2012 Confidential Documents at Risk Study

Sponsored by

WatchDox

Independently conducted by Ponemon Institute, LLC

Publication Date: July 2012

2012 Confidential Documents at Risk Study

Ponemon Institute, July 2012

Part 1. Introduction

Ponemon Institute is pleased to present the results of the *2012 Confidential Documents at Risk Study*. Sponsored by WatchDox, this is the first research study on the state of document-centric security in today's corporate environment. In the wake of WikiLeaks and other document leakage incidents involving highly sensitive information, it is clear that organizations must address security issues related to how they store, share and collaborate on documents.

Specifically, this research attempts to determine the enormous security threats and risks associated with inadequate safeguards over the plethora of confidential business information contained in documents, spreadsheets, presentations, email attachments, mobile devices and more. We also look at the technologies, governance practices and controls necessary to achieving a stronger document-centric security posture.

The tremendous growth in the use of browser-based file sharing applications such as Yousendit!, Dropbox and others have had a positive affect on workplace productivity but also pose privacy and security risks. According to a study by Palo Alto Networks[1], data loss, purposeful or not, and copyright violations are most common business risks. The study looked at application usage in 2,036 organizations worldwide between November 2011 and May 2012 and found an average of 13 different browser-based file sharing documents on each network.

It also seems that organizations are not aware how pervasive the use of these applications is. In this study, more than half (51 percent) of respondents say their employees use at least one browser-based file sharing tools. However, more than one-third (34 percent) of respondents do not know the extent to which these applications are being used in the workplace.

Concerns about the vulnerability of confidential documents exist at all levels of an organization. According to the IT practitioners in our study, document-centric security is most important to reducing the risk of insider negligence and the risks that can negatively impact the business such as the leakage of confidential information.

In another Ponemon Institute study,[2] senior executives surveyed believe the most important information to safeguard is non-financial confidential business information, typically stored as unstructured data. However, these executives also believe this information is most difficult to protect due to the nature of the risks.

Risks to sensitive documents include[3]:

- An authorized insider accidentally (or maliciously) forwarding a document
- An employee leaving the company with documents copied to his or her thumb drive
- An authorized third-party transmitting documents that had been shared with the third party
- A third party that is no longer authorized to access certain documents, but already has these documents in his or her possession, etc.

[1] *The Application Usage & Risk Report: An Analysis of End User Application Trends in the Enterprise*, 9th Edition, Palo Alto Networks, June 2012

[2] *The Business Case for Data Protection: What Senior Executives Think about Data Protection,* conducted by Ponemon Institute and sponsored by IBM, March 2012

[3] *Secure Document Sharing & Online Workspaces for Financial Institutions* by Adi Rupin, CTO WatchDox, February 2012

In this study, we surveyed 622 IT and IT security practitioners (hereafter referred to as IT practitioners) in the United States. On average, respondents have more than 11 years IT or IT security experience and most (56 percent) report to the chief information officer. Fifty-seven percent are employed by organizations with a worldwide headcount of more than 1,000.

Some of the most interesting findings from this research include:

- Ninety percent of organizations represented in this study experienced the leakage or loss of sensitive or confidential documents over the past 12-month period.
- Seventy-one percent of respondents say that controlling sensitive or confidential documents is more difficult than controlling records in databases.
- Seventy percent say documents accessed by mobile data-bearing devices such as smart phones and tablets present a significant security risk.
- Seventy percent of respondents say that employees, contractors or business partners have very frequent or frequent access to sensitive or confidential documents, even though access to this information is not a job or role-related requirement.
- Further, 59 percent say their organization’s controls are ineffective at monitoring employees, contractors or other insiders who access these confidential documents. An even higher percentage (63 percent) do not believe they are effective at assigning privilege to employees, contractors and other insiders whose job or role requires access to sensitive or confidential documents.

Part 2. Key Findings

In this section, we provide the detailed analysis of this research. The complete findings are presented in the appendix to this paper. Topics are organized according to the following themes:

- Awareness of risk to confidential documents
- The negligent insider risk and practices that lead to the loss or theft of confidential documents
- The ability to achieve effective document-centric security and to have the necessary controls in place to mitigate the risk
- Critical success factors and security solutions

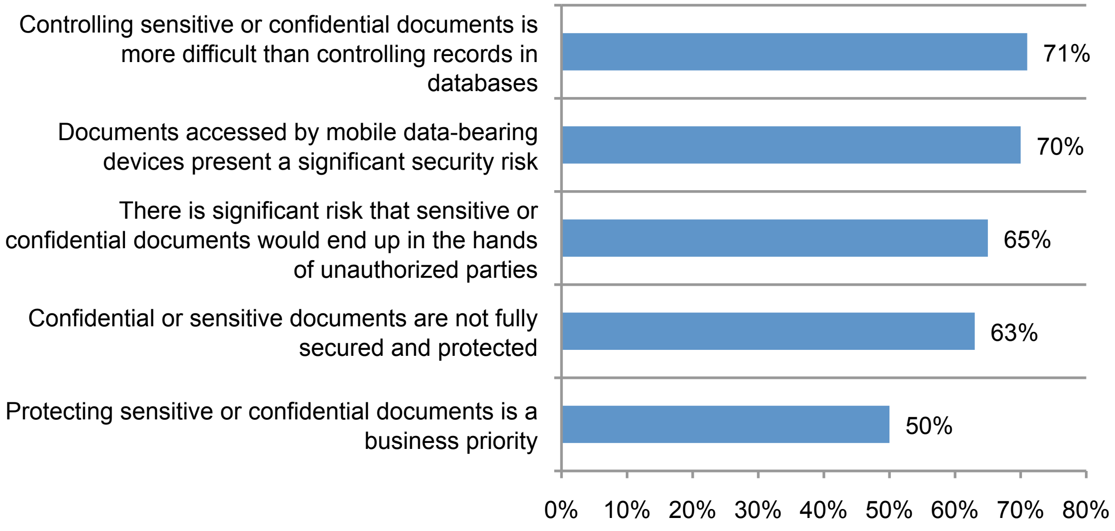
Awareness of risk to an organization's confidential documents

IT practitioners are aware of the risk to confidential documents. Ninety percent of respondents say they are certain (35 percent) or believe it was very likely (55 percent) their organization experienced the leakage or loss of sensitive or confidential documents during the past 12 months.

