Data Loss Risks During Downsizing

As Employees Exit, so does Corporate Data

Independently conducted by Ponemon Institute LLC

Publication Date: February 23, 2009

Sponsored by Symantec Corporation

Data Loss Risks During Downsizing

As Employees Exit so Does the Corporate Data

Presented by Dr. Larry Ponemon, February 23, 2009

Executive Summary

Whether they are losing their jobs because of the current recession or simply looking for better opportunities, there are significant numbers of people exiting their current position. In addition to the HR issues, companies should be aware of the possibility that these employees may be walking off with their sensitive and confidential data. This type of data loss problem may be putting companies at risk for a potential data breach. Moreover stealing proprietary data, such as customer lists, can put the company at a competitive disadvantage.

Sponsored by Symantec, Ponemon Institute independently conducted this national study entitled, *Data Loss Risks During Downsizing* to understand what employees are doing with the data on the laptops their employers provided them. According to our findings, 59% of employees who leave or are asked to leave are stealing company data. Moreover, 79% of these respondents admit that their former employer did not permit them to leave with company data.

Our study reveals that companies are doing a very poor job at preventing former employees from stealing data. Only 15% of respondents' companies review or perform an audit of the paper and/or electronic documents employees are taking. If they conduct a review, 45% say it was not complete and 29% say it was superficial.

It is also surprising to learn that 67% of respondents used their former company's confidential, sensitive or proprietary information to leverage a new job. Approximately 68% are planning to use such information as email lists, customer contact lists and employee records that they stole from their employer. Not only is this putting customer and other confidential information at risk for a data breach but it could affect companies' competitiveness and future revenues.

The survey focused on the following issues:

- Do laid-off or terminated employees keep sensitive or confidential information? If so, how pervasive is this problem?
- If they do take the data, how do they justify their actions?
- What types of data or information is most susceptible to employee theft?
- What can organizations do to protect themselves from this issue?

We surveyed 945 adult-aged participants located in the US who were laid-off, fired or changed jobs in the last 12 months. All participants were assigned a desktop or laptop computer for their use in the workplace and had access and use of proprietary information such as customer data, contact lists, employee records, financial reports, confidential business documents, software tools or other intellectual property. The overall demographics for respondents are summarized at the conclusion of this report.

Implications and recommendations for companies

All companies share the potential risk of having a data breach because of the actions of former employees. In addition, they have allowed competitive information about customers, business partners and other intellectual property to walk out the door putting them at a competitive disadvantage. We recommend that companies immediately assess the potential data loss from former employees who had access to sensitive and confidential data as part of their job.

Other recommendations to implement immediately include the following:

- Ensure that policies and procedures clearly state former employees will no longer have access to sensitive and confidential information they used in their jobs. This includes information on laptops, other data-bearing devices and paper documents. The policy should outline what information is considered sensitive and proprietary.

- As part of the exit interview, the supervisor/business unit manager and/or someone from IT security should conduct a thorough review and audit of the employee's paper and electronic documents. This includes checking electronic devices as well as paper documents.

- Prior to the employee leaving, companies should monitor the employee's access to the network or system to make sure sensitive and confidential data is not being downloaded or send to the employee's personal email account.

- Steps should be taken to ensure that the former employee is not able to access the company's network or system once the relationship has been terminated.

- Extra precautions should be taken with former employees who have been asked to leave and/or are disgruntled. As our study reveals, employees who have unfavorable views of the employer are far more likely to steal data.

These recommendations should be incorporated into all procedures involving employees who are leaving their companies. Doing so will address a significant risk facing companies during a time when so many people are exiting their jobs.

Key Findings

Following are the most salient findings of this survey research. Please note that most of the results are displayed in bar chart format. 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.

Employees are stealing data and are more likely to do so when they don't trust their employer. According to 63% of respondents, their previous job required them to access and use proprietary information such as customer data, contact lists, employee records, financial reports, confidential business documents, software tools or other intellectual properties. More than 59% report that they kept company data after leaving their employer. It is very interesting to note that employees who do not trust their former employer to act with integrity and fairness are more likely to take the data. Sixty-one percent of respondents who were negative about the company took data while only 26% of those with a favorable view took data.

Employees are stealing proprietary and confidential data that might affect their former company's business competitiveness and could result in a data breach. Sixty-five percent of those respondents who admit they took data left with email lists followed by 45% who took non-financial business information and 39% took customer information, including contact lists.

The most susceptible documents to theft are email lists and hardcopy files. Sixty-four percent of respondents took email history and hardcopy files (62%). Of least interest to employees are PDF files (9%), access database files (8%) and source code (3%).

Employees are stealing data in different ways. It is interesting that most employees (61%) who stole valuable customer and other business information are taking it in the form of paper documents or hard files. The next most popular means of transferring data is by downloading information onto a CD or DVD (53%) or onto a USB memory stick (42%) followed by sending documents as attachments to a personal email account (38%).

Employees who take company data are defying company rules. Of those employees who admit to stealing company information, 79% report they do not have permission to do so and 5% are unsure. The top reasons given for stealing data include: "everyone else is doing it, the information may be useful to me in the future, I was instrumental in creating this information, the company can't trace the information back to me and the company does not deserve to keep this information."

Only 16% say they were permitted to keep sensitive, confidential or proprietary information. However, their reasons are suspect. Specifically, the top two reasons for their belief that it was acceptable are "other laid-off employees kept this information when they left the company (54%) and no one checked their belongings when they left the company (50%)." Only 11% report that their former supervisor said it was permissible to keep this information.

Companies are failing to take proper steps to stop data theft. While a small number (4%) of employees told their employers that they were taking data, only 15% of companies conducted a review or performed an audit of the paper and/or electronic documents that employees were taken. If they did, respondents report that it was not complete (45%), or worse, superficial (29%). Approximately 41% of respondents say the review was conducted by their direct supervisor or manager followed by the human resources personnel. Approximately 89% report that their company did not do an electronic scan of devices such a portable data-bearing equipment or USB memory sticks.

Employees leave their laptops but take CDs, USB memory sticks and PDAs. Ninety-two percent of employees took CDs/DVDs followed by USB memory sticks (73%) and PDAs (17%). Only 9% kept their Blackberry and 3% kept their laptops.

Employees were able to access their former employer's computer system or network after departure. According to 24% of respondents, their ability to access data continued after they left the company creating a data security risk. Of these respondents, 32% say that they accessed the system and their credentials worked and 38% say their co-workers told them that their access rights continued. In the case of 35% of the respondents, access to the system continued one week or longer.

