Security of Paper Documents in the Workplace

Sponsored by

Alliance for Secure Business Information

Independently conducted by Ponemon Institute LLC

Publication Date: October 15, 2008

Security of Paper Documents in the Workplace

Executive Summary

Presented by Larry Ponemon, October 15, 2008

The Security of Paper Documents in the Workplace study conducted by Ponemon Institute and sponsored by the Alliance for Secure Business Information (ASBI) dispels the myth that the cause of most or all data breaches is lost or stolen electronic documents. In this study, the vast majority of respondents (80%) who self-reported that their organizations had a data breach, state that they had one or more data breaches in the past 12 months. Forty-nine percent state that one or more of these data breaches involved the loss or theft of paper documents.

In fact, 71% of participants in our study are aware of an incident in which sensitive or confidential paper documents were lost or misplaced in their organization and 53% believe that employees are putting them at risk at communal printers, in meeting rooms or at meetings held outside the office.

The final survey sample consisted of 819 individuals who work in IT operations, IT security, data protection and compliance in large organizations in a variety of industries. Respondents in this sample were selected randomly for the study because of their experience and expertise in assisting their organizations secure sensitive and confidential information and considered the most informed about risks associated with lost or stolen paper documents. Each respondent worked in an organization that had at least one data breach.

Our survey asked participants to respond to the following key issues:

- Do paper documents that contain sensitive or confidential information pose a significant security or privacy risk to organizations?
- Is it easier to protect paper documents than electronic documents from improper access?
- Who in the organization is accountable for safeguarding paper documents?
- Do organizations take reasonable steps to safeguard paper documents from creation to disposal (i.e., over the entire document lifecycle)?
- What practices and controls are being implemented today to protect this type of information?
- What is the economic impact to organizations for failing to secure paper documents?

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.

Businesses are not being responsive to the importance of protecting paper documents containing confidential information. The findings described below and in Bar Chart 1 are reasons why businesses are at risk.

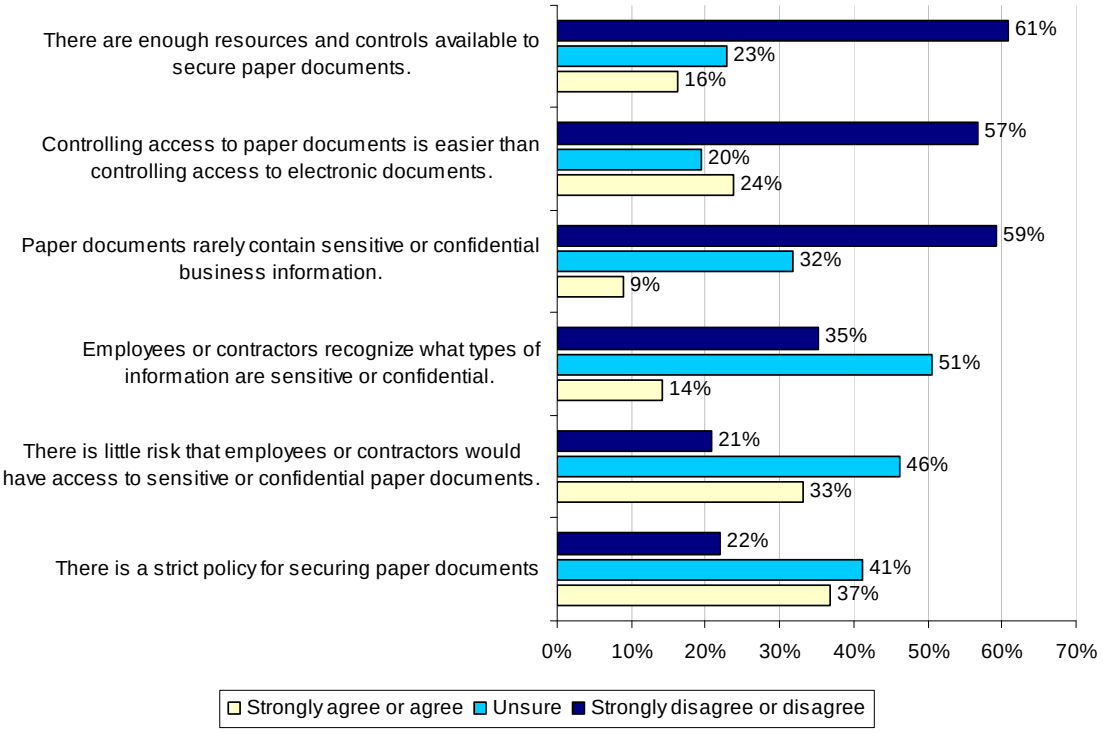
The following bar chart summarizes six attributions concerning the organization's response to the protection of paper documents in the workplace. The scale is reduced, combining strongly agree plus agree and strongly disagree plus disagree.

As can be seen, the percentage sum of disagree and unsure responses are much higher than the percentage of agree responses. This suggests that respondents do not feel their organizations are presently taking appropriate steps to maintain the security of paper documents containing sensitive or confidential information.

Bar Chart 1

Attributions about the respondent's organization

In my organization, . . . (strongly agree, agree, unsure, disagree and strongly disagree)



There are not enough resources available to protect confidential paper documents. Sixty-one percent of individuals surveyed report that there are **not** enough resources and controls available to secure paper documents containing sensitive or confidential information.

Uncertainty about existence of policy intended to protect confidential paper documents. Forty-one percent are uncertain whether there is a strict policy for securing and disposing of paper documents while only 37% strongly agree or agree that there is a strict policy.

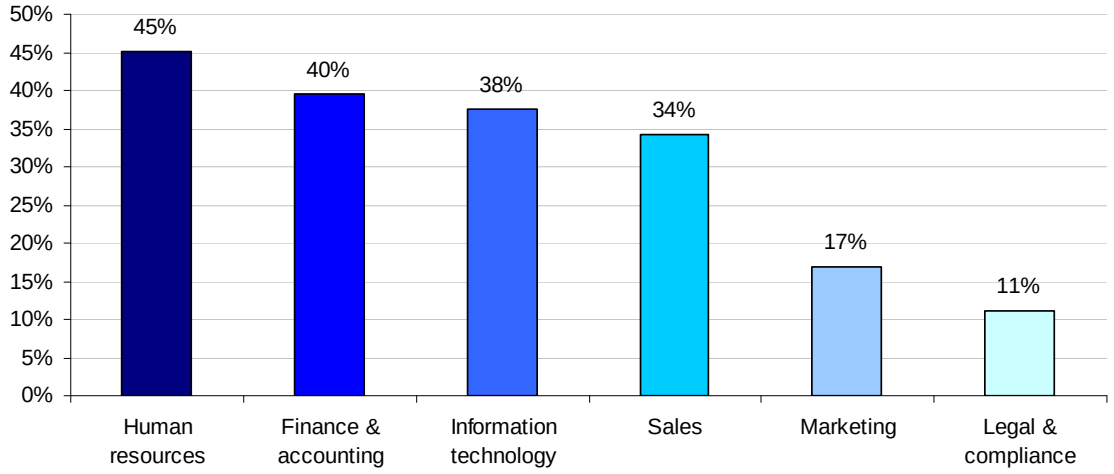
Risk of unauthorized access to confidential paper documents exists. Only 34% believe there is little risk that employees, temporary employee or contractors would have access to paper documents containing sensitive or confidential information.

