



Trends in Insider Compliance with Data Security Policies

Employees Evade and Ignore Security Policies

Sponsored by IronKey

Independently conducted by Ponemon Institute LLC

Publication: June 2009

Trends in Insider Compliance with Data Security Policies *Employees Evade and Ignore Security Policies*

Prepared by Dr. Larry Ponemon, June 2009

Sponsored by IronKey, Ponemon Institute is pleased to present the independent results of a second national survey, *Trends in Insider Compliance with Data Security Policies*. The study was conducted to better understand employee compliance with data security policies in the workplace. In this report, we compare findings from the 2007 study on this topic, *Data Security Policies Are Not Enforced*.

We surveyed 967 individuals who are end-users of corporate information technologies (IT) to determine if they believe their organizations are proactively protecting equipment and information assets by forbidding illegal data transfer, restricting password sharing with co-workers, limiting access to web-based email accounts, seizing legal attachments sent to personal email addresses, and preventing anti-virus or firewall settings from being disabled by employees on their workplace computers.

Based on previous research conducted by Ponemon Institute, IT security practitioners consider malicious or negligent insiders to pose the greatest threat to the safety of an organization's information assets. Hence, it would seem logical that organizations should focus on creating policies that are strictly enforced and training end-users of corporate IT on the importance of complying with these policies.

What we learned in this survey, however, is that individuals believe that their companies do not provide adequate training about compliance with data security policies or requirements, their company's data security policies are ineffective, and the policies are largely ignored by a majority of employees including management personnel.

Some of the most salient findings are:

- A majority of respondents admit to serious non-compliant workplace behaviors that place their companies at risk. Such behaviors include the insecure use of USB memory sticks, web-based email, social media, mobile devices, and more.
- The rate of non-compliant employee behavior appears to be getting worse over time. The most serious example includes the increasing frequency of lost or missing USB memory sticks or other portable data-bearing devices that are not reported to the company (or reported in a timely fashion).
- Employee attitudes about their employers (i.e. favorable vs. unfavorable) appear to temper the level of non-compliant workplace behavior; that is, favorable perceptions are associated with lower levels of non-compliant behavior.
- Employees do not believe their organizations provide ample training or adequate policies to inform them about data protection and security practices in their workplace.

Following are the key findings of this survey research. Please note that most of the results are displayed in either line or bar chart formats. The actual data utilized in each figure and referenced in the paper can be found in the percentage frequency tables attached as the Appendix to this paper.

Employee attitudes

We asked respondents to indicate their agreement, uncertainty or disagreement with a series of statements about their organization. The goal was to learn if the respondents in this study believe

their organization takes the appropriate steps to protect data and if the culture could possibly encourage or discourage compliance with data security policies.

Figure 1 reports participants' perceptions about their organizations according to eight attributions. As can be seen, the most positive attribution concerns customer respect and the least positive attribution concerns the organization's social responsibility. With respect to data protection and security, 42% believe their organization has adequate data protection policies and procedures, 38% believe their organization takes appropriate steps to protect privacy rights, and 37% believe their company has adequate technologies to protect data.

Three of these attributions, noted in light blue, were used to construct a simple index about how participants view their organization's culture. These three attributions include: respect toward employees, integrity of senior leadership, and the organization's social responsibility.

The index is the average value for strongly agree or agree responses for these three items, which is 44% for the entire sample. Thus, a value higher than this average suggests the respondent holds a favorable perception and a value lower than this average suggests the respondent's unfavorable perception. This index value is later used (see Figure 5) to see if favorable or unfavorable perceptions are related to the employee's compliance behaviors with respect to the organization's security policy.

Figure 1
Attributions about participants' companies

Percentage of strongly agree and agree combined.

The three items in light blue are used to construct an index about how participants view their organizations. The index is the average value of the strongly agree or agree responses for all three items (which is 44% for the overall study). A value higher than the mean implies a net favorable perception and a value lower than the mean implies a net unfavorable perception. The dotted red line provides the average response for all eight items.



Executive summary

Figure 2 summarizes individual responses to two sets of questions: one pertaining to what they do (a.k.a. first party construct) and the other pertaining to what others in their organizations do (a.k.a. third party construct). This first and third-party construct is used to assess possible "halo effects" that often accompany questions that are normatively laden. The following are seven commonly cited data security threats in the workplace included in our survey instrument:

1. Use of insecure USB memory stick
2. Use of a web-based personal email account
3. Downloading Internet applications
4. Loss of a mobile data-bearing device
5. Turning off security software such as an anti-virus or scanning application
6. Sharing passwords with co-workers or contractors
7. Use of public social networks

With the exception of social networks, all of these data security threats were incorporated in a survey completed in 2007. Accordingly, we compare responses in this study to findings from the 2007 study to determine trends in compliance with data security policies. We show what respondents do, what they believe others do, and the current state of compliance (or non-compliance) with their organization's formal policies and procedures.

Figure 2
First vs. third-party construct

The difference between the two line graphs is the so-called "halo effect" – that is, the gap between what people say they do versus what they say others do.

What you do versus what you believe others do	What you do	What others do
USB memory stick	61%	71%
Web-based personal email	52%	60%
Downloading Internet software	53%	55%
Loss of mobile data-bearing devices	43%	46%
Turning off security software	21%	28%
Sharing passwords	47%	57%
Social networking in the workplace	31%	0.31

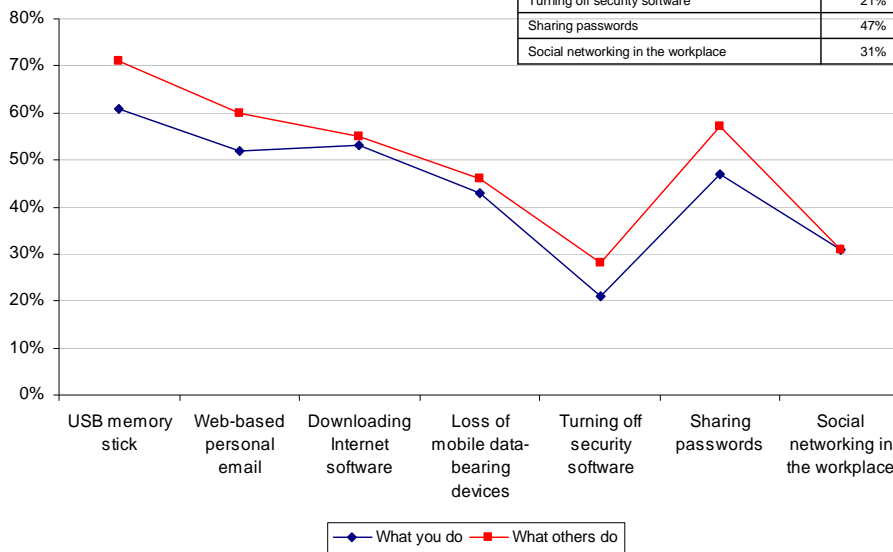


Figure 2 shows approximately the same pattern for the first and third-party responses on all seven threat scenarios. Each point on the line graph is the percentage frequency of end-users who admit to doing what is deemed as a data security threat in the workplace. As can be seen, the highest threat concerns the transfer of confidential information onto a USB memory stick – that is, 61% say they do it and 71% say others do it. The next highest threat concerns the downloading of free Internet software onto a company-assigned laptop computer, use of web-based email, and the sharing of passwords with co-workers.

Figure 3 shows responses to each threat scenario for the present study (blue line) and the earlier study (red line). Here again the response pattern is very similar for both studies, with the misuse of an insecure USB memory stick at the highest percentage frequency and the turning off of security software at the lowest percentage frequency. The difference between the two annual studies is shown below (green line). As can be seen, all six differences are positive suggesting these security threats may have worsened over time.