Based on this experience, respondents are very much aware of the risk to their confidential documents. Figure 1 reveals that 71 percent believe controlling sensitive or confidential documents is more difficult than controlling records in databases and 70 percent say documents accessed by mobile data-bearing devices such as smart phones and tablets present a significant security risk.

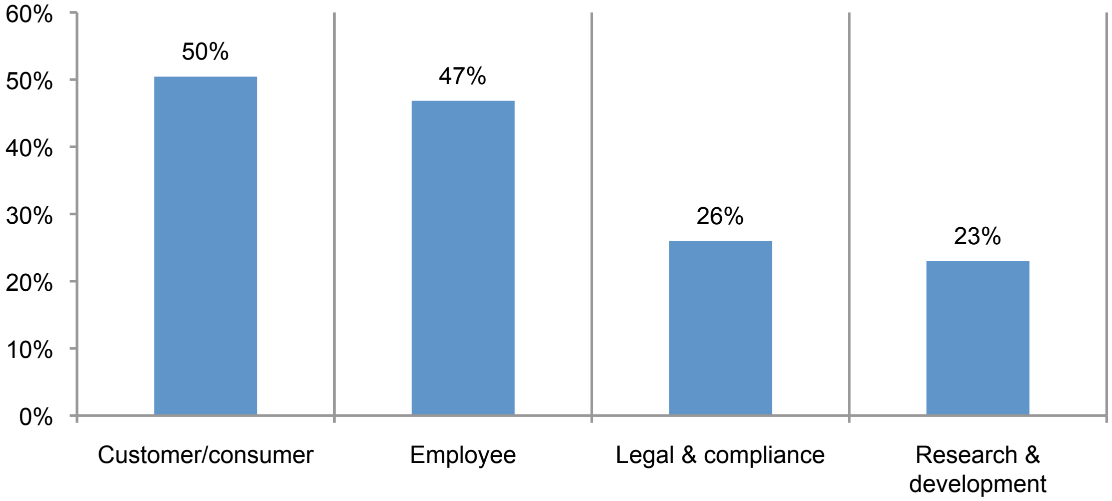
Also shown in Figure 1, 63 percent of respondents do not believe their organizations' confidential or sensitive documents are fully secured and protected and 65 percent believe that there is a risk that these documents could end up in the hands of unauthorized parties such as a competitor. Despite this awareness, only 50 percent say it is a business priority.

Figure 1. Perceptions about data security
Strongly agree and agree response combined



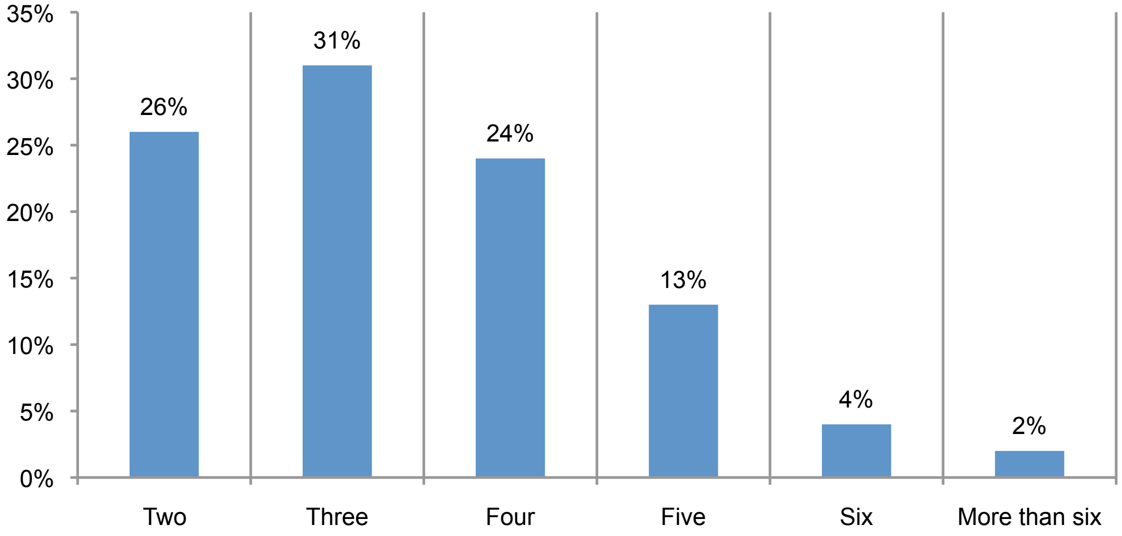
Customer and consumer documents are most at risk. According to 50 percent of respondents, customer and consumer documents are most at risk (Figure 2). This could be attributed to the volume of this information and the access employees and others have to these records. Employee records follow closely at 47 percent. Posing less of a risk are legal and compliance and research development documents, according to 26 percent and 23 percent respectively. Not shown in the figure below are types of information considered less risky. These are: sales (21 percent), finance and accounting (12 percent) and executive or board documents (seven percent)

Figure 2. Information considered most at risk
Two choices permitted



The majority of organizations (67 percent) do have a method for classifying the confidentiality of documents as part of their efforts to assign access rights. The more levels an organization uses show how well it understands the confidential and sensitive information that exists in documents and are most in need of securing. According to the findings shown in Figure 3, 56 percent use two or three levels of confidentiality or sensitivity and the extrapolated average is 3.5 levels.

