/CSO	3%
Chief Risk Officer	1%
Chief Financial Officer	2%
Chief Information Officer	25%
Chief Technology Officer	10%
Chief Privacy Officer	0%
Compliance Officer	1%
General Counsel	6%
Human Resources	4%
Other (please specify)	0%
Total	100%

Q16b. In your organization, **who should be** responsible for ensuring laptop computers are safe and secure? Please check the one best choice.	Pct%
Business unit or departmental management	41%
CISO/CSO	16%
Chief Risk Officer	0%
Chief Financial Officer	0%
Chief Information Officer	10%
Chief Technology Officer	3%
Chief Privacy Officer	3%
Compliance Officer	10%
General Counsel	4%
Human Resources	14%
Other (please specify)	0%
Total	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.	Percent 1+ 2
Business process failures	65%
Technology glitches	59%
Lost or stolen laptops	53%
Cyber crime	52%
Malicious employees	39%
Outsourcing to undependable vendors	36%
Virus or malware infections	32%
Missed or failed security patches	24%
Social engineering	8%
Average	41%

Q18. In your organization, which is more valuable?	Pct%
The replacement value of a lost laptop computer	34%
The data or information residing on the lost laptop computer	51%
Both are of equal value	15%
Total	100%

Q19. Which types of information present the greatest risk when a laptop computer is lost or stolen? Please select only two choices.	Total%
Customer information (such as contact lists)	56%
Employee information	48%
Non-financial confidential information	29%
Financial confidential information	27%
Software programs, tools, applications and source code	13%
Other intellectual properties	23%
Total	196%

Q20. What percentage of your company's confidential data is accessed at any given time by remote workers, contractors or other third parties?	Pct%
Less than 5%	3%
Between 5 and 10%	5%
Between 11 and 20%	9%
Between 21 and 30%	8%
Between 31 and 40%	27%
Between 41 and 50%	24%
Between 51 and 60%	7%
Between 61 and 70%	7%
Between 71 and 80%	1%
Between 81 and 90%	0%
More than 90%	9%
Total	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?	Pct%
None	15%
Less than 10	9%
Between 11 to 100	24%
Between 101 to 1,000	18%
Between 1001 to 5,000	9%
Over 5,000	1%
Don’t know	24%
Total	100%

22a. Approximately, how many laptops were lost or stolen in the past year within your organization (entire enterprise),:	Pct%
None	8%
Less than 10	11%
Between 11 to 20	23%
Between 21 to 50	16%
Between 51 to 100	6%
Between 101 to 200	2%
Between 201 to 500	1%
More than 500	1%
Don't know	31%
Total	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:	Pct%
Zero%	8%
1 to 5%	76%
6 to 10%	14%
11 to 20%	2%
21 to 30%	0%
31 to 40%	0%
41 to 50%	0%
More than 50%	0%
Total	100%

Q23. Are you aware that there are security features designed in laptop hardware that can prevent cyber crime or other malicious attacks?	Pct%
Yes	61%
No	39%
Total	100%

Q24. How has the number of laptop losses changed from prior years?	Pct%
Increasing	65%
Staying the same	21%
Decreasing	7%
Unsure	7%
Total	100%

Q25. What are the most common locations where employees lose their laptop computers? Please check the top three choices.	Total%
Airports	53%
Taxi cabs	14%
Trains or subways	14%
Rental cars	48%
Hotels	56%
Conferences and other events	38%
Client or customer offices	10%
Home locations	22%
Other (please specify)	6%
Total	261%

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 only one.	Pct%
Regulatory action	11%
Negative media and brand damage	19%
Business interruption	16%
Costly remediation efforts	9%
Costly notification efforts	15%
Loss of trust by consumers and other stakeholders	31%
Other (please specify)	0%
Total	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?	Pct%
Yes	75%
No	25%
Total	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.	Pct%
Spilling food or liquids on the laptop	34%
Dropping the laptop accidentally	28%
Not protecting the laptop when traveling	25%
Employee inflicted damage because of anger or frustration	13%
Other (please specify)	0%
Total	101%