Employees and contractors can't recognize sensitive information. Only 14% believe that employees or contractors would recognize what types of information are sensitive or confidential. More than half (51%) are uncertain.

Paper documents, similar to electronic documents, contain confidential information and are not easier to protect. Fifty-nine percent believe that paper documents in their organization contain sensitive and confidential information. Very few individuals surveyed (24%) believe it is easier to control access to paper documents containing sensitive or confidential information than it is to control access to electronic documents.

Certain functions and types of information are believed to be more at risk because of the inability to secure paper documents. Human Resources, Finance & Accounting, Information Technology and Sales are the departments that seem to pose the greatest risk (see Bar Chart 2).

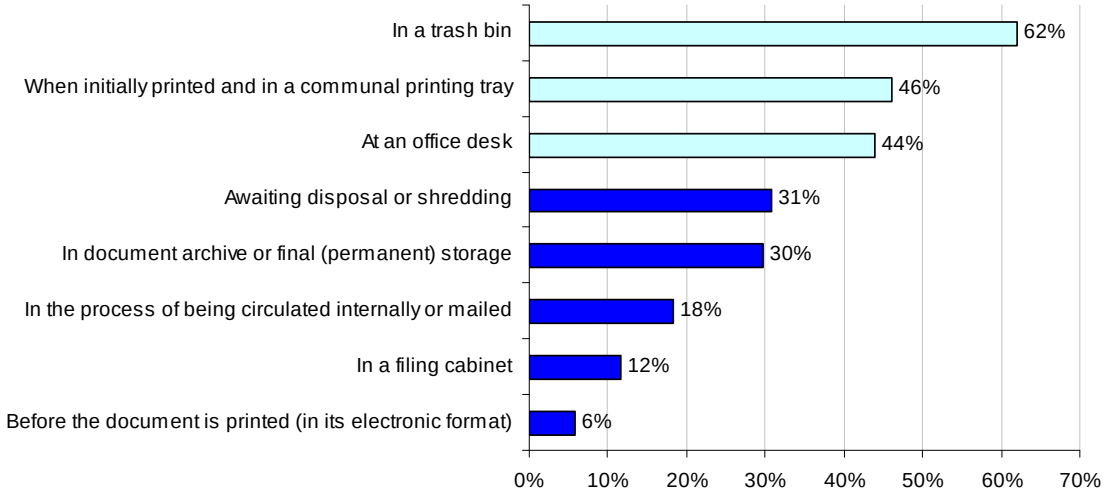
Bar Chart 2
What departments or functions within your organization are most at risk for not being able to protect or secure paper documents?
Respondents were allowed up to three choices.



The top five types of information employees consider to be most at risk are employee records, customer information, management accounting reports and budgets, marketing and sales reports and pre-released financial information and forecasts.

As shown in Bar Chart 3, paper documents are most at risk in a trash bin (62%), when initially printed and in a communal printing tray (46%) and at an office desk (44%). Least risky areas for paper documents are filing cabinets and before printing (in electronic format). Therefore, to reduce the risk to paper documents, organizations should have strict policies describing how sensitive and confidential documents should be disposed of, programs to train employees and third party contractors to follow these policies and easy access to shredding machines.

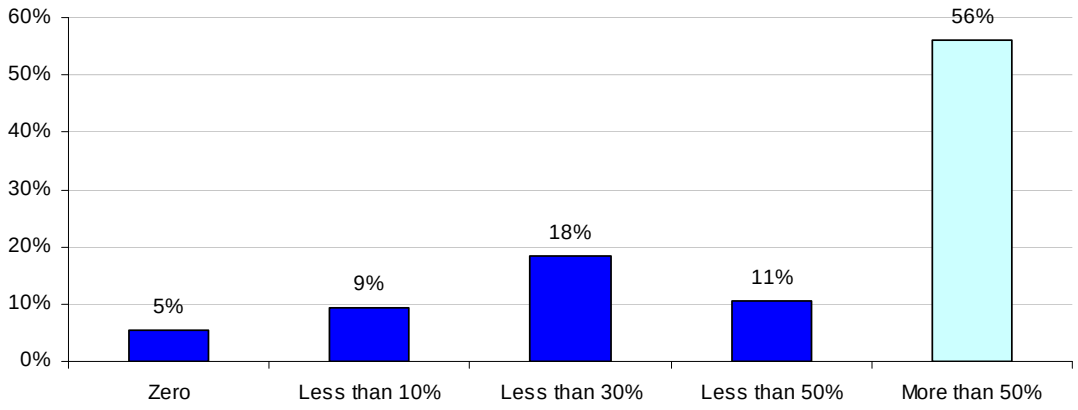
Bar Chart 3
At what stage of a paper document's life cycle is information most at risk?
Following are the respondents' rating for highest risk or very high risk levels combined



Employees are often negligent in the protection of documents that contain sensitive and confidential information. More than half (53%) of individuals surveyed say that employees very often or often put sensitive and confidential information at risk by leaving them at communal printers, in meeting rooms or at meetings held outside the office.

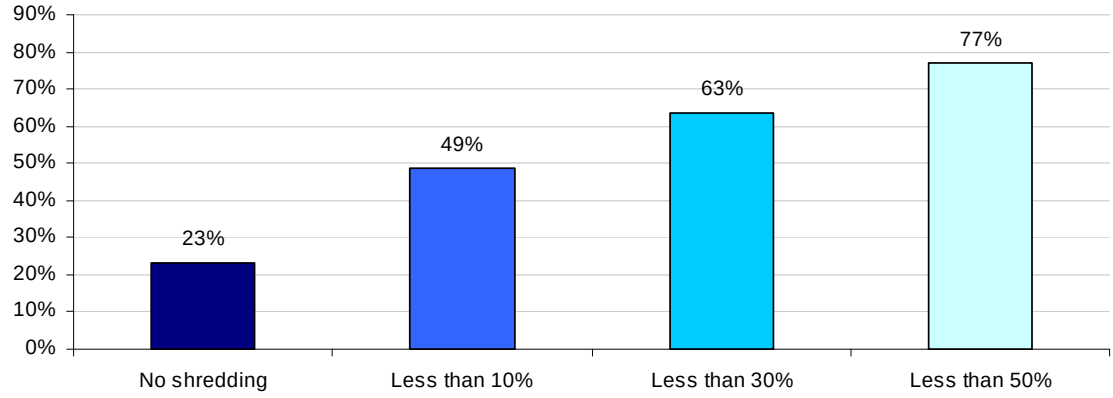
According to 56% of individuals surveyed, more than half of the organizations' sensitive or confidential information is contained within paper documents (see Bar Chart 4).