Figure 3. Levels of confidentiality or sensitivity the organization uses for classification

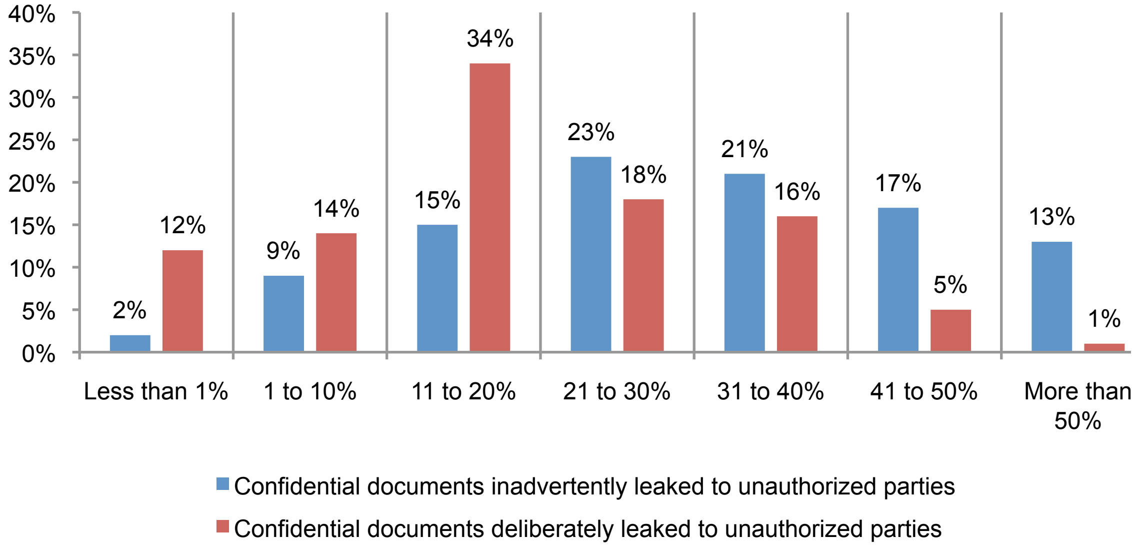


Organizations' experience with the leakage of their confidential documents and areas where they are most vulnerable

The negligent insider seems to pose the greatest risk in part because of poor internal controls. As mentioned above, 90 percent of the respondents say it is certain (35 percent) or most likely (55 percent) their organizations experienced the loss of sensitive or confidential documents during the past year.

Figure 4 reveals that based on an extrapolated average, 31 percent of the sensitive or confidential documents were leaked by unauthorized individuals because of carelessness or internal control issues. In contrast, malicious or criminal insiders, based on an extrapolated average, were cited as leaking 19 percent of these documents.

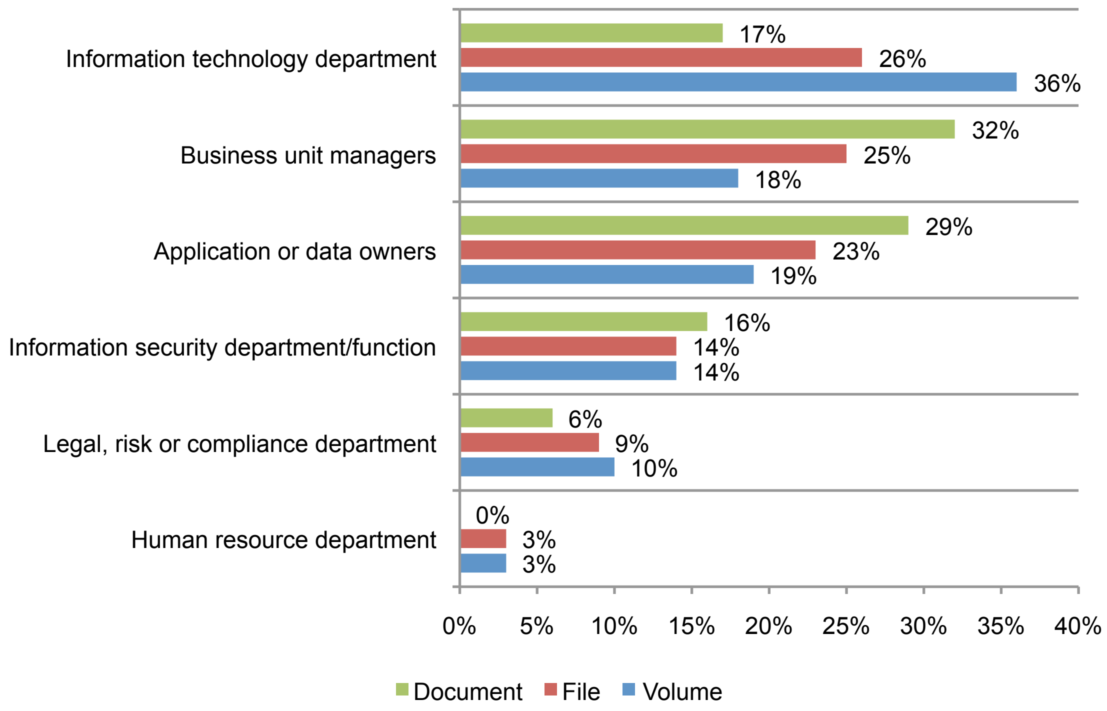
Figure 4. Documents inadvertently and deliberately leaked to unauthorized users



Sensitive documents are most at risk at the document and file level. According to 37 percent of respondents, the greatest threat is when sensitive and confidential information is at the document level and 33 percent say it is at the file level. Only 11 percent say this information is at risk at the volume level or in databases.