Figure 3
Trends = Net change between present and the 2007 study

The difference between the top two line graphs shows the extant experience rate for six scenarios. Rates of change for six scenarios are all positive (see bottom line graph), suggesting experience has increased over two years.

Trends	Present study	2007 study	Change
USB memory stick	61%	51%	10%
Web-based personal email	52%	45%	7%
Downloading Internet software	53%	45%	8%
Loss of mobile data-bearing devices	43%	39%	4%
Turning off security software	21%	17%	4%
Sharing passwords	47%	46%	1%
Social networking in the workplace	31%	NA	NA

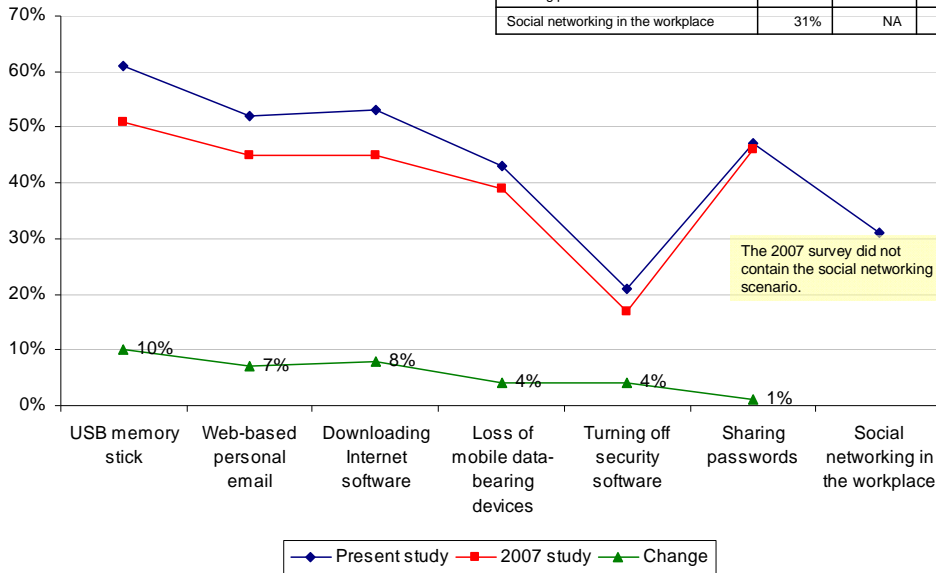
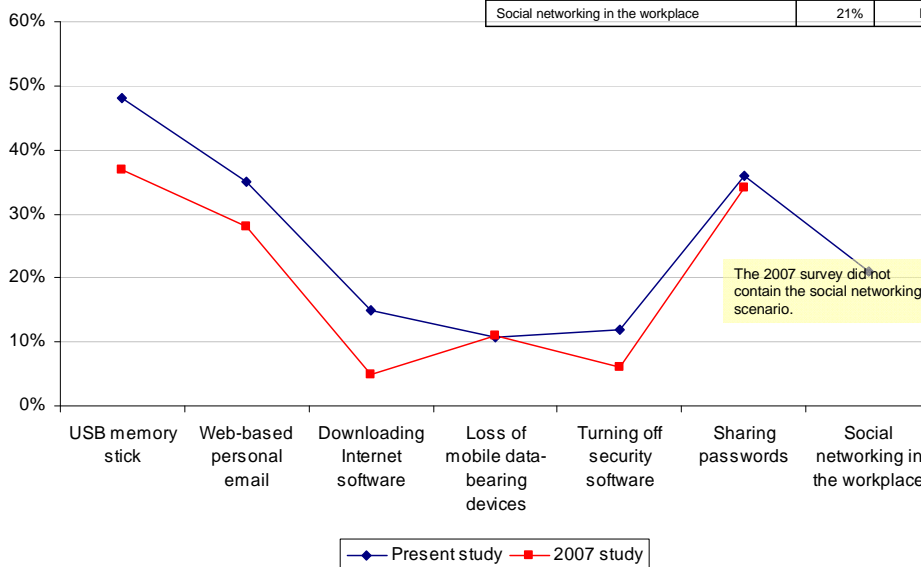


Figure 4 reports the rates of non-compliance for seven threats in the present and earlier studies.

Figure 4
Non-compliance rates for seven security scenarios

The non-compliance rate is defined as the rate of a given behavior (Q. What do you do?) – existence of a policy permitting this behavior.

Scenarios and non-compliance rates	Present study	2007 study
USB memory stick	48%	37%
Web-based personal email	35%	28%
Downloading Internet software	15%	5%
Loss of mobile data-bearing devices	11%	11%
Turning off security software	12%	6%
Sharing passwords	36%	34%
Social networking in the workplace	21%	NA



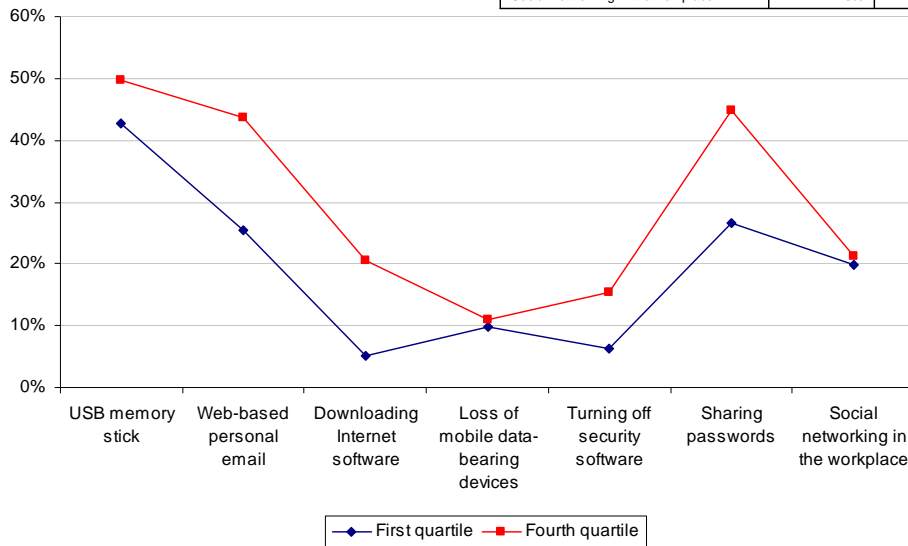
The rate of non-compliance is defined as the extant rate provided by each participant minus the existence of a stated policy that permits this action or behavior. For example, in the present study the extant rate for the transfer of confidential information onto an insecure USB memory stick is 61% (and 51% in the 2007 study). For those who admit they do this, only 13% said their companies have a policy that allows them to engage in this action or behavior.¹ Hence, the non-compliance rate is {61%-13%} = 48% for this scenario. In the 2007 study, we computed the non-compliance using the same method.

The line graph in Figure 4 clearly shows that the non-compliance rate has increased from the 2007 study in almost every scenario except the loss of mobile data-bearing devices. The highest rate of non-compliance appears to be the use of insecure USB memory sticks and the sharing of passwords with co-workers.

Figure 5 reports the non-compliance rate for two quartiles of the present study's sample of respondents. As mentioned in Figure 1, an index value from three attributions was used to rank order all 967 respondents from highest to lowest. Quartiles were then used to place respondents into one of four separate sub-samples of 281 or 282 individuals. Only the first (blue line or most favorable attitude) and fourth (red line or least favorable attitude) quartile results are included in the following line graph for comparison purposes.

Figure 5
Analysis of non-compliance rates for first and fourth quartiles sub-samples

Scenarios and non-compliance rates	First quartile	Fourth quartile
USB memory stick	43%	50%
Web-based personal email	25%	44%
Downloading Internet software	5%	20%
Loss of mobile data-bearing devices	10%	11%
Turning off security software	6%	15%
Sharing passwords	27%	45%
Social networking in the workplace	20%	21%



The above line graph clearly shows that the fourth quartile results for non-compliance with a company's security policy is higher in all but one case than first quartile results. This suggests the importance of the respondent's attitude or view of the company on compliance behavior.