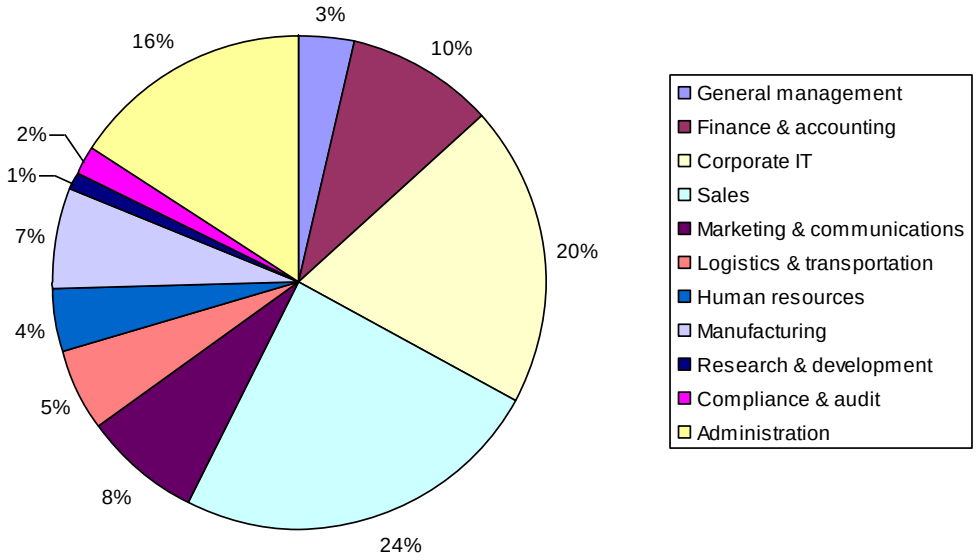
While only 4% report that they gained access using a co-worker's authentication credentials after departure from the company, 51% said their supervisor told them they would have access to the company's system, email or network for a specified period of time. More than 44% continued to receive email on their company's account.

Employees' reasons for leaving are mixed. Approximately 37% were asked to leave, 38% found a new job and 21% moved on because they are anticipating a layoff. Immediately after leaving their former company, 61% took paper documents or hard files, 53% downloaded information onto a CD or DVD and 42% downloaded information onto a USB memory stick.

Detailed Findings

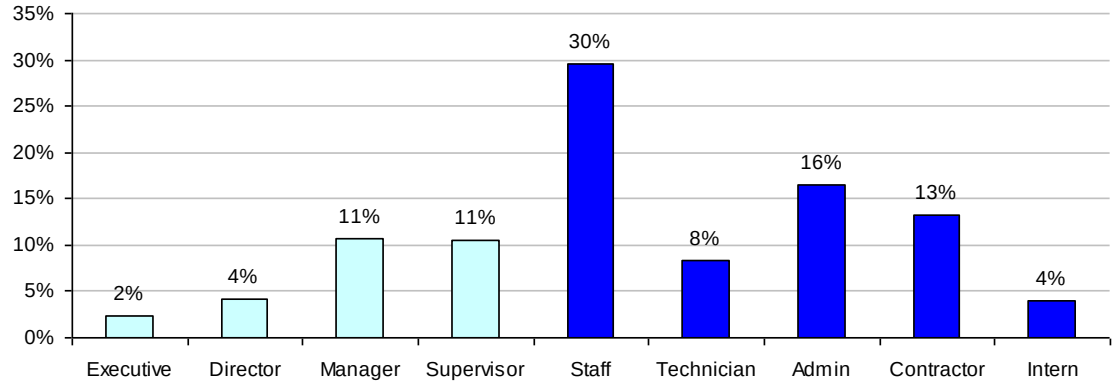
Pie Chart 1 shows the respondent's role, function or departmental affiliation at the previous employers. As can be seen, the largest segments are sales (24%), corporate IT (20%) and general administration (16%).

Pie Chart 1
Department or function that defines respondent's role at previous employer



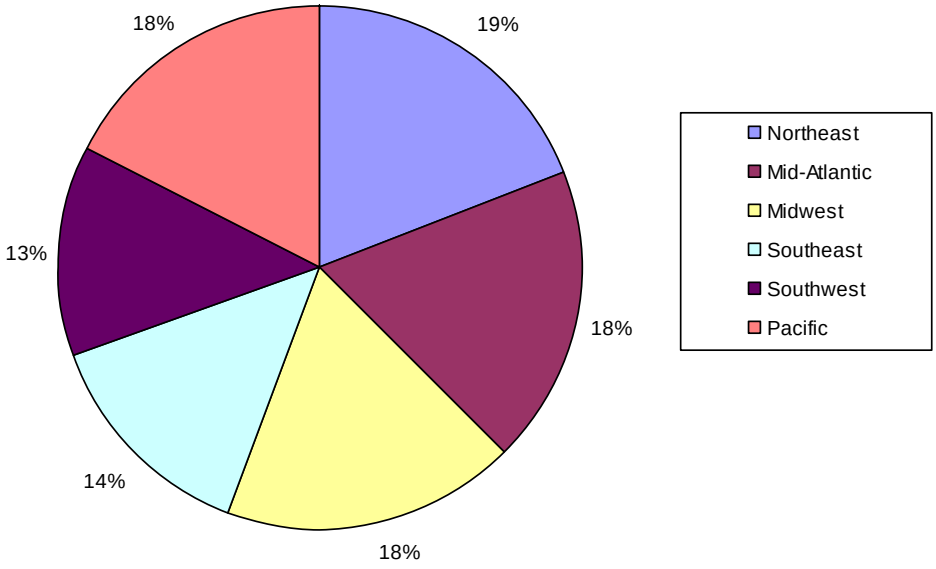
Bar Chart 1 reports the organizational levels of respondents at their previous job. As can be seen, 28% of respondents were in management or supervisory positions. Another 30% define themselves as staff level employees.

Bar Chart 1
What organizational level best describes the respondent's previous position?
Average job experience = 8.11 years. Average time at previous employe = 2.87 years



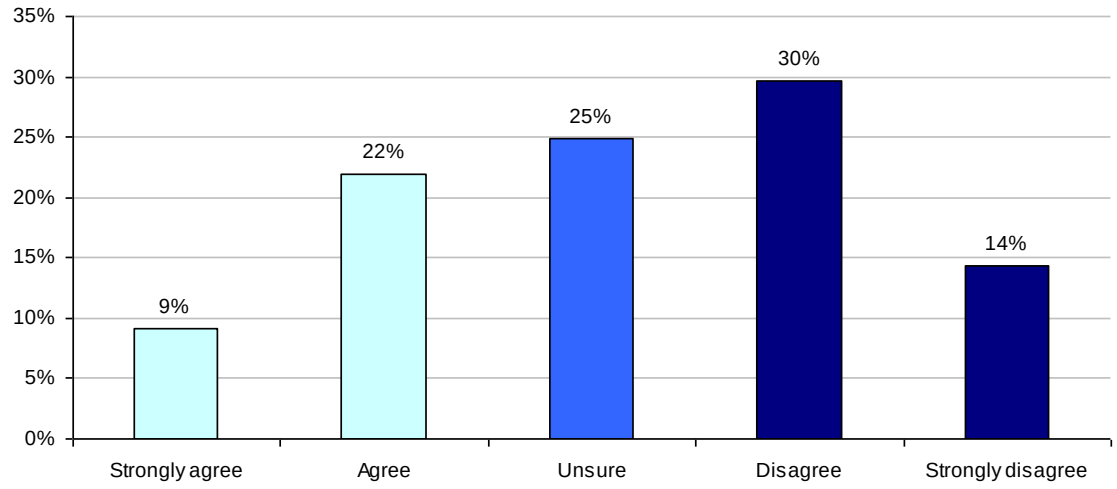
Pie Chart 2 reports the geographic distribution of respondents in our sample. The Northeast region at 19% represents the largest geographic segment in our sample. The Southwest is the smallest geographic region at 13%.