Figure 5 shows the functions respondents believe are most responsible for managing and controlling sensitive information. At the file and document level they are business unit managers and application or data owners. Information technology is most responsible for information at the volume level.

Figure 5. Who manages access to confidential information?

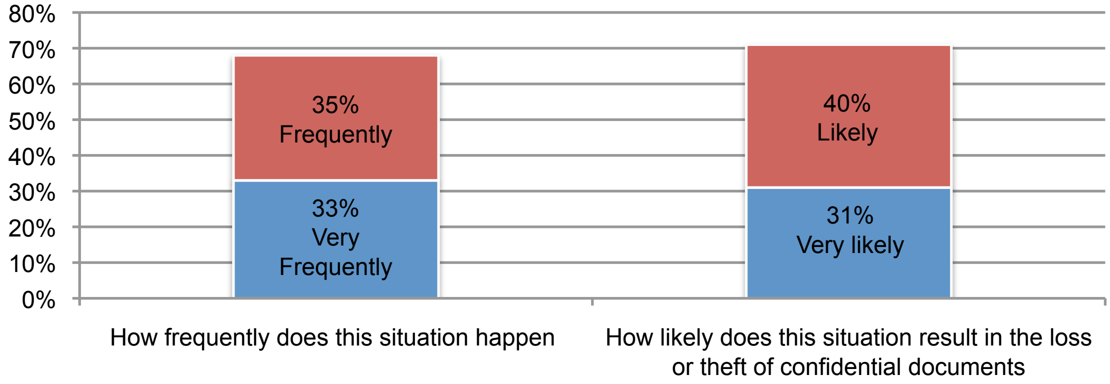


Common practices are putting sensitive documents at risk. Because of employees' improperly accessing and transferring this information there is great risk of losing or having confidential documents stolen. In this study, respondents were asked to respond to five scenarios that can occur in organizations involving negligent or malicious employees.

Respondents were asked their opinion about the frequency of these events occurring and the likelihood that they could result in the loss or theft of confidential information. As revealed, the majority of respondents believe all these situations happen frequently and can result in lost or stolen documents. The following scenarios are listed according to highest frequency and risk.

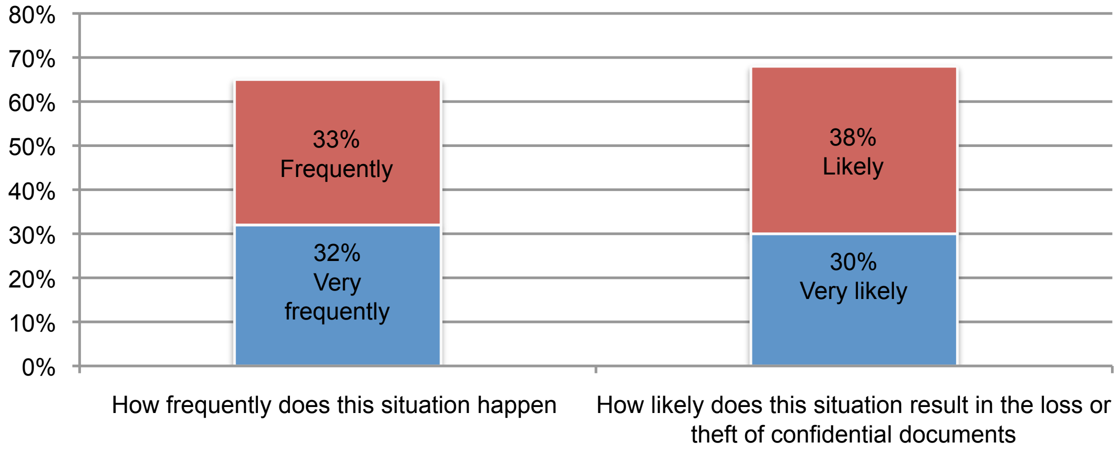
Scenario 1: **Employees attach and send confidential documents (in clear text) from the workplace using web-based (personal) email accounts**. Sixty-eight percent of respondents say this very frequently or frequently happens and 71 percent say it results in the loss or theft of confidential documents (Figure 6).