Bar Chart 4
Percentage of the organization's sensitive or confidential information is available in paper documents



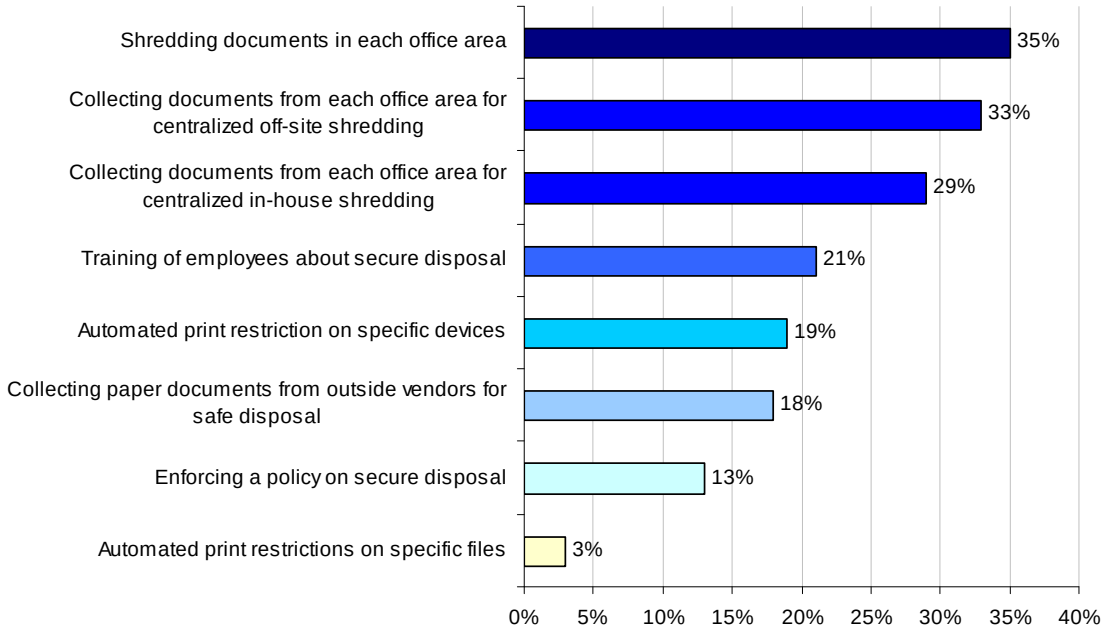
Approximately 77% of respondents say that their organizations shred <u>less than half</u> of all documents containing sensitive or confidential information before disposal (see Bar Chart 5). The relatively low percentage of shredded paper documents suggests organizations are at risk for failing to secure sensitive or confidential information.

Bar Chart 5
Percentage of paper documents containing sensitive or confidential information shredded before disposal



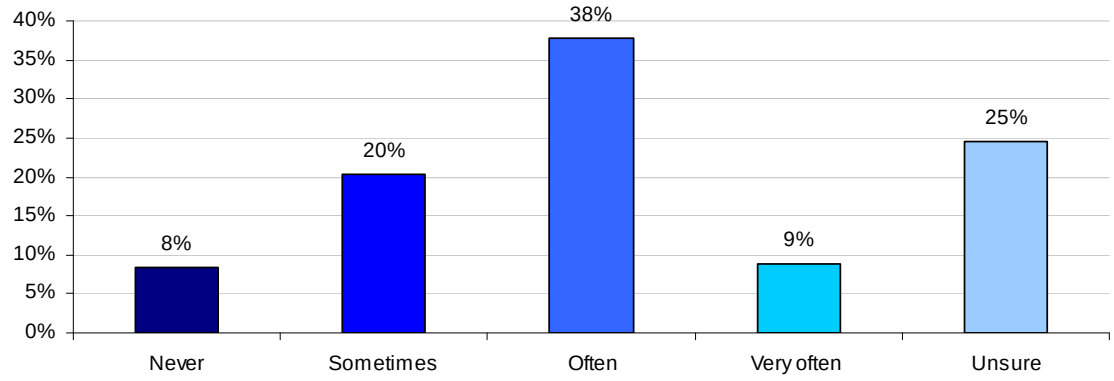
Bar Chart 6 shows the most common steps taken to dispose of paper documents. These are shredding documents in each office area, collecting documents from each office area for centralized off-site shredding and collecting documents from each office area for centralized in-house shredding. Only 21% of those surveyed say that they train employees about disposal.

Bar Chart 6
What steps are taken to safely dispose of paper documents within your organization?



Bar Chart 7 shows that not controlling access to paper documents with sensitive and confidential information increases the risk of a data breach. Forty-seven percent of respondents believe that employees, temporary employees or contractors often (38%) or very often (9%) have access to paper documents that are not pertinent to their role or responsibility. Twenty-five percent are unsure.

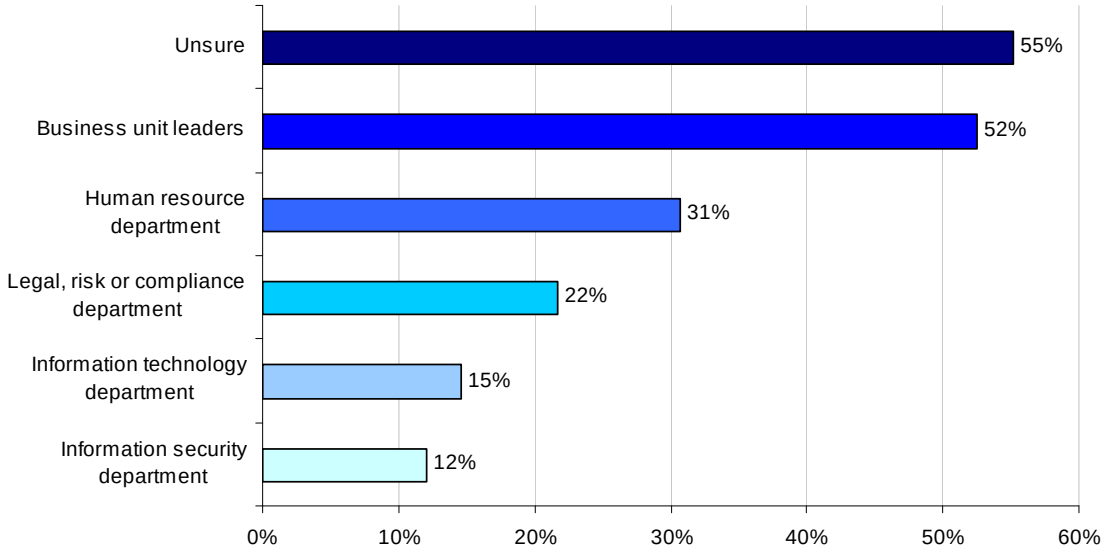
Bar Chart 7
How often does an employee, temporary employee or contractor have access to paper documents that are not pertinent to his or her role or responsibility?