Pie Chart 2
U.S. geographic region of respondents



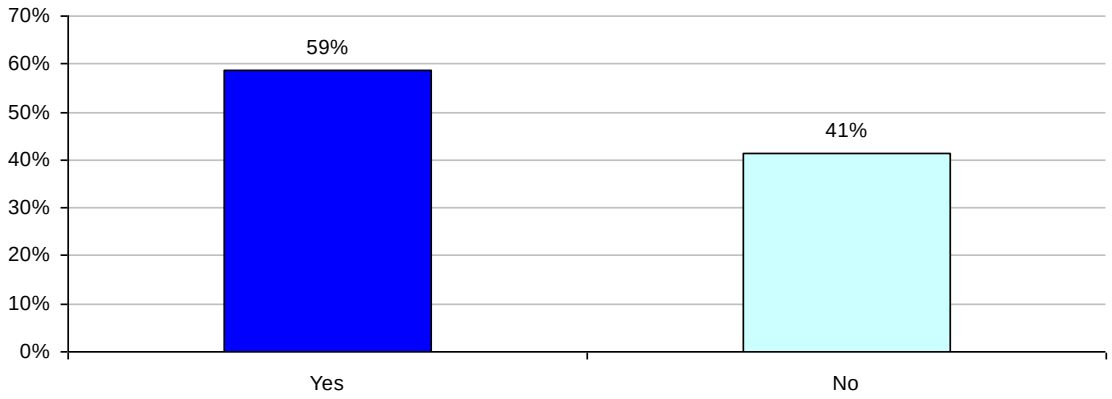
Bar Chart 2 reports the respondents' responses to an attribution about their former employer in terms of integrity and fairness. As can be seen, only 31% of the respondents hold a favorable impression of their former employer. The remainder of respondents have an unfavorable impression (44%) or unsure (25%).

Bar Chart 2
Rate this statement: I trust my former employer to act with integrity and fairness.



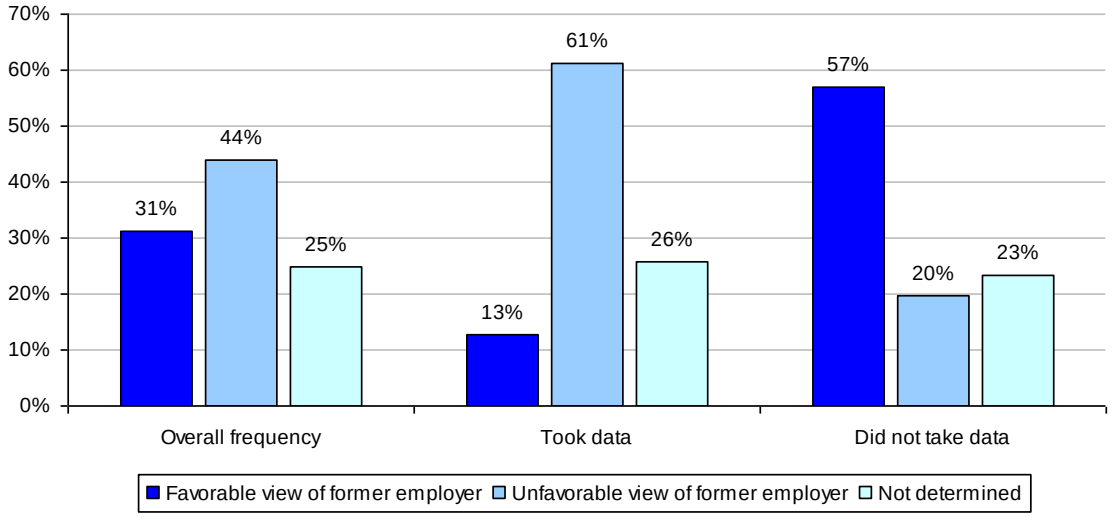
Bar Chart 3 reports the percentage frequency of respondents who state they kept some of their former employer's company information. As can be seen, 59% of respondents admit that they kept some of this information after departing from their former company.

Bar Chart 3
Did you keep any company information after leaving your former employer?



Bar Chart 4 reports the percentage frequency of respondents according to their favorable or unfavorable views about their former employer. The results clearly show that the respondent's decision to take or not take company information is related to their views about their former employer.

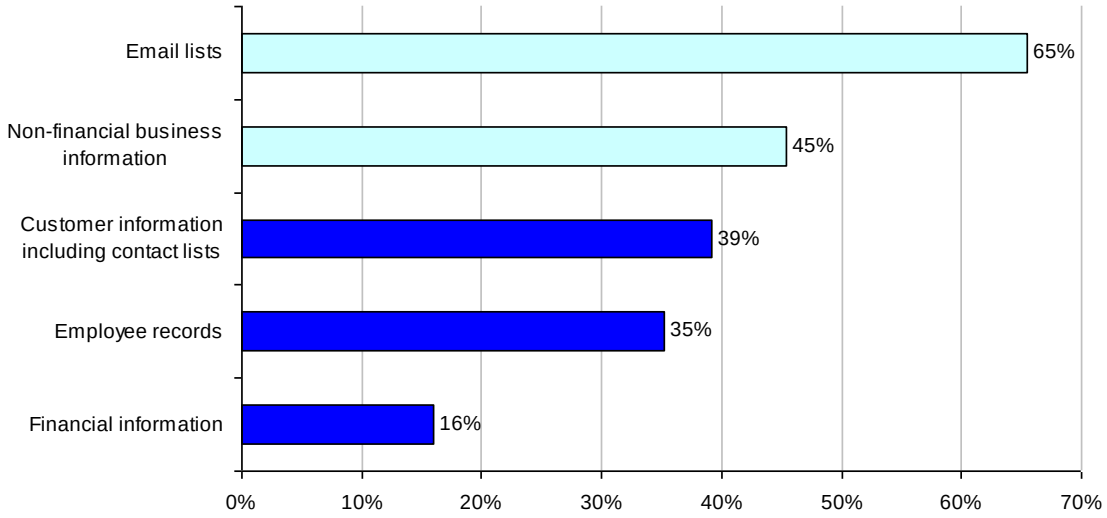
Bar Chart 4
Did you keep the company's information?
Comparison of responses based on the respondent's favorable or unfavorable views



Accordingly, only 13% of respondents who say they had a favorable view kept some of their former company's information. In contrast, more than 61% of respondents with unfavorable views kept some of their former company's information.

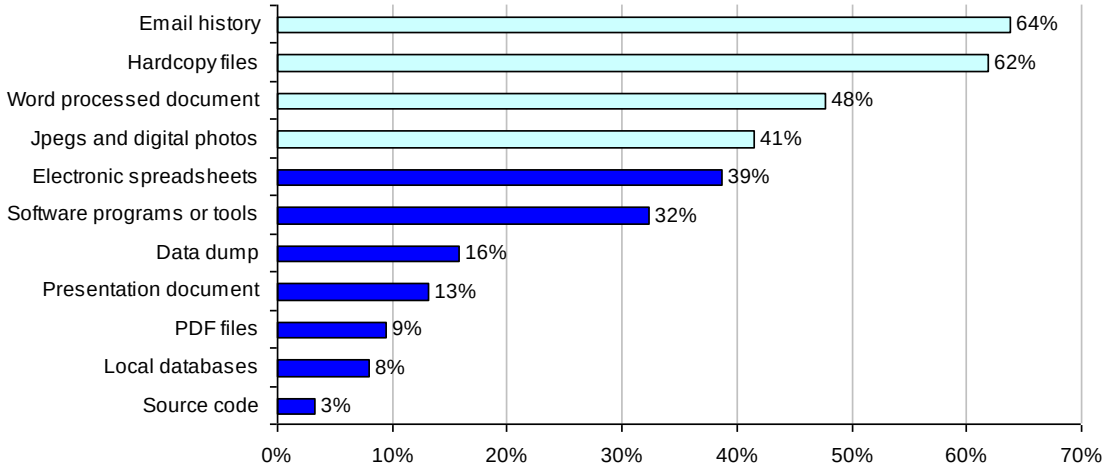
Bar Chart 5 reports the types of confidential business information that respondents say they kept after departure. Email lists, non-financial business information (such as company memos), and customer information including contact lists are the most commonly cited types of data.