Figure 6. Employees attach and send confidential documents using personal email



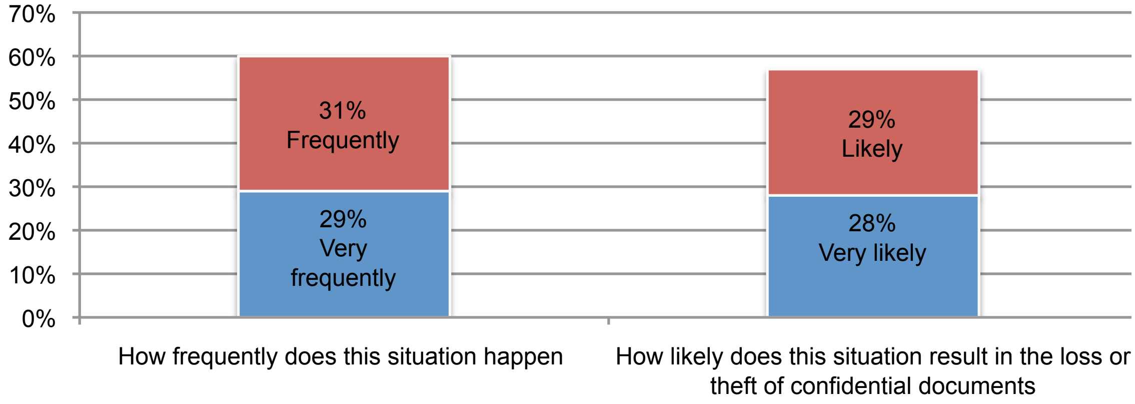
Scenario 2: Employee downloads, temporarily stores and transfers confidential documents (in clear text) from workplace desktop to a generic USB drive. Sixty-five percent say this frequently or very frequently happens and 68 percent say it results in the loss or theft of confidential documents (Figure 7).

Figure 7. Employee downloads, temporarily stores and transfers confidential documents to USB drive



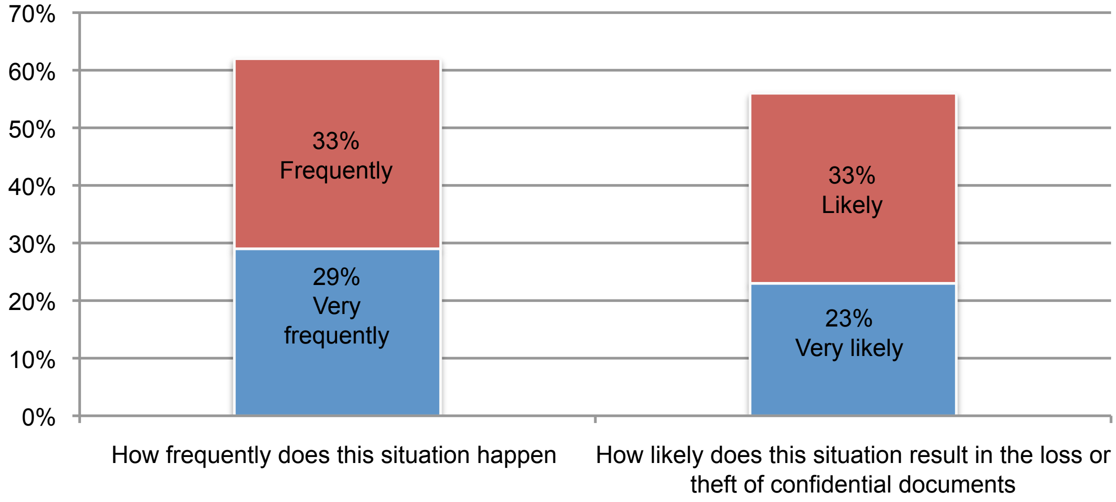
Scenario 3: After registering with Dropbox, an employee moves several large files containing business confidential information to this filesharing application. The employee did not obtain permission from the employer to use Dropbox. According to 60 percent of respondents, this very frequently or frequently occurs and 57 percent believes it can result in the leakage of confidential information (Figure 8).

Figure 8. Employee moves confidential files to Dropbox without permission



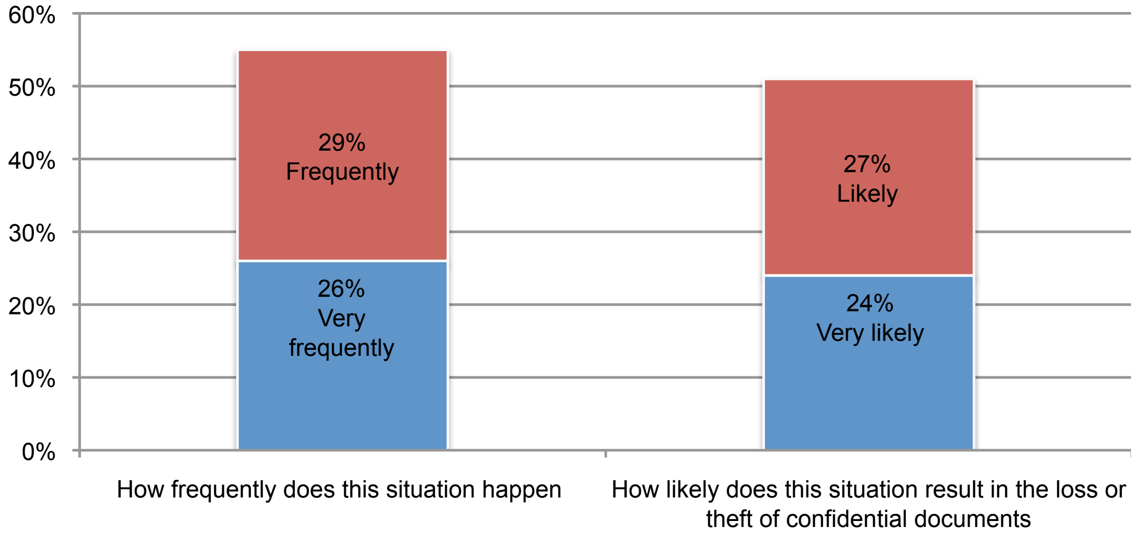
Scenario 4: Employees download confidential documents to a public drive, thus allowing other employees to view and use this information from various mobile devices, including those owned by employees (BYOD). Sixty-two percent say this very frequently or frequently happens and 56 percent say it can result in the loss or theft of confidential documents (Figure 9).