Q28b. Did you ever lose data because of physical damage to your computer?	Pct%
Yes	52%
No	48%
Total	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?	Pct%
Less than 5%	13%
Between 5 and 10%	24%
Between 11 and 20%	30%
Between 21 and 30%	17%
Between 31 and 40%	8%
Between 41 and 50%	4%
Between 51 and 60%	5%
Between 61 and 70%	0%
Between 71 and 80%	0%
Between 81 and 90%	0%
More than 90%	0%
Total	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.	Pct%
Very frequent	8%
Frequent	20%
Not frequent	50%
Rarely	14%
Never happens	7%
Total	100%

Q29b. Employee, temporary employee or contractor puts the organization’s confidential data at risk?	Pct%
Very frequent	17%
Frequent	54%
Not frequent	19%
Rarely	9%
Never happens	1%
Total	100%

Q30. What are the greatest threats caused by employees to your organization’s confidential data? Please select the top two threats.	Pct%
Failing to use proper authentication or passwords	41%
Not protecting laptops when traveling	36%
Transferring files on USB memory sticks	27%
Downloading free apps or widgets with embedded malware	24%
Not shredding paper documents containing confidential information	22%
Sharing passwords	18%
Downloading Internet apps with P2P file sharing	17%
Turning off security applications	13%
Other (please specify)	1%
Total	198%

Q31. What methods does your organization use to reduce the risk of lost or stolen laptop computers? Please check all methods deployed today.	Total%
Policy focused on laptop security	72%
Training and awareness for employees focused on laptop security	69%
Identity management and access controls	52%
Whole disk encryption	41%
Network device scanning tools	30%
File or record level encryption	26%
Anti-theft technologies such as location tracking	19%
Digital rights management	9%
Total	317%

Q32. Please rate the <u>effectiveness</u> 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= Not effective	Percent 1+ 2
Anti-theft technologies such as location tracking	56%
Whole disk encryption	58%
File or record level encryption	50%
Digital rights management	35%
Network device scanning tools	17%
Identity management and access controls	25%
Training and awareness for employees focused on laptop security	31%
Policy focused on laptop security	41%
Average	39%

Q33a. In your opinion, the risk of having lost or stolen laptop computers will:	Pct%
Increase over the next 12 to 24 months	41%
Stay the same over the next 12 to 24 months	38%
Decrease over the next 12 to 24 months	22%
Total	100%

Q33b. If the risk **increases or stays the same**, why? Check all that apply.	Total%
Lack of support from senior management	42%
Poor coordination of threat management	33%
Ineffective security leadership	45%
Insufficient resources to enforce compliance	57%
Lack of suitable technology solutions	41%
Other (please specify)	2%
Total	221%

Q33c. If the risk **decreases**, why? Check all that apply.	Total%
Support from senior management	8%
Coordination of threat management	42%
Effective security leadership	50%
Sufficient resources to enforce compliance	66%
Suitable technology solutions	61%
Other (please specify)	0%
Total	228%

Q35. Did you ever discover the following on an employee's laptop?	Pct% = Yes
Inappropriate pictures or videos	72%
Links to inappropriate content/websites in browser history	70%
Evidence of inappropriate interactions with other employees	65%
Resumes and other evidence of job searches	63%
Average	68%

Q36. In general, what are the greatest threats to your organization's information security? Please select the top two.	Total%
Attack on network/firewall	32%
A data security breach involving a remote end-user device not protected by the corporate firewall	78%
Third parties and contractors with unauthorized access to your network	67%
Information not properly backed up	40%
Inability to properly identify and authenticate users to your organization's multiple systems	56%
Total	272%

Q37. 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?	Pct%
Employees younger than 25	3%
Employees between the ages of 26 and 35	30%
Employees between the ages of 36 and 45	24%
Employees 46 and older	43%
Total	100%

Q37a. Which of the following is the primary reason this age group is best at practicing safe data security? Please select the top two reasons.	Total%
This age group is more knowledgeable about how to protect their organization's information security	22%
This age group understands best how a data breach can adversely affect their organization	43%
This age group believes practicing safe security is an important part of their job	60%
They do not understand how to circumvent data security procedures	33%
	158%

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.