Bar Chart 5
What type of confidential, sensitive or proprietary information did you keep after leaving your former company?



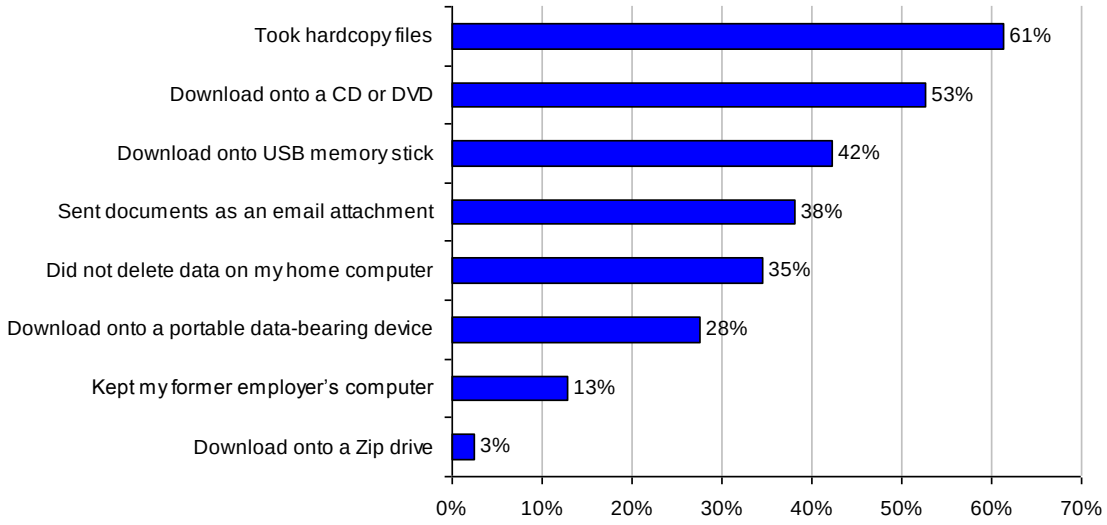
Bar Chart 6 reports the kinds of electronic or paper files that respondents kept after departing their former employer. Consistent with the above chart, email history, paper files, word processed documents, and digital photos are the most commonly cited files kept by respondents.

Bar Chart 6
What kinds of electronic or paper files did you keep?



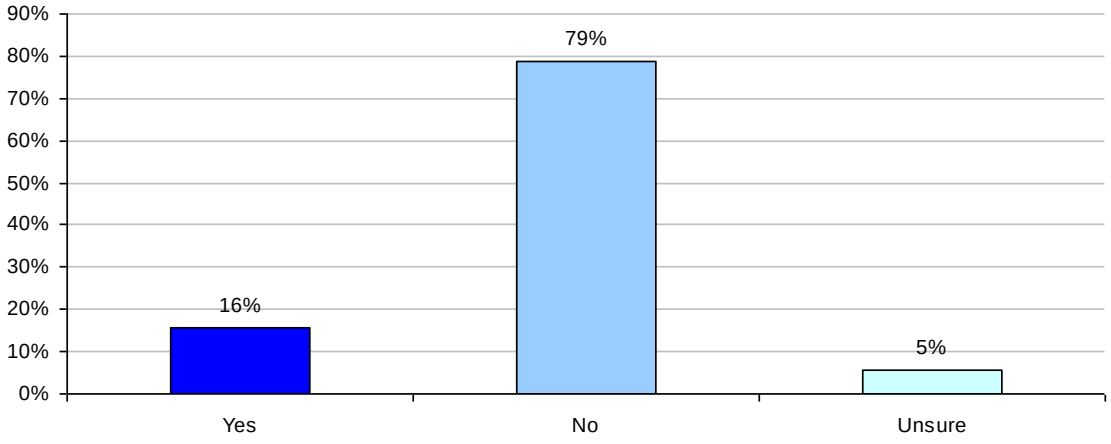
How did the transfer of confidential information happen? Bar Chart 7 reports how respondents took their former company's information. The most common methods include: hand carrying of paper documents (61%), downloading of documents onto a CD or DVD (53%), and downloading electronic files onto a USB memory stick (a.k.a. thumb drive) (42%).

Bar Chart 7
How did the information transfer happen?



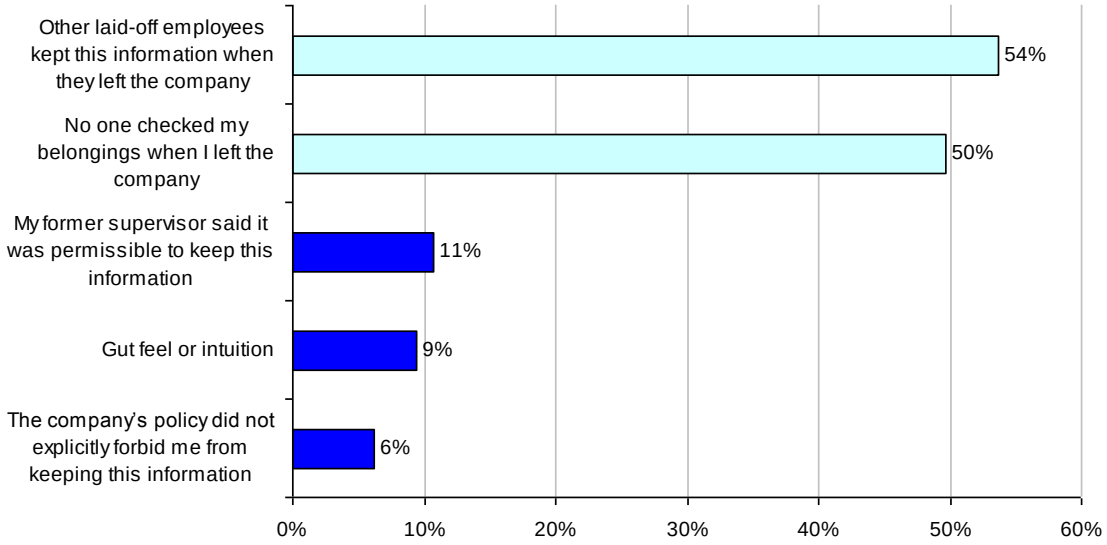
Bar Chart 8 reports the percentage responses to a survey question about permission to keep the information. More than 79% of respondents admit to taking information without permission. Only 16% say they did receive permission in advance.

Bar Chart 8
Did your former company permit you to keep any of this sensitive, confidential or proprietary information?