Figure 9. Confidential documents downloaded to a public drive to allow access by mobile devices



Scenario 5: Employees download confidential documents to a public drive. The purpose is to collaborate with business partners. This allows them to view and use the information on their tablet computers (such as an iPad). Fifty-five percent say this very frequently or frequently happens and slightly more than half (51 percent) say it results in leakage of these documents (Figure 10).

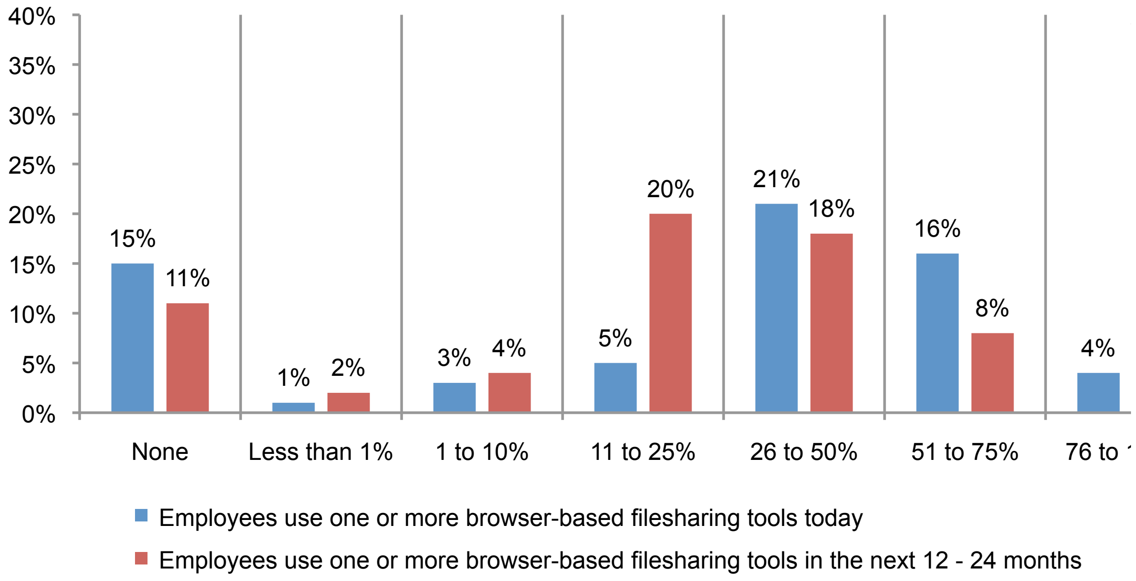
Figure 10. Employees download confidential documents to public drive to collaborate with business partners



An area of growing vulnerability is employees' use of browser-based file sharing tools and their importance is expected to increase. On average, employees are using slightly more than two browser-based file sharing tools like Yousendit!, Dropbox, Box.net and others. Currently, respondents say that based on an extrapolated average, 34.5 percent of employees use these tools and this is expected to increase to an average of 42 percent.

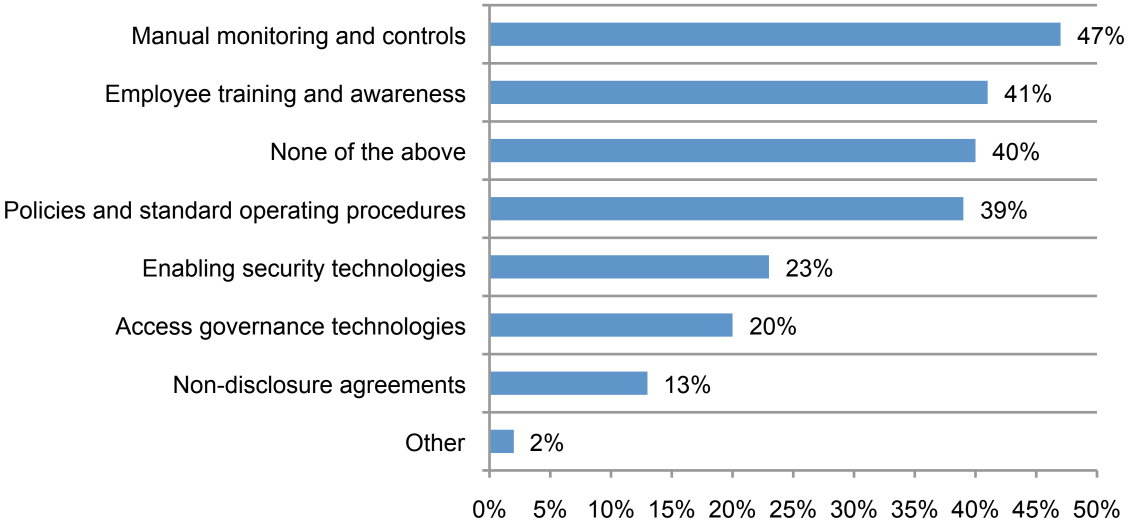
However, despite the risk identified in the third scenario, only 50 percent say it will become more important to secure and protect the sensitive or confidential documents in browser-based file sharing tools over time.