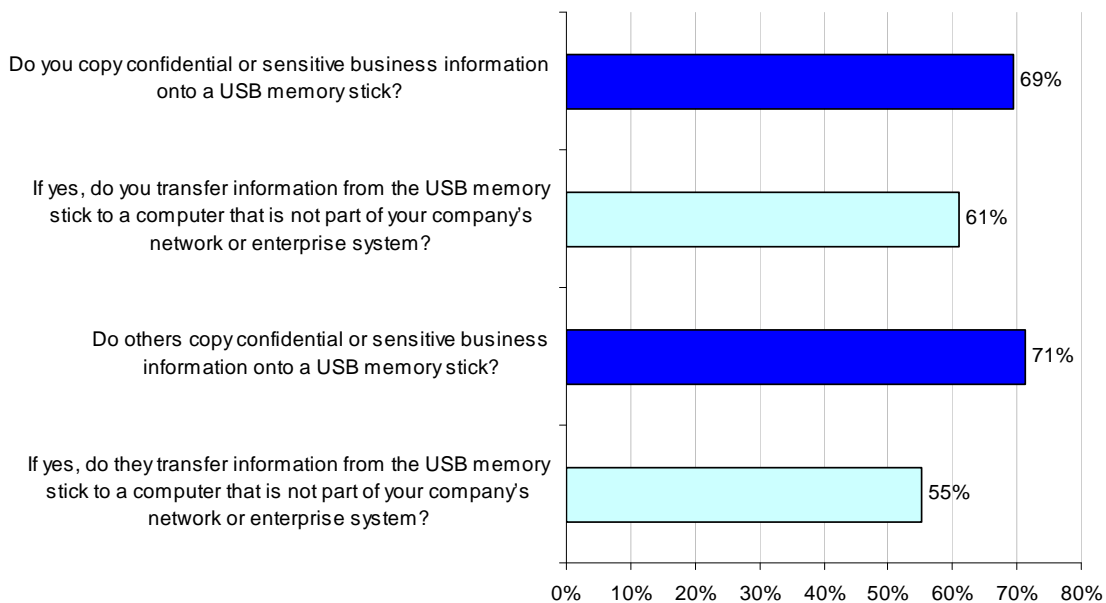
The next section provides more detail about compliance with each one of the seven security threat scenarios included in our present study.

¹ The information collected in this survey is self-assessed by each respondent. The researcher was unable to validate these self-reported results used to construct the non-compliance rates for each scenario.

Transferring confidential business data on insecure USB memory sticks

USB memory sticks are often used to copy confidential or sensitive business information and transfer it to another computer that is not part of the company's network or enterprise system. As noted in Bar Chart 1, 69% of respondents transfer confidential or sensitive business information onto a USB memory stick, and 61% of those in this group admit to transferring information onto a computer that is not part of their company's approved network or enterprise system.

Bar Chart 1: Percentage Yes response



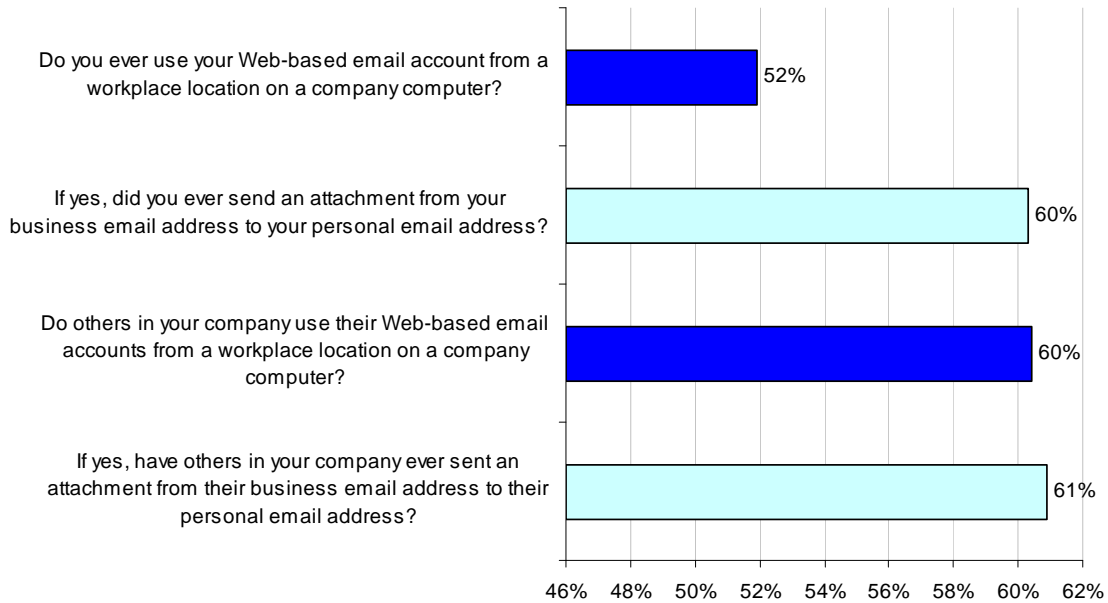
According to 71% of the respondents, others in the organization copy sensitive information and more than half (55%) believe that others transfer information from the USB memory stick to a computer that is not part of the company's network or enterprise system. As already noted in Figure 4, the non-compliance rate increased 11% from 37% in 2007 to 48% in this study.

Use of web-based personal email in the workplace

In the present study, only 17% of respondents say their companies permit employees to access their web-based email accounts from the workplace on company-assigned computers. However, as noted in Bar Chart 2, over 52% state they have accessed their web-based email accounts from work, and 60% believe that others in their organization routinely use or access their web-based email accounts from their workplace computers. As shown previously in Figure 4, the non-compliance rate has increased from 28% to 35% in the present study.

In essence, web-based email accounts are inherently insecure, exacerbating data security risks and other related vulnerabilities. For example, outbound emails containing business confidential attachments – such as customer lists, employee records, and so forth – can be transferred without a company's detection. In addition, incoming web-based emails often bypass a company's spam filters or anti-virus tools – thus permitting insidious software downloads such as worms and Trojans that aim to infiltrate corporate networks.

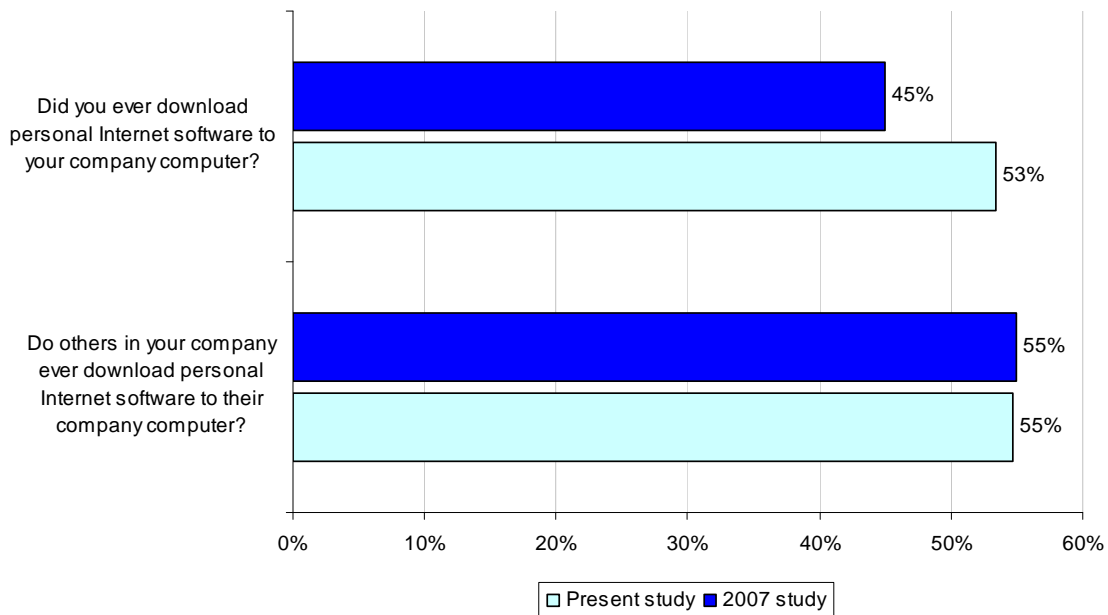
Bar Chart 2: Percentage Yes response



Downloading Internet software

Bar Chart 3 shows 53% of respondents admitting to downloading personal software on a workplace computer, and 55% believe others do the same.