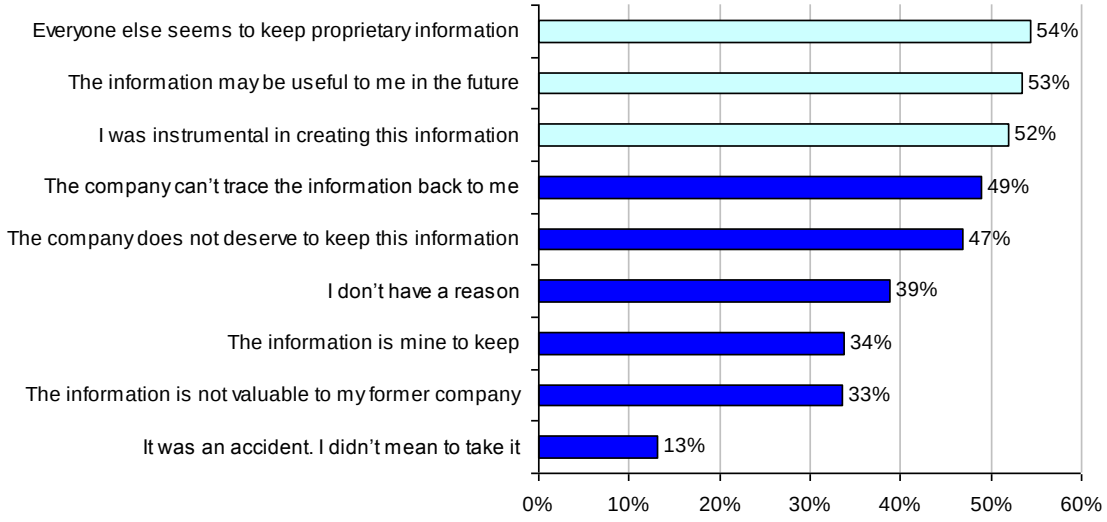
For those who state they received permission to keep some of their company's information, Bar Chart 9 reports how respondents came to believe that permission was given. As shown, the number one reason is "other laid-off employees kept information" (54%) and "no one checked my belongings when I left" (50%). Only 11% of respondents say they received explicit permission from their supervisor.

Bar Chart 9
How did you know or confirm that it was acceptable to keep this sensitive, confidential or proprietary information?



For those who say they did not receive permission to keep their company's information, Bar Chart 10 reports why these respondents feel it was okay to keep it anyway.

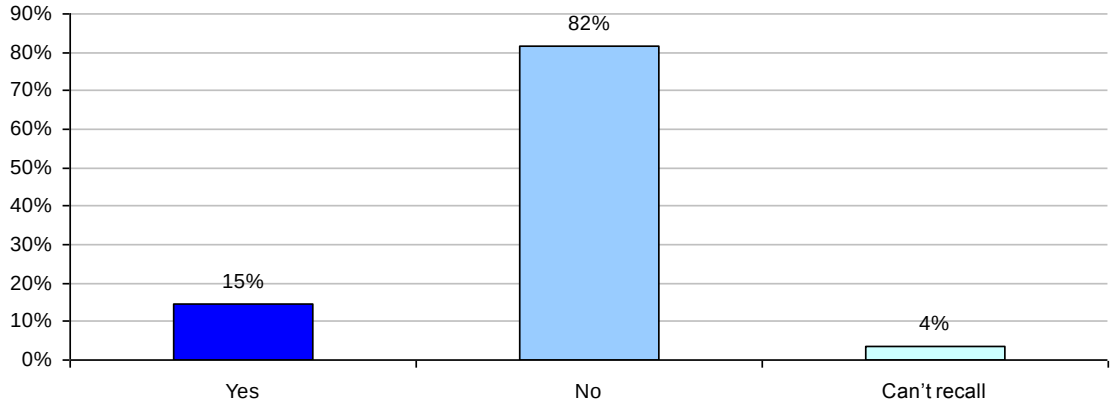
Bar Chart 10
Why did you feel it was okay to keep this information anyway even though you did not receive permission to take it?



The most commonly cited reasons for taking the company's information is "everyone else does this" (54%), "the information may be useful to me in the future" (53%), and "I was instrumental in creasing this information" (52%). It is also interesting to see that 39% report they did not have any reason.

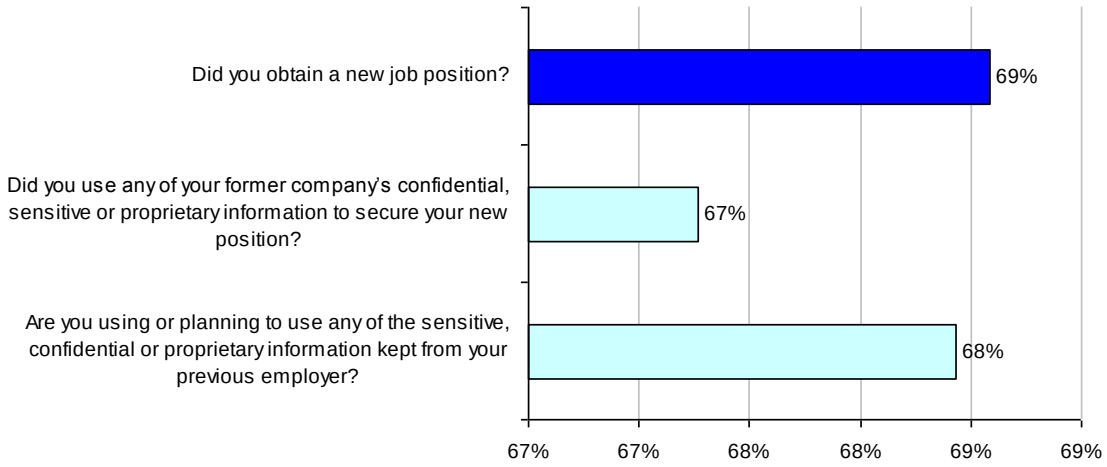
Bar Chart 11 shows that 82% of respondents report that their former company did not perform a review or audit of documents and other information sources as part of the exit process.

Bar Chart 11
Did the company review or perform an audit of the paper and/or electronic documents you were taking with you when you left?



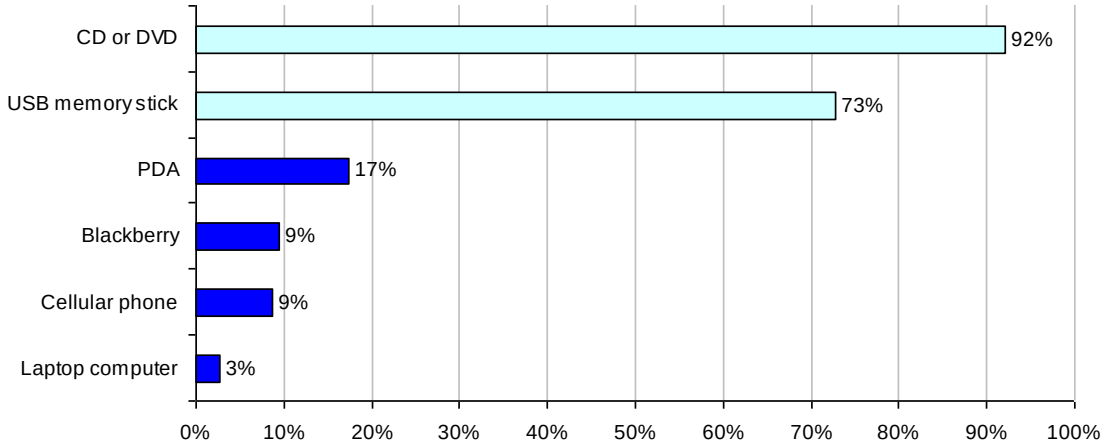
Bar Char 12 shows that 69% of the respondents who kept former company's information say they found a new job. Of these individuals, 67% presently use the information at their new employer and 68% said they plan to use this information in the future.