Figure 11. Employees' use of browser-based file sharing tools today and in the near future



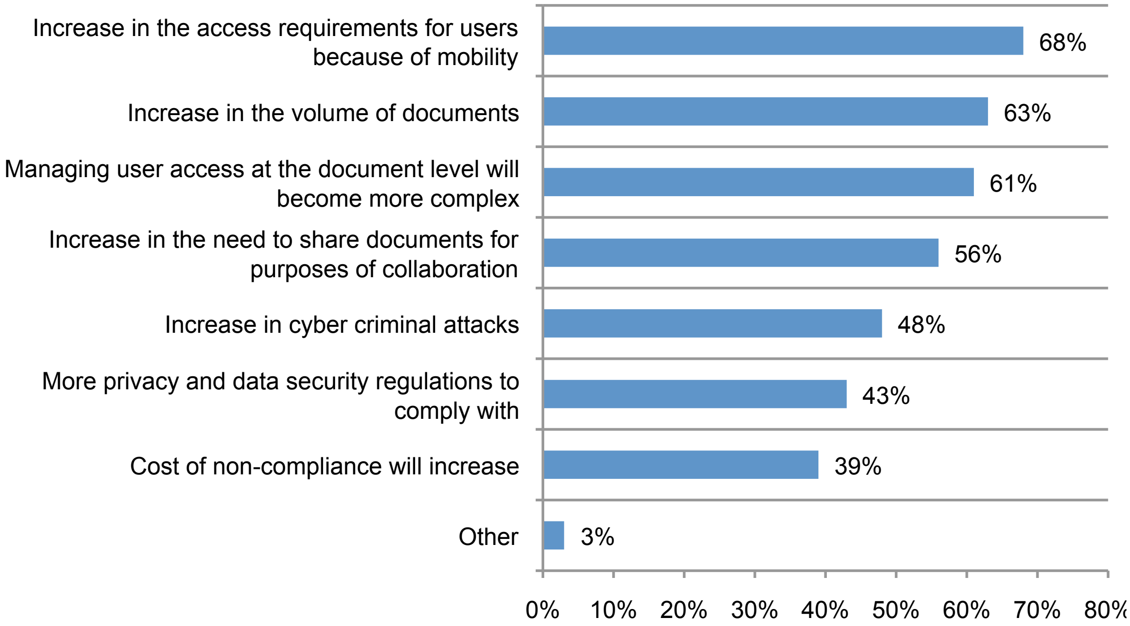
As shown in Figure 12, organizations typically are using manual monitoring and controls (47 percent) and employee training and awareness (41 percent). Forty percent say they are not doing any of the suggested steps.

Figure 12: Steps taken to reduce risk of browser-based file sharing tools



According to Figure 13, of the 50 percent who say it will become more important to increase browser-based security, the following are the primary reasons given: increase in access requirements for users because of mobility, increase in the volume of documents, managing user access at the document level will become more complex and increase in the need to share documents for purposes of collaboration.

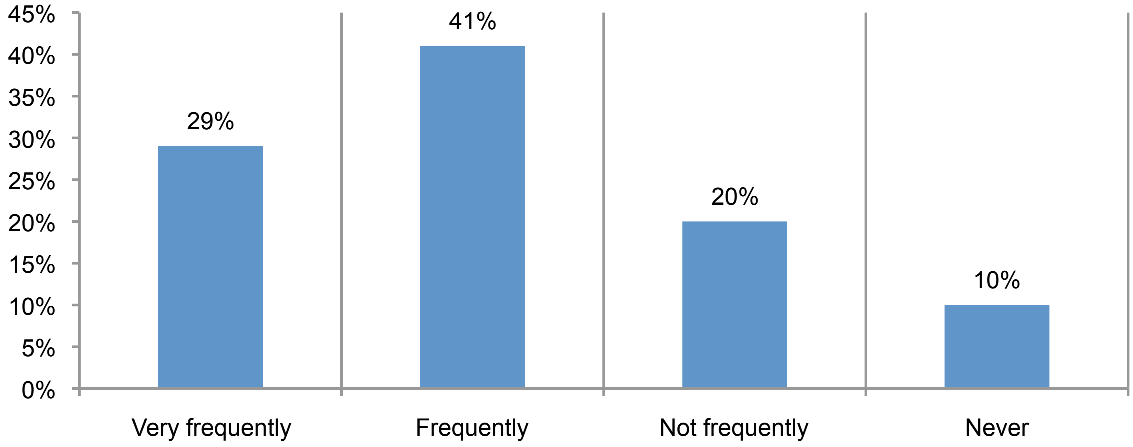
Figure 13. Reasons security of browser-based file sharing will become more important
More than one response permitted



Effectiveness of organizations' ability to achieve document-centric security and the controls in place to mitigate the risk