In many organizations, there is uncertainty about who should be accountable for granting access to paper documents.

According to the study, 55% are unsure followed by business unit leaders (52%) and human resource department (31%).

Bar Chart 8
Who is accountable within your organization for granting access to paper documents containing sensitive or confidential information?



A lack of training and awareness about sensitive and confidential information puts the organization at risk.

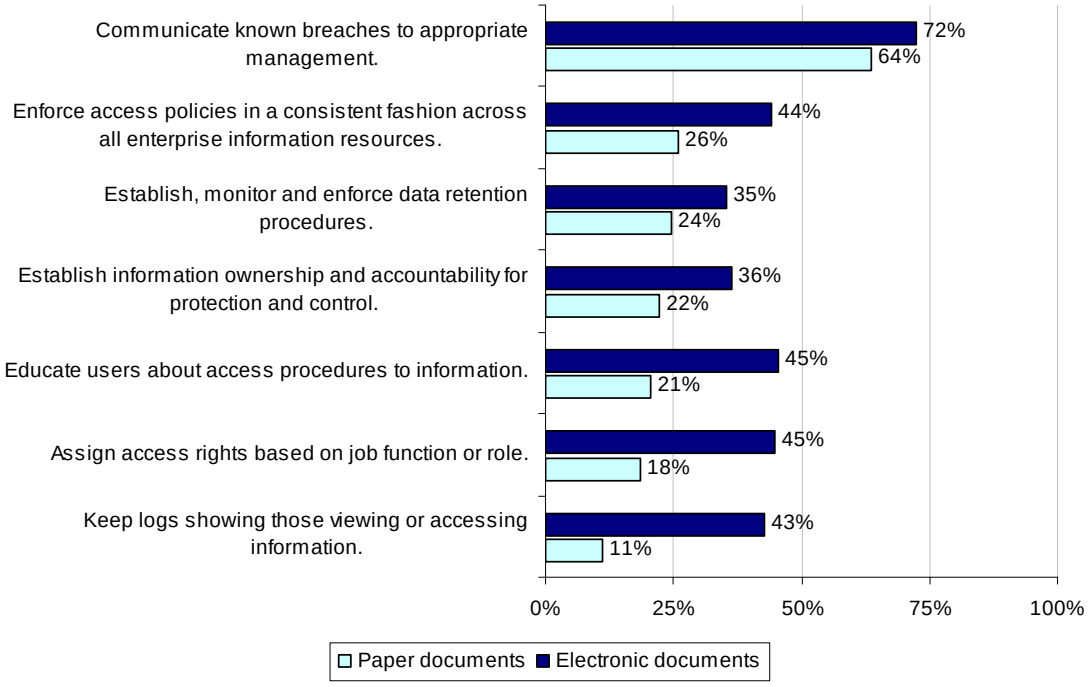
Most businesses (78%) have a policy that explains how paper documents with sensitive or confidential information should be secured and disposed of safely. However, only 29% of employees receive training about the policy and what types of information might be considered sensitive or confidential in these documents.

In general, organizations are better able to govern the use, protection and disposal of electronic documents than paper documents.

According to respondents, organizations are better able to enforce access policies for electronic documents in a consistent fashion across all enterprise information resources. Fifty-three percent are not confident that their organization has visibility to all users of sensitive or confidential business information contained in paper documents and electronic files.

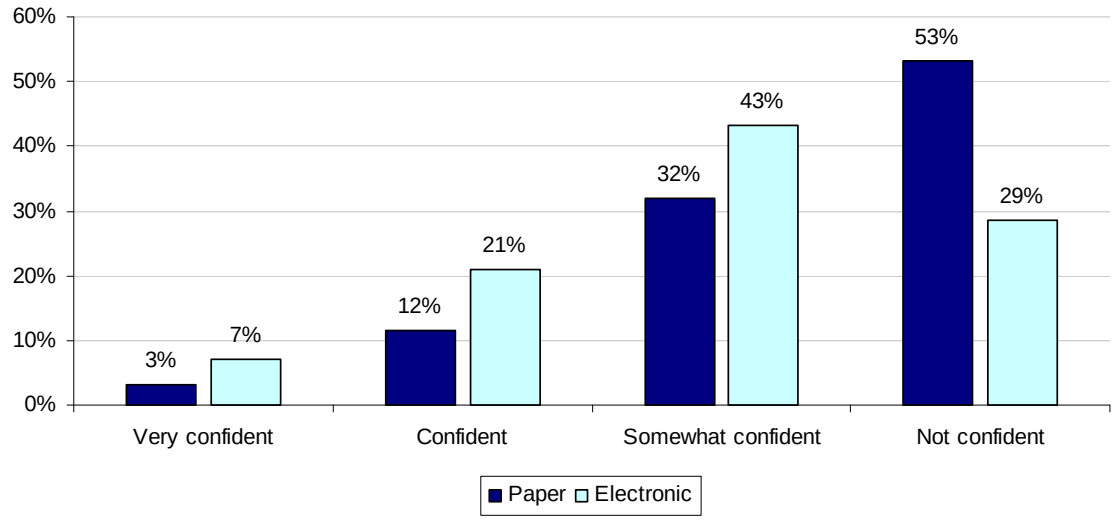
Bar Chart 9 compares perceptions about the use, protection and disposal of paper and electronic documents. While organizations seem to be almost equally good at communicating data breaches involving both paper and electronic documents (72% vs. 64%), it is not the case when it comes to activities involving access to electronic and paper documents. As shown in Bar Chart 9, organizations believe they are much better at safeguarding electronic documents than paper documents in such areas as: educating employees about access procedures, assigning access rights based on an individual's role and keeping logs about who is accessing information.