Bar Chart 3: Percentage Yes Response

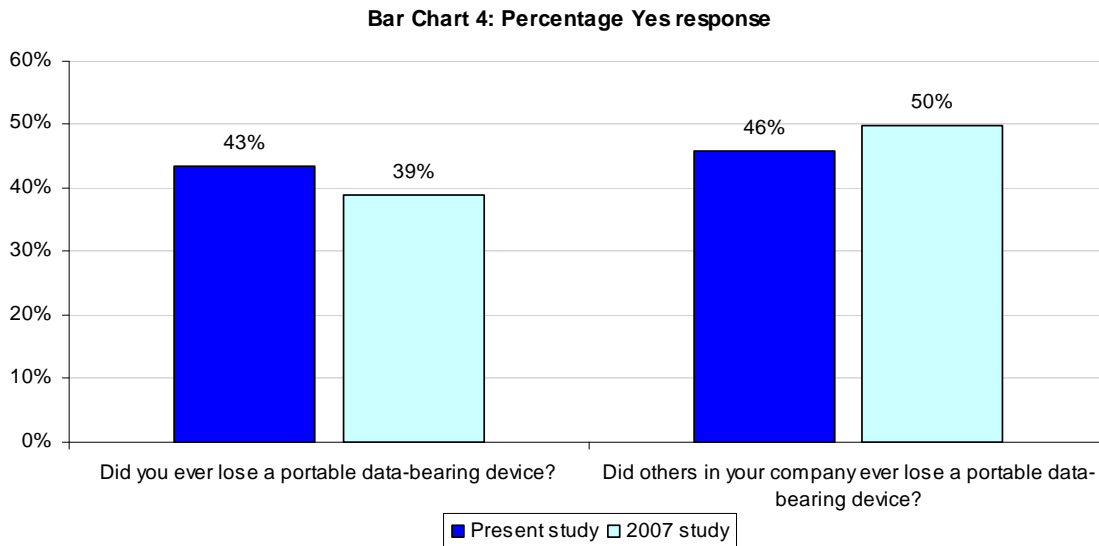


This finding is potentially serious for companies, especially if it involves peer-to-peer file sharing applications that have been shown, in some instances, to create opportunities for data loss or theft. It is interesting to note that the percentage of respondents downloading Internet software has increased from the 2007 study. The number of companies permitting downloads has

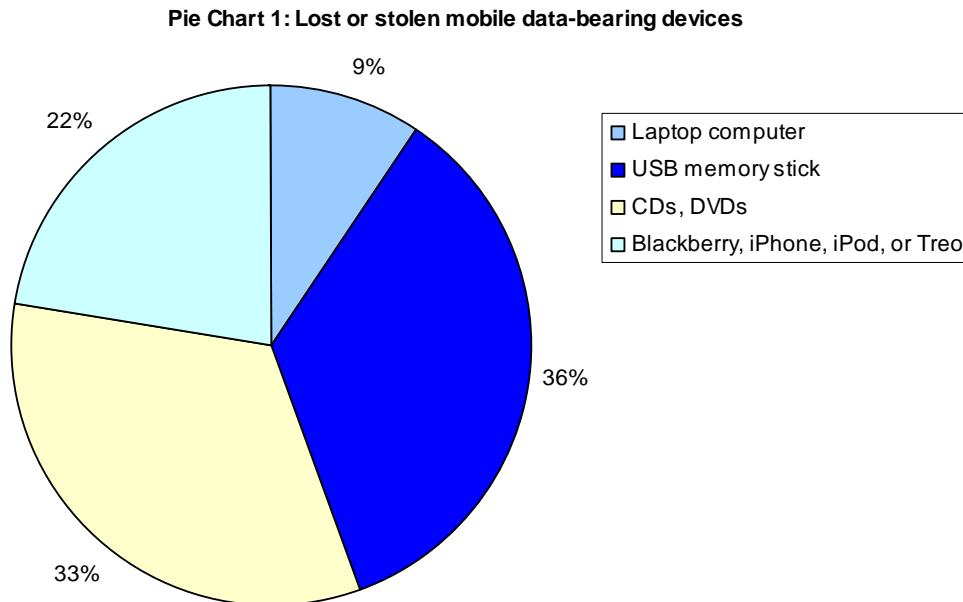
decreased from 40% to 38%. Thirty-seven percent say their organization does not have a policy about this issue. As shown in Figure 4, the non-compliance rate has increased from 5% in 2007 to 15% in this study because more companies are starting to forbid the downloading of Internet software in policy and procedures.

Loss of data-bearing devices

As reported in Bar Chart 4, more than 43% of respondents admit they have lost or had stolen a portable data-bearing device such as a USB memory stick, CD/DVD, PDA, or laptop computer that contained sensitive or confidential information at some point in the recent past. Over 46% of respondents also believe that others within their company have experienced the loss or theft of a portable storage device.

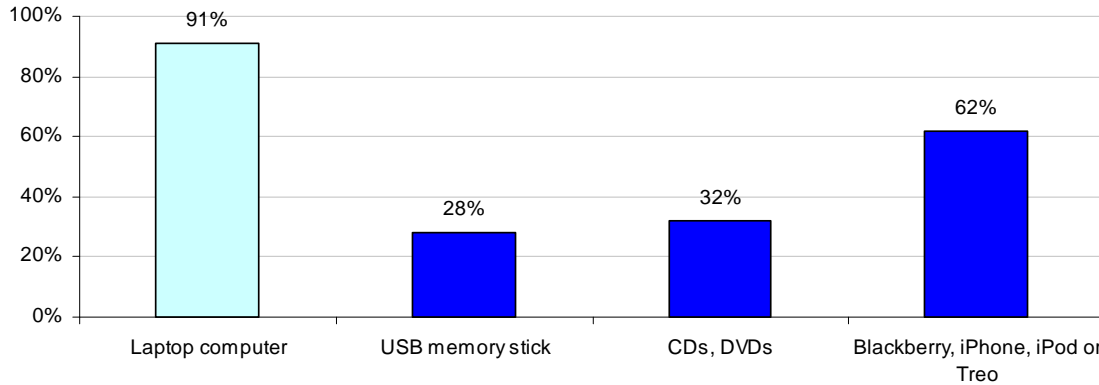


Pie Chart 1 reports the most frequently cited lost, stolen or misplaced portable storage devices by respondents in our study.



Awareness about company procedures for reporting the loss of a mobile data-bearing device has increased from 24% in the previous study to 40%. Despite this awareness, 40% did not follow procedures and never reported this loss to their supervisor or other appropriate people. As shown in Bar Chart 5, reporting rates of lost or stolen laptops is highest (91%) as opposed to USB memory sticks at (28%).