Bar Chart 12
Reuse of former employer's information in present job
Each bar represents the Yes% response



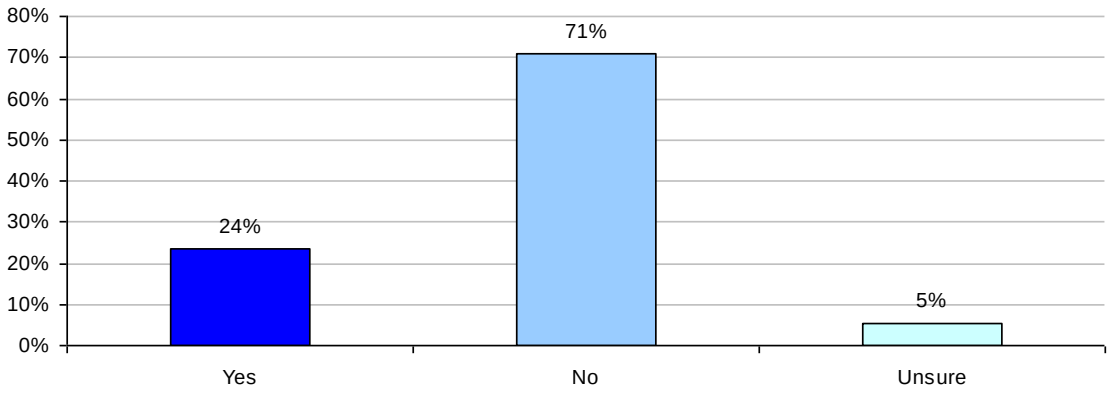
Bar Chart 13 reports the electronic storage media or devices kept by respondents after they departed their former employer. As can be seen, 92% report they kept a CD or DVD containing company information. Another 73% say they kept a USB memory stick. Only 3% admit to keeping a laptop computer.

Bar Chart 13
Did you keep any of the following electronic storage devices assigned to you by your former employer?



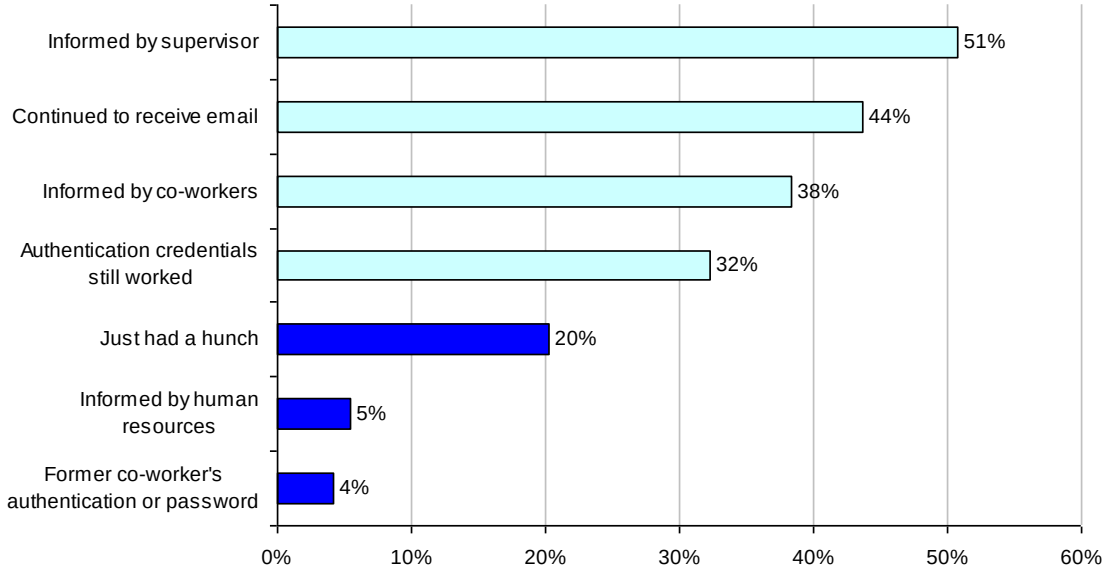
Bar Chart 14 shows the percentage frequency of respondents to the question, "Did you have access to your former company's computer system or network after departure or termination of employment?" More than 24% state that they did have access to company systems after they departed and 71% say they did not.

Bar Chart 14
Did you have access to the company's computer system or network after departure from your former company?



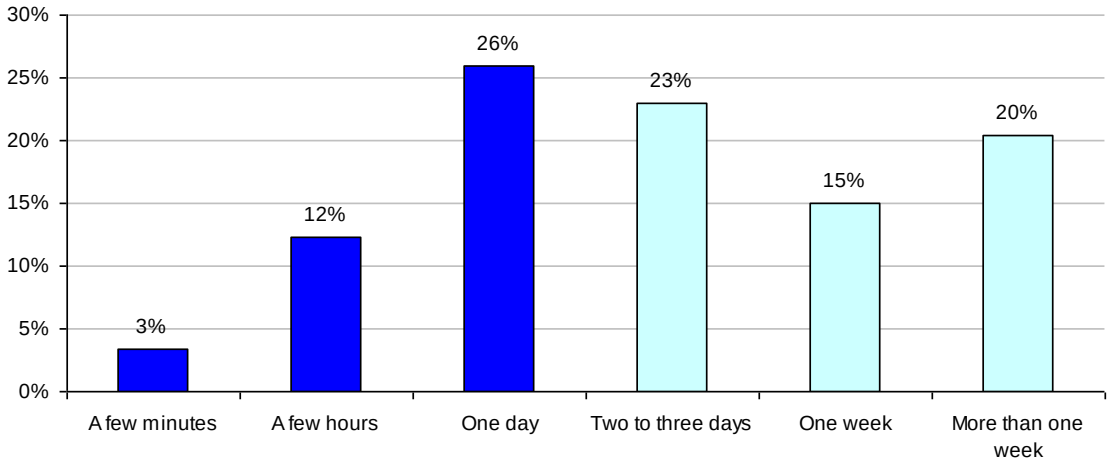
How did respondents know they continued to have access to their former company's system or network after exiting the company? Bar Chart 15 lists the top reasons such as being told by a supervisor (51%), continued receiving email on company account (44%), informed by co-workers (36%), and authentication (such as passwords) still worked (32%).

Bar Chart 15
How did you know you had access after you left your former company?



How long after exiting their former company did they continue having access to systems and networks? Bar Chart 16 shows an alarming pattern, wherein 58% of respondents state that they had access to proprietary systems for two or more days after departing the company.

Bar Chart 16
How long after leaving did you have access to the system or network?