Bar Chart 9
How well is your organization able to govern the use, protection and disposal of paper documents and electronic documents?
Each percentage is the sum of excellent or good responses only



As shown in Bar Chart 10, more than half (53%) are not confident that they have visibility to all users of sensitive and confidential business information in paper documents

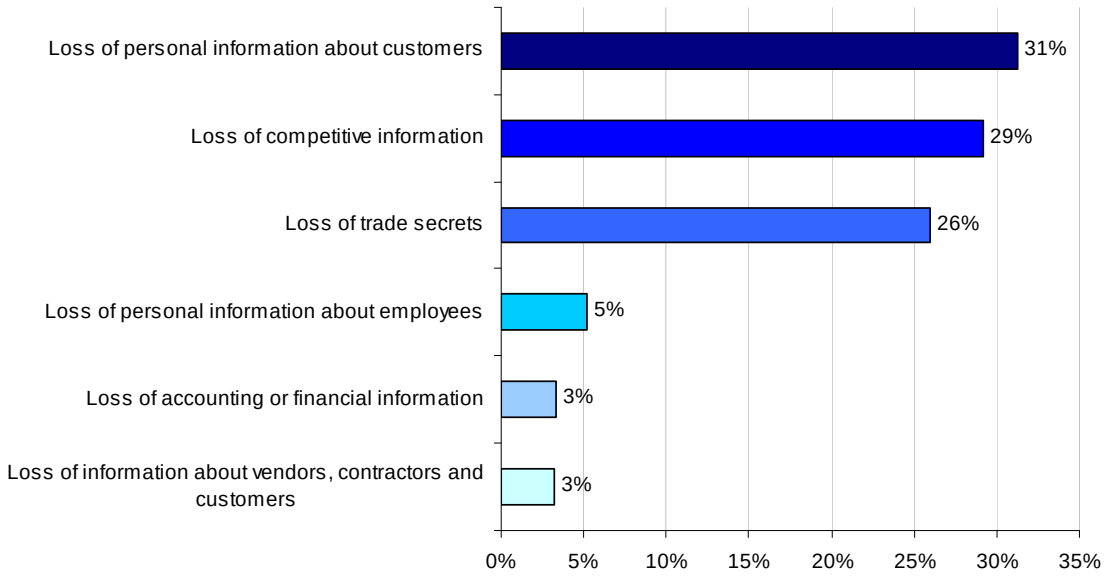
Bar Chart 10
How confident are you that your organization has visibility to all users of sensitive or confidential information contained in paper documents and electronic files?



Organizations can suffer significant economic impact when paper documents are lost, missing or stolen.

Eighty-four percent of respondents believe that their organizations lose time, money and other resources as a result of lost, missing or stolen business information contained in paper documents. Approximately 46% of those surveyed estimate that the financial impact is between $10 million to $30 million per year. As shown in Bar Chart 11, the top three root causes of this financial loss are personal information about customers, loss of competitive information and loss of trade secrets.

Bar Chart 11
Root causes of the organization's financial loss due to the loss or theft of paper documents containing confidential or sensitive information.



Recommendations

The risk of having sensitive and confidential paper documents lost or stolen is not going away. Despite the widespread use of computers in the workplace, we still seem to be dependent upon paper. In fact, 65% of those surveyed state that the availability and use of printed or hardcopy documents has stayed the same or increased during the past two years.

Further, these experts believe the reason to protect paper documents is to reduce identity theft of customers' and employees' personal information. They also believe to a lesser extent it is to reduce the exposure of the company's sensitive or confidential information that may impact brand.

What are the top six steps that organizations can take to protect confidential and sensitive documents? According to survey participants they are:

- Strict enforcement of non-compliance with document handling and disposal procedures.
- Shredding machines that are easily accessible by employees.
- Senior level executive support.
- Ample budget to manage and control sensitive paper documents.

- Rigorous compliance of procedures for monitoring document protection and safe disposal.

- Establish accountability to business unit leaders to secure paper documents and files.

The information security experts in our study agree that businesses are vulnerable to data breaches involving paper documents. We have also shown in this study the economic impact to businesses that lose confidential and sensitive information.

The positive news is that this is a risk that can be reduced through identification of areas in an organization that are most vulnerable and making sure there are procedures to properly dispose of paper documents. Training and awareness of what the organization thinks is confidential and sensitive is critical. Employees, contractors and third parties need to understand their role in disposing of sensitive and confidential information. In turn, organizations should help employees to be more accountable by making it efficient and convenient to safeguard documents.

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 security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used 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 13,989 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 lists of IT, security, compliance and data protection professionals.

Table 1 Description	Total	Pct%
Sampling frame	13989	100.0%
Bounce back	2016	14.4%
Total responses	1128	8.1%
Cancellations from screening	210	1.5%
Reliability rejections	99	0.7%
Net sample before reliability checks	819	5.9%

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

As shown in Table 1, 1,128 respondents completed their survey results within an eight-day research period. Of returned instruments, 99 survey forms were rejected because of reliability checks and another 210 were rejected because of screening criteria. A total of 819 surveys were used as our final sample. This sample represents a 5.9 percent net response rate. The margin of error on all adjective scale and Yes/No/Unsure responses is ≤ 3.5 percent.

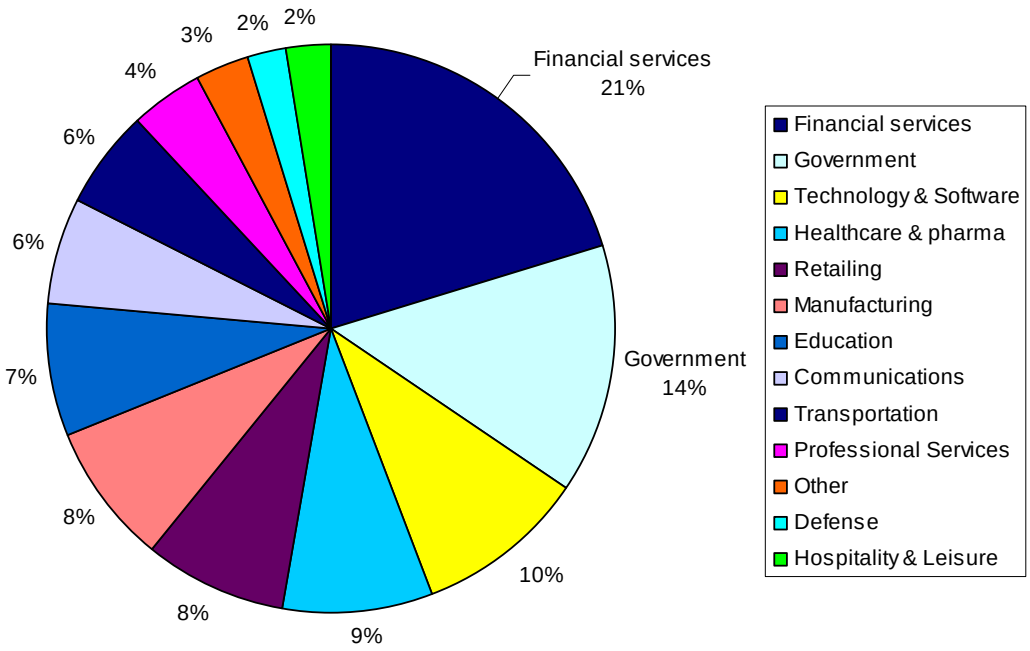
Over 95% of respondents completed all survey items within 13 minutes. Following are key demographics and organizational characteristics for U.S. respondents. Table 2a reports the functional areas represented within our sample. Table 2b provides the self-reported organizational level of respondents. As can be seen, the majority of respondents are at the director, manager or supervisor level (60%).