Bar Chart 5: Percentage of respondents who reported the loss

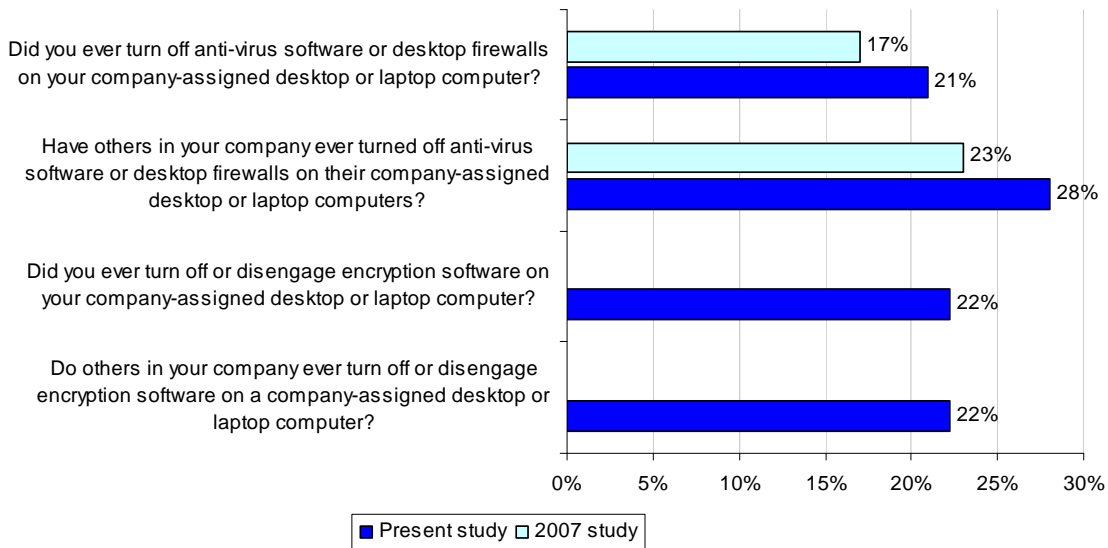


When asked if an employee lost a mobile device, how long it would take the company to determine the type and quantity of data at rest on the missing device, 44% said never. This is an improvement over the 2007 study, in which 57% stated that the lost data would never be known to the company.

Turning off security settings on personal computers in the workplace

Bar Chart 6 shows that a small percentage of respondents (21%) admit they turn off (change or manipulate) their anti-virus software settings or client firewalls – for example, to expedite the receipt of inbound emails or to gain access to Internet portals that may be marked as off-limits.

Bar Chart 6: Percentage Yes response

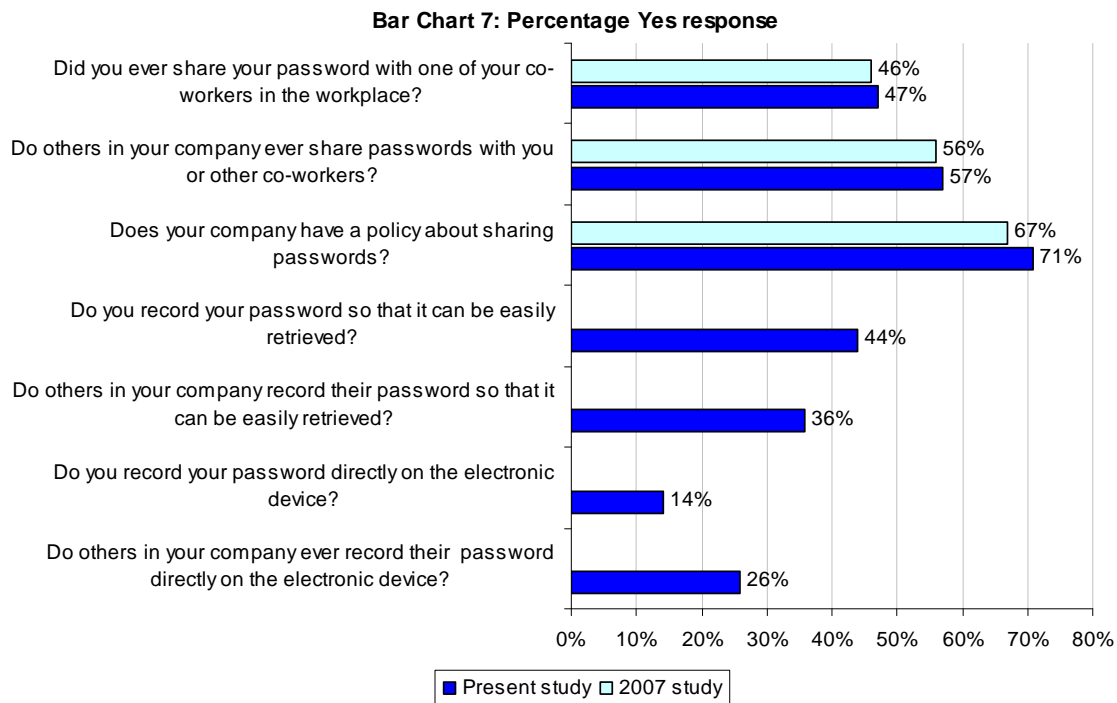


Also, a small percentage of respondents (28%) say others turn off their anti-virus software settings or desktop firewalls. And 22% say they have turned off or disengaged encryption

software. Only 9% say their company permits respondents to disengage security software such as anti-virus, desktop firewalls, or encryption.

Sharing passwords in the workplace

A persistent and serious security threat in the workplace is the sharing of passwords among employees, temporary employees, and contractors.



According to Bar Chart 7, 47% of respondents admit they share passwords with co-workers, and 57% believe others in their organizations routinely share their passwords too. Over 71% admit that their company has a policy about sharing passwords, and only 11% report that the company permits password sharing. In the 2007 study, 12% said that their company permits sharing of passwords. The non-compliance rate in the password sharing category increased slightly from 34% in 2007 to 36%.

Use of public social networks in the workplace

In this year's study we asked respondents about the risk of sharing confidential or sensitive company information with other participants in a social network as well as surreptitious downloads including malware attacks. Only 10% of respondents say that their organization has a policy about social networking and, as reported in Bar Chart 8, 31% say they use or access social networking sites such as Facebook or MySpace in the workplace. The same percentage says that others in the organization use Facebook or MySpace.

Thirty-four percent of those who responded yes to the use of social networking have also shared information about their company. These respondents also believe that 71% of others in the organization who access social networks have shared company information on such sites as Facebook, MySpace, Twitter, LinkedIn, and others.

Bar Chart 8: Percentage Yes response

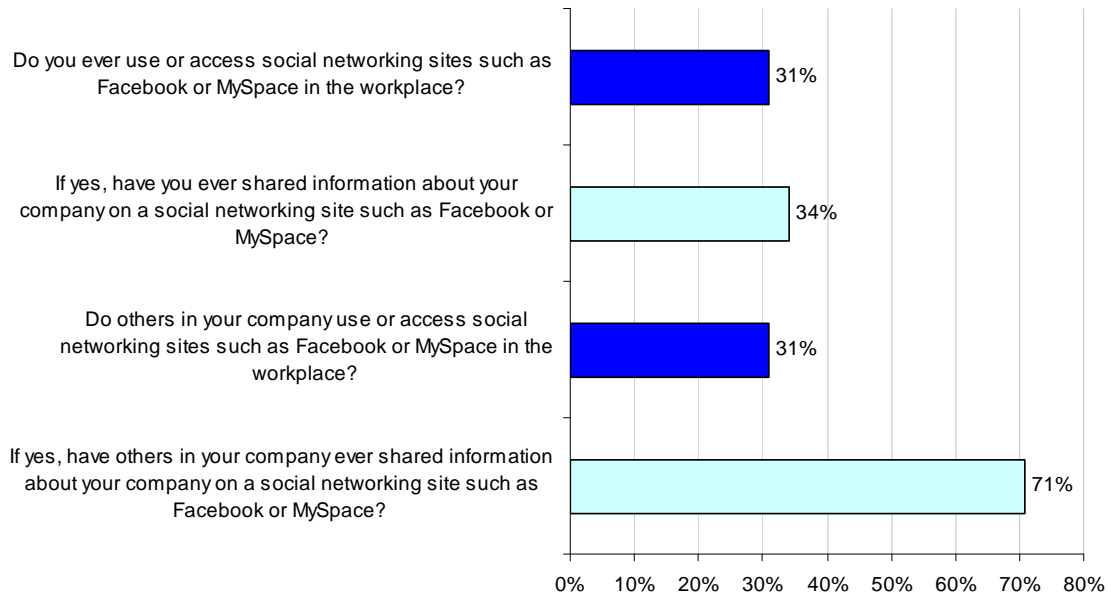


Table 1 summarizes the extrapolated non-compliance rates for seven data security scenarios in our study. While these scenarios are not intended to be an exhaustive list of workplace data security threats, it is clear that a large number of respondents admit to behaviors that are risky for their organizations and, hence, are very likely to violate data security policy or procedure.