Methods

A large national random sampling frame of 351,563 adult-aged consumers who reside within the United States was used to recruit participants to this web survey.[1]

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

Table 1 Sample description	Freq.
Consumer sampling frame	351,563
Bounce-back	49,880
Total returns	26,059
Rejected surveys	992
Total sample	25,067
Removed surveys from screening	24,122
Final sample	945
Total response after screening	0.27%

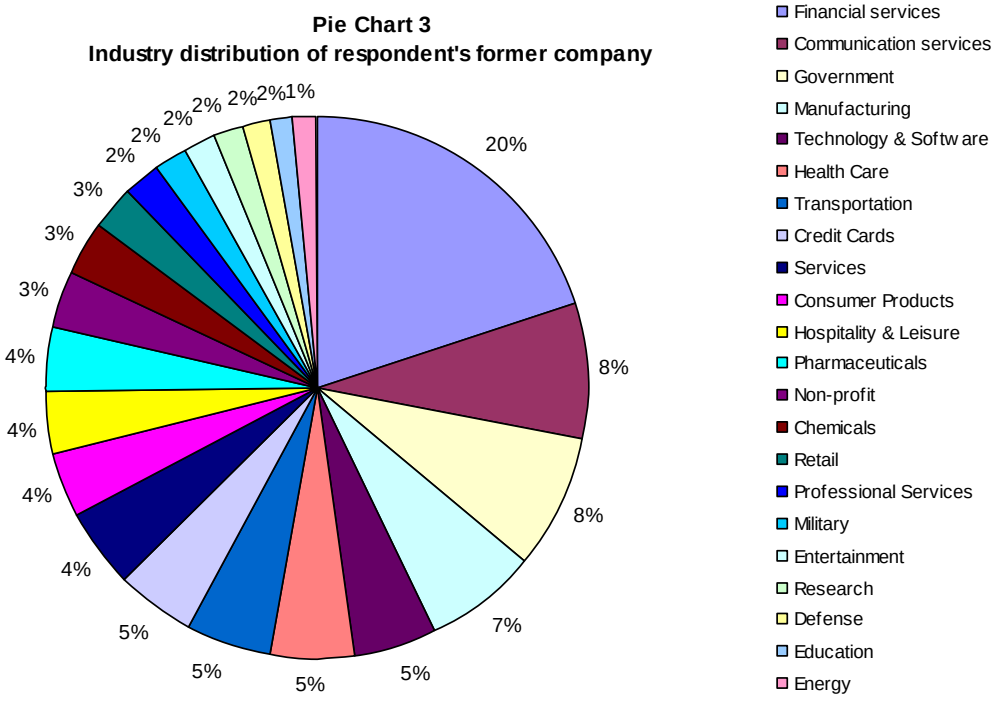
Three screening questions were used to filter the sample to those individuals who recently lost their position or changed jobs.

- **Screen 1**: Did you change employer or lose your job sometime during the past 12 months?
- **Screen 2**: When you were employed, did your employer assign a desktop or laptop computer for your use in the workplace?
- **Screen 3**: Did your previous job require you to access and use proprietary information such as customer data, contact lists, employee records, financial reports, confidential business documents, software tools, or other intellectual properties?

According to Table 1, 945 respondents passed screening criteria and provided reliable survey returns during within an eight-day research (holdout) period. This sample represents .27% of the initial pre-screened consumer panel. The margin of error on adjective scale responses is ≤ 3 percent.

Pie Chart 3 shows the distribution of the former organization's primary industry classification. As shown, financial services, including banking, brokerage, insurance and credit cards, represent the largest industry segment in the final sample.

Pie Chart 3
Industry distribution of respondent's former company



Over 95% of respondents completed all survey items within 15 minutes. Respondents, on average, have 8.1 years of overall experience and 2.9 years at their former employer. About 51% of respondents are female and 49% male. More than 37% of respondents say they were involuntarily terminated from their former company.

Table 2a reports the respondent's present employment status, with 51% stating they found full time positions. Table 2b provides the highest attained education levels of respondents. As can be seen, 41% state they attended or completed college or a university program.

Table 2a **Please check your present employment status:**	**Pct%**
Full time employee	51%
Part time employee	10%
Contract employee	11%
Small business owner	8%
Full time student	8%
Retired	7%
Disabled	5%
Other	1%
Total	100%

Table 2b **Highest level of education**	**Pct%**
High school	29%
Vocational school	19%
College or university	41%
Graduate school	8%
Doctorate (MD, Ph.D., JD)	2%
Other	1%
Total	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 in the workforce. We acknowledge bias may be caused by compensating respondents to complete this research within a holdout period. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

The detailed results of this study can be found in the attached Appendix. For more information about this study please contact the Ponemon Institute.

Ponemon Institute, LLC
Attn: Research Department
2308 US 31 North
Traverse City, MI 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: Survey Results

Following are the results of a web-based survey involving 945 adult-aged participants located in the United States who experienced termination from employment within the past 12 months. All research was conducted in January 2009. These results are presented in a percentage frequency format. Pct% = only one choice permitted. Total% = two or more choices are permitted.

Parameters of the sample	Freq.
US consumer sampling frame	351,563
Bounce-back	49,880
Total returns	26,059
Rejected surveys	992
Total sample	25,067
Removed surveys from screening	24,122
Final sample	945
Total response after screening	0.27%

Screening questions Q1 to Q3 are used to define the final sample. Question Q4 is used to establish the respondent's perception of their former employer.

S1. Did you change employer or lose your job sometime during the past 12 months?	Freq.	Pct%
Yes	4,214	17%
No (stop)	20,853	83%
Total	25,067	100%

S2. When you were employed, did your employer assign a desktop or laptop computer for your use in the workplace?	Freq.	Pct%
Yes	1,510	36%
No (stop)	2,704	64%
Total	4,214	100%

S3. Did your previous job require you to access and use proprietary information such as customer data, contact lists, employee records, financial reports, confidential business documents, software tools, or other intellectual properties?	Freq.	Pct%
Yes	945	63%
No (stop)	565	37%
Total	1,510	100%

S4. Rate this statement: I trust my former employer to act with integrity and fairness	Freq.	Pct%
Strongly agree	87	9%
Agree	207	22%
Unsure	235	25%
Disagree	280	30%
Strongly disagree	136	14%
Total	945	100%

Q1. Did you keep any company data or information after leaving your former employer?	Freq.	Pct%
Yes	553	59%
No (go to Part 3)	392	41%
Total	945	100%

Q2 to Q12 are based on 553 survey responses.	
Q2. What type of confidential, sensitive or proprietary information did you keep after leaving your former company? Please check all that apply.	Total%
Email lists	65%
Non-financial business information	45%
Customer information including contact lists	39%
Employee records	35%
Financial information	16%
Other (please specify)	1%
Total	202%

Q3. What kinds of electronic or hard (paper) files did you keep after leaving your former company? Please check all that apply.	Total%
Copies of emails (history)	64%
Printed documents or other hard (paper) files	62%
Word (or other word processed documents)	48%
Jpegs and digital photos	41%
Excel (or other electronic spreadsheet documents)	39%
Software programs or tools	32%
Data dump from corporate database systems	16%
PowerPoint (or other presentation documents)	13%
PDF files	9%
Access database files (or other local databases)	8%
Source code	3%
Other (please specify)	3%
Total	338%

Q4. How did you transfer this sensitive, confidential or proprietary information from your former company's systems or network? Please check all that apply.	Total%
Took paper documents or hard files	61%
Downloaded information onto a CD or DVD	53%
Downloaded information onto USB memory stick	42%
Sent documents as attachments to a personal email account	38%
Decided not to delete the information already residing on my home computer	35%
Downloaded information onto a portable data-bearing device such as a PDA, Blackberry, iPod, phone or other mobile device	28%
Kept my former employer's computer, laptop or other portable data-bearing device	13%
Downloaded information onto a Zip drive	3%
Other (please specify)	2%
Total	273%