Table 2a Respondents' functional areas	Pct%
IT security	41%
IT operations	29%
Compliance	10%
Risk management	8%
Human resources	5%
Procurement	2%
Application development	2%
Research	1%

Table 2b Respondents' position level	Pct%
Senior Executive	1%
Vice President	2%
Director	13%
Manager	22%
Supervisor	25%
Technician/staff level	27%
Other	10%

Pie Chart 1 reports the average distribution of respondents by their organization's primary industry classification. As shown, 21% of respondents are employed by financial service companies (including insurance, banking, credit cards, brokerage and investment management), and 14% work for federal or local government.

Pie Chart 1: Industry Distribution



On average, respondents have 8.9 years of overall work experience and 8.0 years in the IT, security, compliance or data protection fields. In total, 59% of respondents were males and 41% 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 organization's geographic location, showing that the majority of respondents' companies are headquartered in the United States. Table 3b provides the approximate headcounts of these organizations. As can be seen, 64% of respondents are employed by larger-sized organizations (with more than 5,000 employees).

Table 3a Geographic location	Pct%
Northeast	20%
Mid-Atlantic	17%
Midwest	15%
Southeast	13%
Southwest	11%
Pacific	18%
Outside U.S.	7%
Total	100%

Table 3b. Organizational headcount	Pct%.
Less than 500 people	4%
500 to 1,000 people	10%
1,001 to 5,000 people	21%
5,001 to 25,000 people	34%
25,001 to 75,000 people	19%
More than 75,000 people	11%
Total	100%

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 e-mail:

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: Percentage Frequency of Survey Respondents

Part I concerns the respondents' organizations data breach history. Please note that Q1a was used as a screening question. In total, 210 individuals said NO to Q1a and, hence, were eliminated from the sample pool. It is interesting to see that almost half of all respondents said one or more of their organization's data breach concerned the loss or theft of paper documents.

Part 1: Data breach		
Q1a. Did your organization experience a data breach in the past 12 month period?	Freq	Pct%
Yes, only one incident	287	28%
Yes, two to five incidents	351	34%
Yes, more than five incidents	181	18%
No (STOP)	210	20%
Total	1,029	100%

Q1b. If yes, did one or more of these data breaches involve the loss or theft of paper documents?	Freq	Pct%
Yes	401	49%
No	418	51%
Total	819	100%

Part 2 of the survey asked respondents to provide their opinions about six statements (attributions) about their organization's response to the security and control of paper documents.

Part 2: Attributions: Please rate your opinion for Q2 to Q7 using the scale provided below each statement.	
Q2. {Attribute 1} My organization has a strict policy for securing and disposing of paper documents with sensitive or confidential information.	Pct%
Strongly agree	13%
Agree	24%
Unsure	41%
Disagree	15%
Strongly disagree	7%
Total	100%

Q3. {Attribute 2} In my organization, there is little risk that employees, temporary employees or contractors would have access to paper documents containing sensitive or confidential information.	Pct%
Strongly agree	11%
Agree	23%
Unsure	46%
Disagree	16%
Strongly disagree	5%
Total	100%

Q4. {Attribute 3} In my organization, employees or contractors recognize what types of information are sensitive or confidential.	Pct%
Strongly agree	4%
Agree	10%
Unsure	51%
Disagree	23%
Strongly disagree	12%
Total	100%

Q5. {Attribute 4} In my organization, paper documents rarely contain sensitive or confidential business information.	Pct%
Strongly agree	3%
Agree	6%
Unsure	32%
Disagree	45%
Strongly disagree	14%
Total	100%

Q6. {Attribute 5} In my organization, controlling access to paper documents with sensitive or confidential information is easier than controlling access to electronic documents with sensitive or confidential information.	Pct%
Strongly agree	3%
Agree	21%
Unsure	20%
Disagree	44%
Strongly disagree	12%
Total	100%

Q7. {Attribute 6} In my organization, there are enough resources and controls available to secure paper documents containing sensitive or confidential information.	Pct%
Strongly agree	6%
Agree	10%
Unsure	23%
Disagree	40%
Strongly disagree	21%
Total	100%

Part 3 provides the core questions about how respondents' organizations are managing, securing and controlling sensitive or confidential information contained on paper documents.

Part 3: Security of paper documents in your organization

Q8. In your opinion, what departments or functions within your organization are most at risk for not being able to protect or secure paper documents? Please check up to three choices.	Total%
Human resources	45%
Finance & accounting	40%
Information technology	38%
Sales	34%
Marketing	17%
Legal & compliance	11%
Research & development	9%
Logistics/distribution	6%
Executive management	4%
Manufacturing	3%
Communications and public relations	2%
Procurement	2%
Total	210%

Q9. In your opinion, how often are employees putting sensitive and confidential paper documents at risk by leaving them at communal printers, in meeting rooms or at meetings held outside the office?	Pct%
Never	5%
Sometimes	28%
Often	35%
Very often	18%
Unsure	14%
Total	100%

Q10. What types of information contained in paper documents do you believe your employees consider most at risk in your organization? Please check up to three choices.	Total%
Employee records, including salaries and employee benefits	45%
Customer information	43%
Management accounting reports and budgets	39%
Marketing & sales reports	22%
Pre-released financial information and forecasts	15%
Legal and/or audit documents	10%
Intellectual property, formulae, source code etc.	10%
Procurement and vendor lists	8%
Strategic documents (including information about mergers and acquisitions)	8%
Details about new product designs	5%
Minutes of executive board meetings	3%
Other	2%
Total	209%

Q11. In your opinion, at what stage of a paper document's life cycle is information most at risk? Please rate the following stages using the five-point scale: 1 = high risk to 5 = low risk.	Avg	Rank	1	2	3	4	5
Before the document is printed (in its electronic format)	3.96	8	3%	2%	26%	33%	36%
When initially printed and in a communal printing tray	2.65	3	16%	30%	31%	18%	5%
At an office desk	2.60	2	27%	17%	31%	20%	6%
In a filing cabinet	3.57	6	4%	7%	29%	46%	13%
In a trash bin	2.25	1	29%	33%	22%	15%	0%
In the process of being circulated internally or mailed	3.58	7	4%	15%	28%	28%	26%
Awaiting disposal or shredding	3.20	5	10%	21%	24%	30%	15%
In document archive or final (permanent) storage	3.10	4	1%	29%	36%	27%	7%
Average by rating	3.11	4.5	12%	19%	28%	27%	13%

Q12a and 12b extrapolate the percentage of respondents' organizations sensitive or confidential information available in paper form. We estimate 50% of all sensitive or confidential information is contained in paper documents, for which only 27% are shredded before disposal.