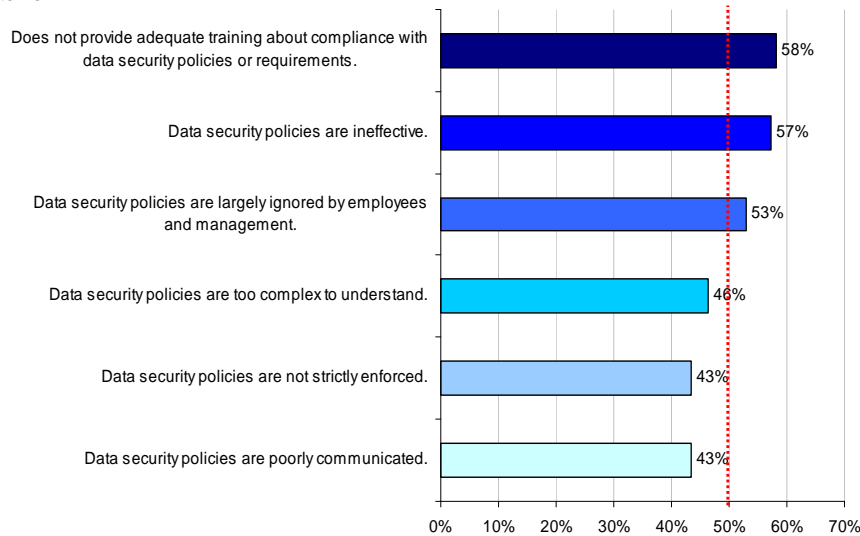
Table 1: Seven survey scenarios	Experience rates in 2009	Compliance with data security policy
Copying confidential information onto USB memory stick	61% say they do it	87% believe that policy forbids it
Accessing web-based email accounts from workplace computer	52% say they do it	74% believe there is no stated policy that forbids it
Losing a portable data-bearing device	43% say they lost a portable data-bearing device	72% did not report a lost or missing device immediately
Downloading Internet software	53% say they do it	60% believe there is no stated policy that forbids it
Turning off security software	21% say they do it	71% believe there is no stated policy that forbids it
Sharing passwords with co-workers	47% say they do it	71% believe the company's policy forbids it
Using public social networks in the workplace	31% say they do it	84% believe this is no stated policy that forbids it

Figure 6 summarizes the strongly agree and agree response to six attributions about the respondent company's data security policies. As can be seen, a large percentage of respondents believe their company's data security policies are ineffective (57%), largely ignored (53%), too complex (46%), not strictly enforced (43%), and poorly communicated (43%). More than 58% admit they did not receive adequate training to comply with the company's data security policy or requirements.

Figure 6 Attributions about the respondent company's data security policies

Each bar shows the percentage of strongly agree and agree combined. The dotted red line provides the average response for all six items.

A five-point adjective scale ranging from strongly agree to strongly disagree was used to capture responses.



Caveats to this study

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.

Sample

A random sampling frame of 17,021 adult-aged individuals who reside within the United States was used to recruit participants to this survey. Our randomly selected sampling frame was selected from national lists of employees. Screening criteria were used to ensure only employees who are assigned a company laptop or desktop computer were included in the final sample.

In total, 1,102 respondents completed their survey within an eight-day holdout period. Of returned instruments, 135 survey forms failed reliability checks. A total of 967 surveys were used as our final sample. This sample represents a 5.7% net response rate. The margin of error on all adjective scale and Yes/No/Unsure responses is less than 5%.

Table 2: Sample description	Freq.
Sampling frame	17,021
Bounce back	2,315
Total sample	1,102
Rejections	135
Final sample	967
Response rate	5.7%

Over 90% of respondents completed all survey items within 15 minutes. Following are key demographics and organizational characteristics for respondents. Table 3a reports the respondent's employment status. Table 3b provides the self-reported organizational level of respondents. As can be seen, the largest segment of respondents are associate, staff, or other rank-and-file positions.

Table 3a. Employment status	Pct%
Full-time employee	71%
Part-time employee	12%
Owner/partner of business	8%
Independent contractor	8%
Other	0%
Total	100%

Table 3b. Organizational level that best describes current position	Pct%
Executive	1%
Vice President	3%
Director	9%
Manager	16%
Supervisor	12%
Administrative	10%
Associate, staff, and below	48%
Total	100%

On average, respondents have more than five years of work-related experience and almost three years of experience in their current position. In total, 51% of respondents are female and 49% male.

Pie Chart 2 reports the percentage distribution of respondents by major industry sector. As shown below, 17% of respondents work for financial service companies such as banks, insurance, credit card, brokerage, and others. Over 14% of respondents are employed in federal, state, or local governmental organizations. Another 9% are employed in healthcare and pharmaceuticals or manufacturing companies.

Pie Chart 2: Industry distribution

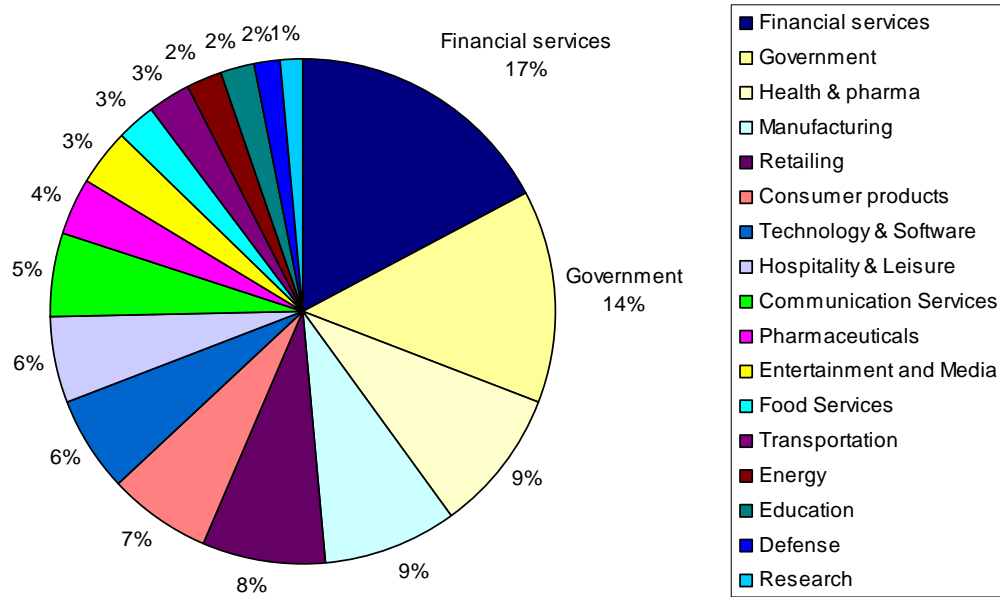


Table 4a reports the location of respondents according to six geographical regions. Table 4b provides the approximate headcounts of these organizations. As can be seen, over 52% of respondents are employed by larger-sized organizations (with more than 5,000 employees).