Q5a. Did your former company permit you to keep any of this sensitive, confidential or proprietary information?	Pct%
Yes	16%
No (Go to Q5c)	79%
Unsure (Go to Q5c)	5%
Total	100%

Q5b. If yes, how did you know or confirm that it was acceptable to keep this sensitive, confidential or proprietary information?	Total%
No one checked my belongings when I left the company	50%
My former supervisor said it was permissible to keep this information	11%
The company's policy did not explicitly forbid me from keeping this information	6%
Other laid-off employees kept this information when they left the company	54%
Gut feel or intuition	9%
Other (please specify)	0%
Total	130%

Q5c. If no or unsure, why did you feel it was okay to keep this information anyway? Please check all that apply.	Total%
Everyone else seems to keep proprietary information	54%
The information may be useful to me in the future	53%
I was instrumental in creating this information	52%
The company can't trace the information back to me	49%
The company does not deserve to keep this information	47%
I don't have a reason	39%
The information is mine to keep	34%
The information is not valuable to my former company	33%
It was an accident. I didn't mean to take it	13%
Total	375%

Q6. Did you inform the company that you were keeping this information upon your exit or departure?	Pct%
Yes	4%
No	96%
Total	100%

Q7a. Did the company review or perform an audit of the paper and/or electronic documents you were taking with you when you left?	Pct%
Yes	15%
No	82%
Can't recall	4%
Total	100%

Q7b. If yes, how detailed was this review or audit conducted upon your exit or departure?	Pct%
Very complete	0%
Complete	10%
Somewhat complete	16%
Not complete	45%
Superficial	29%
Total	100%

Q7c. Did the company's review include an electronic scan of devices such as portable data-bearing equipment or USB memory sticks when you left?	Pct%
Yes	3%
No	89%
Can't recall	8%
Total	100%

Q7d. Who conducted the review or audit of the paper and/or electronic documents you were taking with you when you left?	Pct%
Direct supervisor or manager	41%
Human resources personnel	34%
IT department personnel	6%
Security department personnel	5%
Compliance or audit department personnel	0%
Legal department personnel	10%
Outside consultant	0%
Other (please specify)	3%
Total	100%

Q8a. Did you obtain a new job position?	Pct%
Yes	69%
No (Go to Q9)	31%
Total	100%

Q8b. Did you use any of your former company's confidential, sensitive or proprietary information to secure your new position?	Pct%
Yes	67%
No	33%
Total	100%

Q8c. Are you using or planning to use any of the sensitive, confidential or proprietary information kept from your previous employer?	Pct%
Yes	68%
No	32%
Total	100%

Q8d. What kinds of sensitive, confidential or proprietary information from your previous employer are you using (or planning to use)? Please check all that apply.	Pct%
Email lists	63%
Customer information including contact lists	39%
Employee records	34%
Software tools	32%
Non-financial business information	28%
Other intellectual properties	5%
Other (please specify)	3%
Source code	2%
Financial information	1%
Total	207%

Q9. Did you keep any of the following electronic storage devices assigned to you by your former employer? Please check all that apply.	Pct%
CD or DVD	92%
USB memory stick	73%
PDA	17%
Blackberry	9%
Cellular phone	9%
Laptop computer	3%
Other (please specify)	1%
Total	204%

10a. Did you have access to the company's computer system or network after departure from your former company?	Pct%
Yes	24%
No (Go to 11)	71%
Unsure (Go to 11)	5%
Total	100%

10b. How did you know you had access after you left your former company?	Total%
I was informed by my supervisor that I would have access to the company's system, email or network for a specified period of time.	51%
I continued to receive email on my company's account	44%
I was informed by co-workers that I had access to the company's system or network.	38%
I accessed the system and my authentication credentials still worked.	32%
Just had a hunch that I could access the company's system or network	20%
I was informed by human resources that I would have access to the company's system or network for a specified period of time.	5%
A co-worker allowed me to use his or her authentication credentials after departure from the company.	4%
Other (please explain)	2%
Total	197%

10c. How long after leaving your former company did you have access to the system or network?	Total%
Just a few minutes	3%
A few hours	12%
About one day	26%
About two to three days	23%
About one week	15%
More than one week	20%
Total	100%

Q11. Why did you leave your former company?	Pct%
Asked to leave	37%
Found a new job	38%
Anticipated layoff	21%
Other personal reasons	4%
Total	100%

Q12. Please indicate the following actions you took prior to or immediately after leaving your former company. Please check all that apply [reliability check on Q4].	Total%
Took paper documents or hard files	61%
Downloaded information onto a CD or DVD	53%
Downloaded information onto USB memory stick	42%
Sent documents as attachments to a personal email account	38%
Decided not to delete the information already residing on my home computer	35%
Downloaded information onto a portable data-bearing device such as a PDA, Blackberry, iPod, phone or other mobile device	28%
Kept my former employer's computer, laptop or other portable data-bearing device	13%
Downloaded information onto a Zip drive	3%
Other (please specify)	1%
Total	274%

Organizational characteristics and demographics	
What organizational level best describes your previous position?	Pct%
Senior Executive	1%
Vice President	2%
Director	4%
Manager	11%
Supervisor	11%
Associate/Staff	30%
Technician	8%
Administrative	16%
Contractor/consultant	13%
Intern	4%
Other (please describe)	1%
Total	100%

Check the department or function that best defined your role within your previous employer.	Pct%
General management	3%
Finance & accounting	10%
Corporate IT	19%
Sales	24%
Marketing & communications	7%
Logistics & transportation	5%
Human resources	4%
Manufacturing	7%
Research & development	1%
Compliance & audit	2%
Administration	16%
Other	3%
Total	100%

What is the worldwide headcount of your previous organization?	Pct%
Less than 500 people	15%
500 to 1,000 people	26%
1,001 to 5,000 people	28%
5,001 to 25,000 people	16%
25,001 to 75,000 people	8%
More than 75,000 people	6%
Total	100%

Total years of experience	8.11
Total years in previous job	2.87

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

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

Were you involuntarily terminated from your former company?	Pct%
Yes	40%
No	56%
Unsure	4%
Total	100%

Please check your present employment status:	Pct%
Full time employee	51%
Part time employee	10%
Contract employee	11%
Small business owner	8%
Full time student	8%
Retired	7%
Disabled	5%
Other	1%
Total	100%

Highest level of education	Pct%
High school	29%
Vocational school	19%
College or university	41%
Graduate school	8%
Doctorate (MD, Ph.D., JD)	2%
Other	1%
Total	100%

What industry best describes your former organization's industry concentration or focus?	Pct%
Agriculture	0%
Airlines	1%
Automotive	2%
Banking	12%
Brokerage	5%
Cable & Wireless	4%
Chemicals	3%
Consumer Products	4%
Credit Cards	5%
Defense	2%
Education	2%
Energy	1%
Entertainment	2%
Government	4%
Health Care	3%
Hospitality & Leisure	4%
Insurance	5%
Internet & ISPs	5%
Manufacturing	7%
Military	2%
Non-profit	3%
Pharmaceuticals	4%
Professional Services	2%
Research	2%
Retail	3%
Services	4%
Technology & Software	5%
Telecommunications	2%
Transportation	4%
Total	100%