Q12a. Approximately what percentage of your organization's sensitive or confidential information is available in paper documents?	Pct%	Median	Estimated
Zero (0%)	5%	0.00%	0%
Less than 10%	9%	8.00%	1%
10 to 30%	18%	20.00%	4%
31 to 50%	11%	40.00%	4%
51 to 70%	25%	60.00%	15%
71 to 90%	15%	80.00%	12%
More than 90%	16%	92.00%	14%
Total	100%		50%

Q12b. What percentage of these documents is shredded before disposal?	Pct%	Median	Estimated
Zero (0%)	23%	0.00%	0%
Less than 10%	26%	8.00%	2%
10 to 30%	15%	20.00%	3%
31 to 50%	13%	40.00%	5%
51 to 70%	13%	60.00%	8%
71 to 90%	5%	80.00%	4%
More than 90%	5%	92.00%	5%
Total	100%		27%

Q13a. Are you aware of any incident in your organization in which sensitive or confidential paper documents were lost or misplaced?	Pct%
Yes	71%
No (Go to question 13)	29%
Total	100%

Q13b. If yes, what types of information were in these documents?	Total%
Personal information about customers	59%
Personal information about employees	57%
Don't know	28%
Competitive information	17%
Accounting or financial information	13%
Information about vendors, contractors and customers	6%
Trade secrets	4%
Total	185%

Q14. Please estimate how often an employee, temporary employee or contractor has access to paper documents that are not pertinent to their role or responsibility:	Total%
Never	8%
Sometimes	20%
Often	38%
Very often	9%
Unsure	25%
Total	100%

Q15. Who is accountable within your organization for granting access to paper documents containing sensitive or confidential information? Please check only two responses.	Total%
Information technology department	15%
Information security department	12%
Legal, risk or compliance department	22%
Business unit leaders	52%
Human resource department	31%
Unsure	55%
Total	187%

Q16a. Does your organization have a policy that explains how paper documents with sensitive or confidential information should be secured and disposed of safely?	Pct%
Yes	78%
No (Go to question 17a)	22%
Total	100%

Q16b. If yes, do employees in your organization receive training about this policy to understand what types of information in your organization are considered sensitive and confidential?	Pct%
Yes	29%
No	71%
Total	100%

Q17a Does your organization have a process for disposing of paper documents containing sensitive or confidential information after they are no longer needed?	Pct%
Yes	46%
No (Go to question 18)	54%
Total	100%

Q17b. If yes, what steps are taken to safely dispose of paper documents within your organization?	Pct%
Training of employees about secure disposal	21%
Enforcing a policy on secure disposal	13%
Shredding documents in each office area	35%
Collecting documents from each office area for centralized in-house shredding	29%
Collecting documents from each office area for centralized off-site shredding	33%
Collecting paper documents from outside vendors for safe disposal	18%
Automated print restriction on specific devices	19%
Automated print restrictions on specific files	3%
Other (please specify)	2%
Total	173%

PAPER: Q18. How well is your organization able to govern the use, protection and disposal of paper documents and electronic documents? Please use the following scale to rate each task provided. 1 = excellent, 2 = good, 3 = fair, 4 = poor, 5 = procedure is not performed	**Avg**	**Rank**	**1**	**2**	**3**	**4**	**5**
Assign access rights based on job function or role	3.23	3	6%	13%	46%	25%	11%
Establish information ownership and accountability for protection and control.	3.45	4	9%	13%	31%	18%	29%
Enforce access policies in a consistent fashion across all enterprise information resources.	3.72	6	5%	21%	19%	7%	48%
Keep logs showing those viewing or accessing information.	4.13	7	8%	3%	18%	9%	62%
Educate users about access procedures to information.	3.46	5	6%	14%	37%	12%	31%
Communicate known breaches to appropriate management.	2.29	1	24%	39%	20%	16%	1%
Establish, monitor and enforce data retention procedures.	3.09	2	10%	14%	38%	32%	6%
Average	3.34	4.0	10%	17%	30%	17%	27%

ELECTRONIC: Q18. How well is your organization able to govern the use, protection and disposal of paper documents and electronic documents? Please use the following scale to rate each task provided. 1 = excellent, 2 = good, 3 = fair, 4 = poor, 5 = procedure is not performed.	**Avg**	**Rank**	**1**	**2**	**3**	**4**	**5**
Assign access rights based on job function or role	2.64	2	16%	29%	36%	15%	5%
Establish information ownership and accountability for protection and control.	2.77	4	17%	20%	40%	18%	6%
Enforce access policies in a consistent fashion across all enterprise information resources.	2.70	3	23%	21%	29%	17%	10%
Keep logs showing those viewing or accessing information.	2.80	5	18%	25%	22%	29%	6%
Educate users about access procedures to information.	3.04	7	11%	34%	16%	17%	22%
Communicate known breaches to appropriate management.	2.02	1	30%	42%	24%	3%	1%
Establish, monitor and enforce data retention procedures.	2.89	6	10%	25%	36%	22%	6%
Average	2.69	4.0					

Q19. How confident are you that your organization has visibility to all users of sensitive or confidential business information contained in paper documents and electronic files?	**Paper**	**Electronic**
Very confident	3%	7%
Confident	12%	21%
Somewhat confident	32%	43%
Not confident	53%	29%
Total	100%	100%

Q20. What are the critical success factors for implementing controls over paper documents across your enterprise? Please rate the following success factors using the following scale: 1 = Very important, 2 = important, 3 = sometimes important, 4 = not important, 5 = irrelevant.	Avg	Rank	1	2	3	4	5
Senior level executive support	2.19	3	32%	27%	31%	8%	1%
Ample budget	2.32	4	30%	25%	30%	11%	3%
Technologies that restrict printing or copying of sensitive or confidential materials	2.59	6	24%	21%	38%	5%	12%
Clear and concise policies and standard operating procedures for document classification based on level of sensitivity or confidentiality.	3.24	10	10%	15%	32%	28%	16%
Shredding machines that are easily accessible by employees.	2.06	2	40%	30%	19%	5%	6%
Employee education or training and document handling and safe disposal	2.75	7	12%	29%	35%	20%	4%
Access rights assigned using role or function-based methods	2.89	9	19%	15%	40%	10%	16%
Rigorous compliance procedures for document protection and safe disposal	2.46	5	27%	34%	16%	14%	9%
Strict enforcement of non-compliance with document handling and disposal procedures	1.77	1	37%	31%	40%	1%	-9%
Monitoring of users	2.81	8	20%	26%	18%	25%	11%
Average	2.51	5.5	25%	25%	30%	13%	7%