Table 4a. Region of the United States	Pct%
Northeast	19%
Mid-Atlantic	18%
Midwest	17%
Southeast	13%
Southwest	14%
Pacific	19%
Total	100%

Table 4b. Worldwide headcount	Pct%
Less than 500 people	8%
500 to 1,000 people	13%
1,001 to 5,000 people	27%
5,001 to 25,000 people	26%
25,001 to 75,000 people	14%
More than 75,000 people	12%
Total	100%

Implications

In our previous study, we noted that there was a critical need for organizations to address and mitigate serious threats resulting from employees’ non-compliance with organizational security policies. Two years later, we find that many organizations are still not doing basic “blocking and tackling” such as training employees to reduce data protection or privacy threats. We suggest the following five areas for improvement:

- Create a security conscious culture among employees, temporary employees, and contractors. This can be accomplished, at least in part, by more effective security leadership.
- Strengthen existing policies, especially in areas of emerging technology such as mobile devices and the use of social media in the workplace.
- Enforce non-compliance with stated policies and establish clear accountability for security and data protection practices.

- Establish training activities for all employees as part of an enterprise-wide data security awareness program.
- Monitor basic security practices and procedures conducted by employees in the business environment.

In conclusion, we believe creating policies to address the vulnerabilities described in our study, strengthening existing policies, and training insiders to comply with these policies should be a priority for organizations seeking to reduce their risk to the theft or loss of sensitive information.

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

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.

Appendix: Responses to Survey Questions

Audited results prepared by Dr. Larry Ponemon, May 1, 2009

The following tables provide the frequency and percentage frequency of survey responses from a panel of individuals who are employed in the United States. Whenever possible, we compare current survey results with findings completed in an earlier study (June 2007).

The new results are in the column labeled Pct%. The earlier results are in an adjacent column labeled FY2007. A gray column indicates this question was not included in the 2007 study and, hence, no direct comparison can be made.

Sample description	Freq.
Sampling frame	17,021
Bounce back	2,315
Total sample	1,102
Rejections	135
Final sample	967
Response rate	5.7%

Attributions about your company 1=Strongly agree, 2=Agree, 3=Unsure, 4=Disagree, 5=Strongly disagree	1+2	1	2	3	4	5
Q1a. My company has adequate data protection policies and procedures.	42%	17%	25%	30%	15%	13%
Q1b. My company has adequate technologies such as encryption and data loss protection solutions to protect data.	37%	17%	20%	25%	16%	21%
Q1c. My company is a socially responsible organization.	33%	12%	21%	33%	22%	12%
Q1d. My company takes appropriate steps to protect privacy rights.	38%	8%	30%	46%	6%	10%
Q1e. My company treats me and other employees with respect.	50%	20%	30%	21%	22%	7%
Q1f. My company treats our customers with respect.	62%	24%	39%	18%	14%	6%
Q1g. My company's senior leadership manages with integrity.	48%	17%	32%	34%	11%	7%
Q1h. My company has ample resources to protect sensitive or confidential information.	39%	15%	24%	24%	20%	17%

Q2. Use of USB Memory Sticks

Q2a. Do you ever copy confidential or sensitive business information such as private documents or spreadsheets containing sensitive or confidential business information from your desktop or laptop computer to a USB memory stick?	Pct%	
Yes	69%	
No	31%	
Total	100%	

Q2b. If yes, do you ever transfer information from the USB memory stick to another computer that is not part of your company's network or enterprise system (such as your private laptop, PDA, or home computer)?	Pct%	FY2007
Yes	61%	51%
No	39%	49%
Total	100%	100%

Q2c. Do others in your company copy confidential or sensitive business information such as private documents or spreadsheets containing customer or employee records from their desktop or laptop computer to a USB memory stick?	Pct%	FY2007
Yes	71%	57%
No	20%	27%
Can't determine	9%	16%
Total	100%	100%

Q2d. If yes, do others in your company transfer information from the USB memory stick to another computer that is not part of your company's network or enterprise system (such as your private laptop, PDA, or home computer)?	Pct%	
Yes	55%	
No	45%	
Total	100%	

Q2e. Does your company's policy permit you to copy sensitive business information onto a USB memory stick?	Pct%	FY2007
Yes	14%	13%
Yes, but only if encrypted	23%	23%
No	34%	32%
Our company does not have a policy that covers this issue	23%	22%
Don't know	7%	11%
Total	100%	100%

Q3. Web-based Personal Email

Q3a. Do you ever use your web-based email account from a workplace location and company-assigned computer?	Pct%	FY2007
Yes	52%	45%
No	48%	55%
Total	100%	100%

Q3b. If yes, did you ever send a document or spreadsheet attachment from your business email address to your personal email address?	Pct%	
Yes	60%	
No	40%	
Total	100%	

Q3c. Do others in your company use their web-based email accounts from a workplace location and company-assigned computer?	Pct%	FY2007
Yes	60%	40%
No	40%	60%
Total	100%	100%

Q3d. If yes, have others in your company ever sent a document or spreadsheet attachment from their business email address to their personal email address?	Pct%	
Yes	61%	
No	22%	
Can't determine	18%	
Total	100%	

Q3e. Does your company's policy permit you to use your web-based email account in the workplace?	Pct%	FY2007
Yes	17%	17%
No	36%	38%
Our company does not have a policy that covers this issue	25%	23%
Don't know	22%	23%
Total	100%	100%

Q4. Downloading Internet Software

Q4a. Did you ever download personal Internet software applications such as music players or widgets to your company-assigned desktop or laptop computer?	Pct%	FY2007
Yes	53%	45%
No	47%	55%
Total	100%	100%

Q4b. Do others in your company ever download personal Internet software to their company-assigned desktop or laptop computer?	Pct%	FY2007
Yes	55%	48%
No	38%	40%
Can't determine	7%	12%
Total	100%	100%

Q4c. Does your company's data security policy permit you to download personal Internet software onto your company-assigned desktop or laptop computer?	Pct%	FY2007
Yes	38%	40%
No	22%	21%
Our company does not have a policy about this issue	37%	
Don't know	3%	39%
Total	100%	100%

Q5. Loss of Mobile Data-bearing Devices

Q5a. Did you ever lose a PDA, cellular phone, memory stick, zip drive, or laptop computer that contained unprotected confidential or sensitive business information such as private documents or spreadsheets containing sensitive or confidential business information?	Pct%	FY2007
Yes	43%	39%
No	57%	61%
Total	100%	100%

Q5b. If yes, what kind(s) of portable or mobile data-bearing device did you lose? For each device selected, please check if it was lost or stolen. Or, select "unsure" if you were unable to determine the cause.	Lost	Stolen	Unsure
Laptop computer	5%	4%	2%
Flash drive (USB memory stick)	33%	2%	5%
CDs, DVDs	31%	2%	3%
Blackberry, iPhone, iPod, Treo	20%	3%	7%
Other	1%	2%	0%
Total	91%	13%	18%

Q5c For each data-bearing device listed above, please provide the <u>approximate</u> number of portable or mobile devices lost or stolen in your company each year.	Less than 10	10 to 100	100 to 500	More than 500	Total
Laptop computer	46%	47%	7%	0%	100%
Flash drive (USB memory stick)	16%	21%	35%	28%	100%
CDs, DVDs	11%	28%	35%	26%	100%
Blackberry, iPhone, iPod, Palm Pilot, Treo	33%	40%	23%	4%	100%
Other	53%	39%	9%	0%	100%
Total	159%	175%	109%	57%	

Q5d. If yes (to Q5a), did you report this loss to your supervisor or other appropriate people within your company?	Pct%	FY2007
Yes, immediately	25%	28%
Yes, but I waited a few days	35%	34%
No	40%	38%
Total	100%	100%

Q5e. Have others in your company ever lost a PDA, cellular phone, memory stick, or laptop computer that contained unprotected confidential or sensitive business information such as private documents or spreadsheets containing customer or employee records? If yes, did they report this loss to their supervisor or other appropriate people within your company?	Pct%	FY2007
Yes	46%	50%
No	40%	25%
Can't determine	14%	25%
Total	100%	100%