Q21. In your opinion, how has the availability and use of printed or hardcopy materials within your organization changed during the last 24 months?	Pct%
Decreased over time.	13%
Stayed the same over time.	37%
Increased over time.	28%
Can't determine.	22%
Total	100%

Q22. In your opinion, why is the security of printed or paper documents important? Please select your top reason.	Pct%
To reduce identity theft from stolen customer information	29%
To reduce identity theft from stolen employee information	29%
To reduce loss of trade secrets and other proprietary information leaked to competitors	9%
To reduce exposure of the company's sensitive or confidential information that may impact the brand	23%
To reduce the risk of litigation and fines	5%
To reduce inefficiencies in the management of printed materials	3%
To reduce leakage of information about financial results	1%
Total	100%

Q23. Please rank your organization's paper document management priorities for the following five (5) key activities from 1=highest to 5=lowest. If possible, avoid tied ranks.	Avg	Rank	1	2	3	4	5
Protecting information from leaking out	1.81	1	37%	51%	6%	6%	0%
Instituting document disposal procedures such as a company-wide shredding program	2.48	2	23%	35%	16%	24%	3%
Migrating documents to an enterprise content management system such as SharePoint	2.80	3	14%	27%	32%	19%	8%
Streamlining document retention practices to reduce clutter	4.21	5	2%	5%	12%	32%	49%
Classifying content based on sensitivity level	3.63	4	3%	10%	36%	24%	27%
Average	2.99	3	16%	25%	20%	21%	17%

Part 4 attempts to measure the economic impact of paper document insecurity within both business and governmental organizations. As can be seen, 688 respondents completed this section based on a YES response to Q24a.

Part 4: Economic impact

Q24a. Based on your experience, does your organization lose time, money and other resources as a result of lost, missing or stolen business information?	Freq	Pct%
Yes	688	84%
No (Go to Part 5)	13	2%
Unsure (Go to Part 5)	118	14%
Total	819	100%

Q24b. If yes, please estimate how much money your organization has lost due to lost, missing or stolen business information per year?	Pct%	Median value ($000,000)	Estimated value ($000,000)
Less than $1 million	4%	0.8	0.03
Between $1 to $2 million	3%	1.5	0.05
Between $2 to $5 million	2%	3	0.06
Between $5 to $10 million	6%	7.5	0.44
Between $10 to $15 million	14%	12.5	1.70
Between $15 to $20 million	20%	17.5	3.52
Between $20 to $30 million	12%	25	3.12
Between $30 to $40 million	6%	35	2.07
Between $40 to $50 million	2%	45	0.70
Between $50 to $100 million	4%	75	2.76
Between $100 to $200 million	12%	150	18.13
Over $200 million	16%	220	34.95
Total	100%		$67.53

Q24c. Approximately, what percentage of this financial loss is due to lost, missing or stolen business information contained in paper documents?	Pct%	Median prob value	Estimated prob value
Less than 5%	2%	0.025	0.04%
Between 5% to 10%	9%	0.075	0.71%
Between 10% to 20%	9%	0.15	1.37%
Between 20% to 30%	17%	0.25	4.14%
Between 30% to 40%	21%	0.35	7.46%
Between 40% to 50%	21%	0.45	9.61%
Between 50% to 60%	15%	0.55	8.46%
Between 60% to 70%	2%	0.65	1.09%
Between 70% to 80%	0%	0.75	0.19%
Between 80% to 90%	2%	0.85	1.80%
Between 90% to 100%	1%	0.95	1.16%
Total	100%		36.02%

Q24d. Please allocate your organization's percentage of financial loss to the following root causes. Please express your allocation to the nearest 10% with the sum of your allocation totaling 100%.	Percentage must sum to 100%
Loss of trade secrets	26%
Loss of competitive information	29%
Loss of personal information about customers	31%
Loss of personal information about employees	5%
Loss of information about vendors, contractors and customers	3%
Loss of accounting or financial information	3%
Compliance violations resulting in fines and penalties	1%
Lawsuits and legal actions	1%
Total	100%

Organizational Characteristics

Part 5 of the survey asked respondents to complete several questions that defined their position levels, organization and related business experiences.

What organizational level best describes your current position?	Pct%
Senior Executive	1%
Vice President	2%
Director	13%
Manager	22%
Supervisor	25%
Technician/staff level	27%
Other	10%
Total	100%

Check the **Primary Person** you or your IT security leader reports to within the organization.	Pct%
IT Operations	29%
Application development	2%
Compliance	10%
Research	1%
Human resources	5%
Procurement	2%
Security	41%
Risk management	8%
Total	100%

Location	Pct%
Northeast	20%
Mid-Atlantic	17%
Midwest	15%
Southeast	13%
Southwest	11%
Pacific	18%
Outside U.S.	7%
Total	100%

Experience levels	Mean
Total years of business experience	8.91
Total years of IT or security experience	8.03
Total years in current position	3.99

What is the worldwide headcount of your organization?	Pct%
Less than 500 people	4%
500 to 1,000 people	10%
1,001 to 5,000 people	21%
5,001 to 25,000 people	34%
25,001 to 75,000 people	19%
More than 75,000 people	11%
Total	100%

What is the approximate size of your IT department in terms of full-time equivalent (FTE) headcount?	Pct%
Less than 5 people	3%
5 to 50 people	2%
51 to 100 people	7%
101 to 500 people	12%
500 to 1,000 people	15%
1,001 to 5,000 people	23%
5,001 to 10,000 people	23%
Over 10,000 people	15%
Total	100%

What industry best describes your organization's industry focus?	Pct%
Financial services	20%
Government	14%
Technology & Software	10%
Healthcare & pharma	9%
Manufacturing	8%
Communications	6%
Hospitality & Leisure	2%
Transportation	6%
Retailing	8%
Professional Services	4%
Defense	2%
Education	7%
Energy	1%
Entertainment and Media	1%
Other	1%
Total	100%

Is your organization subject to any of the following data protection or privacy regulatory requirements? Please check all that apply.	Total%
HIPAA	10%
Sarbanes Oxley	19%
PCI	79%
Federal Privacy Act	8%
Basel II	10%
European Union Data Protection Directive	24%
Gramm-Leach-Bliley (GLBA)	17%
Data breach notification laws (various states)	83%
FACTA	68%
Total	317%