Q5f. If an employee lost a mobile device, how long would it take your company to determine the types of data the device contained?	Pct%	FY2007
Less than an hour	7%	8%
½ day	12%	10%
1 day	9%	5%
Less than a week	10%	5%
Month	5%	4%
More than a month	10%	11%
Never	44%	57%
Total	100%	100%

Q5g. Does your company's policy explain procedures for reporting the loss of a mobile data-bearing device?	Pct%	FY2007
Yes	40%	24%
No	24%	43%
Our company does not have a policy about this issue	17%	
Don't know	19%	33%
Total	100%	100%

Q6. Turning off Security Software

Q6a. Did you ever turn off anti-virus software or desktop firewalls on your company-assigned desktop or laptop computer?	Pct%	FY2007
Yes	21%	17%
No	79%	83%
Total	100%	100%

Q6b. Have others in your company ever turned off anti-virus software or desktop firewalls on their company-assigned desktop or laptop computers?	Pct%	FY2007
Yes	28%	23%
No	30%	29%
Can't determine	42%	48%
Total	100%	100%

Q6c. Did you ever turn off or disengage encryption software on your company-assigned desktop or laptop computer?	Pct%	
Yes	11%	
No	38%	
We don't have encryption software on laptop or desktop computers	51%	
Percentage Yes adjusted for those companies using encryption	22%	
Total	100%	

Q6d. Do others in your company ever turn off or disengage encryption software on a company-assigned desktop or laptop computer?	Pct%	
Yes	11%	
No	25%	
We don't have encryption software on laptop or desktop computers	51%	
Can't determine	13%	
Percentage Yes adjusted for those companies using encryption	22%	
Total	100%	

Q6e. Does your company permit you to turn off or disengage security software such as anti-virus, desktop firewalls, or encryption?	Pct%	
Yes	19%	
No	28%	
Our company does not have a policy about this issue	43%	
Don't know	10%	
Total	100%	

Q7. Sharing Passwords

Q7a. Did you ever share your password with one of your co-workers or a third-party contractor in the workplace?	Pct%	FY2007
Yes	47%	46%
No	53%	54%
Total	100%	100%

Q7b. Do others in your company ever share passwords with you, other co-workers, or a third-party contractor?	Pct%	FY2007
Yes	57%	56%
No	13%	12%
Can't determine	30%	32%
Total	100%	100%

Q7c. Do you record your password so that it can be easily retrieved?	Pct%	
Yes	44%	
No	56%	
Total	100%	

Q7d. Do others in your company record their password so that it can be easily retrieved?	Pct%	
Yes	36%	
No	36%	
Can't determine	28%	
Total	100%	

Q7e. Do you record your password directly on the electronic device?	Pct%	
Yes	14%	
No	86%	
Total	100%	

Q7f. Do others in your company ever record their password directly on the electronic device?	Pct%	
Yes	26%	
No	37%	
Can't determine	28%	
Total	100%	

Q7g. Does your company have a policy about sharing passwords with co-workers or third parties?	Pct%	FY2007
Yes	71%	67%
No	11%	12%
Don't know	18%	21%
Total	100%	100%

Q8. Social Networking in the Workplace

Q8a. Do you ever use or access social networking sites such as Facebook or MySpace in the workplace?	Pct%	
Yes	31%	
No	66%	
Total	100%	

Q8b. If yes, have you ever shared information about your company on a social networking site such as Facebook or MySpace?	Pct%	
Yes	34%	
No	66%	
Total	100%	

Q8c. Do others in your company use or access social networking sites such as Facebook or MySpace in the workplace?	Pct%	
Yes	31%	
No	21%	
Can't determine	48%	
Total	100%	

Q8d. If yes, have others in your company ever shared information about your company on a social networking site such as Facebook or MySpace?	Pct%	
Yes	71%	
No	21%	
Can't determine	8%	
Total	100%	

Q8e. Does your company have a policy that permits you to use social networking sites in the workplace?	Pct%	
Yes	10%	
No	24%	
Our company does not have a policy about this issue	60%	
Don't know	6%	
Total	100%	

How do you feel about your company's security policies? 1=Strongly agree, 2=Agree, 3=Unsure, 4=Disagree, 5=Strongly disagree	1+2	1	2	3	4	5
Q9a. Our company's data security policies are too complex to understand.	46%	10%	37%	32%	13%	9%
Q9b. Our company's data security policies are ineffective.	57%	24%	33%	21%	9%	12%
Q9c. Our company's security policies are poorly communicated.	43%	15%	29%	24%	25%	8%
Q9d. Our company does not provide adequate training about compliance with data security policies or requirements.	58%	29%	29%	14%	12%	16%
Q9e. Our company's data security policies are not strictly enforced.	43%	17%	26%	22%	14%	21%
Q9f. Our company's data security policies are largely ignored by employees and management.	53%	23%	30%	20%	5%	22%

Respondents' organization characteristics and demographics

Q10. Please check your age range	Pct%
Between 18 to 25 years	12%
Between 26 to 35 years	29%
Between 36 to 45 years	21%
Between 46 to 55 years	18%
Between 56 to 65 years	9%
Between 66 to 75 years	9%
Over 75 years	1%
Total	100%

Q11. Over the past year, how many hours each week did you spend at work?	Pct%
20 hours or less	2%
20-40 hours	22%
40-50 hours	67%
More than 50 hours	8%
Total	100%

Q12. What organizational level best describes your current position?	Pct%
Executive	1%
Vice President	3%
Director	9%
Manager	16%
Supervisor	12%
Administrative	10%
Associate and below	48%
Total	100%

Q13. What is your highest level of education attained?	Pct%
High School	22%
Vocational	20%
University (4 yr. degree)	38%
Attending Graduate	11%
Post Graduate (Master's)	9%
Doctorate (PhD, MD, JD)	1%
Total	100%

Q14. What best describes your employment status today?	Pct%
Full-time employee	71%
Part-time employee	12%
Owner/partner of business	8%
Independent contractor	8%
Other	0%
Total	100%

Q15. Approximately, what is your household income?	Pct%
Less than \$20,000	11%
\$20,000 to \$40,000	15%
\$41,000 to \$60,000	29%
\$61,000 to \$80,000	11%
\$81,000 to \$100,000	15%
\$101,000 to \$150,000	8%
\$151,000 to \$200,000	7%
\$201,000+	3%
Total	100%

Q16. Does your employer provide a workplace computer?	Pct%
Yes	96%
No	4%
Total	100%

Q17. Gender	Pct%
Female	51%
Male	49%
Total	100%

Q18. Region of the United States	Pct%
Northeast	19%
Mid-Atlantic	18%
Midwest	17%
Southeast	13%
Southwest	14%
Pacific	19%
Total	100%

Q19. What industry best describes your organization's industry focus?	Pct%
Financial services	17%
Government	14%
Health & pharma	9%
Manufacturing	9%
Retailing	8%
Consumer products	7%
Technology & Software	6%
Hospitality & Leisure	6%
Communication Services	5%
Pharmaceuticals	4%
Entertainment and Media	3%
Food Services	3%
Transportation	3%
Energy	2%
Education	2%
Defense	2%
Research	1%
Total	100%

Q20. How often do you work remotely each week (approximately)?	Pct%
Never	18%
Less than an hour each week	5%
About ½ day each week	21%
About 1 day each week	26%
About 2 to 3 days each week	19%
Most of the time	11%
Total	100%

Q21. What is the worldwide headcount of your organization?	Pct%
Less than 500 people	8%
500 to 1,000 people	13%
1,001 to 5,000 people	27%
5,001 to 25,000 people	26%
25,001 to 75,000 people	14%
More than 75,000 people	12%
Total	100%