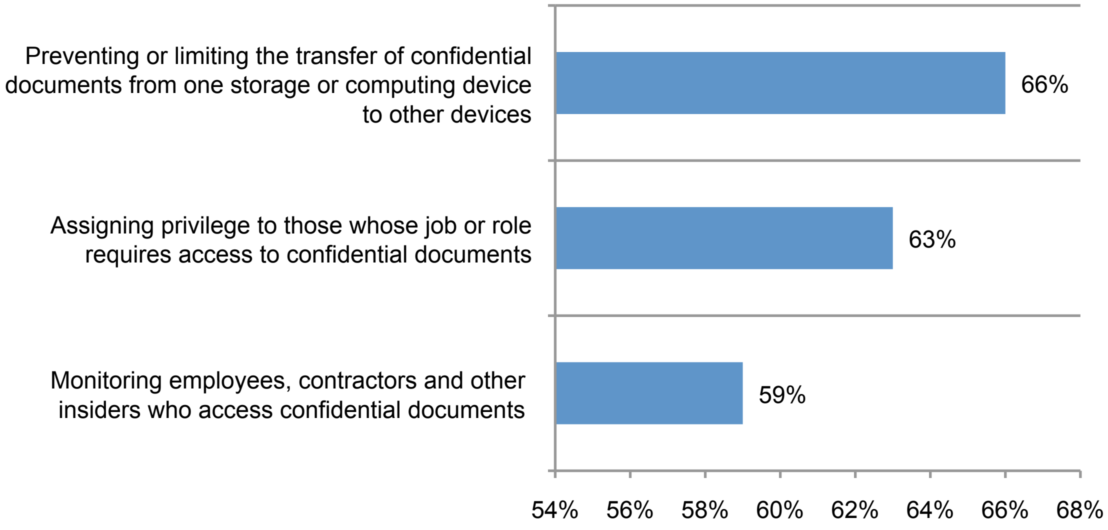
As the findings reveal, respondents are aware of the risk and the gaps that exist in addressing the risk to confidential documents. A contributing factor to the risk is that 70 percent of respondents say that employees, contractors or business partners have very frequent or frequent access to sensitive or confidential documents even though access to this information is not a job or role-related requirement (Figure 14).

Figure 14. Frequency of access to confidential documents



As shown in Figure 15, 59 percent say their controls are ineffective at monitoring employees, contractors and other insiders who access these confidential documents. However, an even higher percentage do not believe they are effective at assigning privilege to employees, contractors and other insiders whose job or role requires access to sensitive or confidential documents or preventing or limiting the transfer of these documents from one storage or computing device to other devices, 63 percent and 66 percent, respectively.

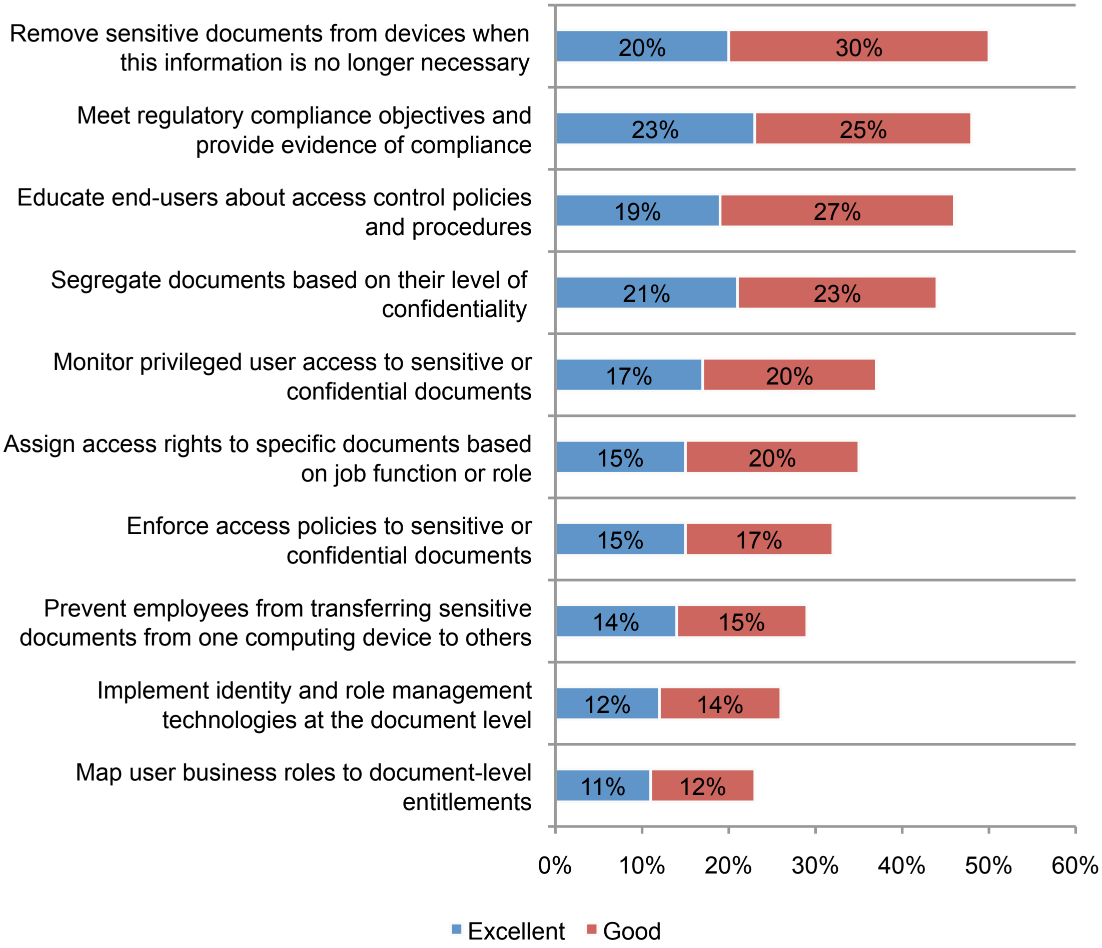
Figure 15. Ineffectiveness of document control process



Governance tasks or procedures for privilege and access to sensitive documents are in need of improvement. Figure 16 reveals a scorecard that rates how well organizations are completing certain governance procedures. Fifty percent say they are excellent or good at removing sensitive or confidential documents from storage or computing devices when information is no longer needed.

However, respondents do not give their organizations high marks for the more difficult and critical steps. These include monitoring privilege user access, assigning access rights to specific documents based on job function or role, preventing employees from transferring documents from one computing device to others and enforcing access policies to these documents are rated fair, poor or not being done by the majority of respondents.

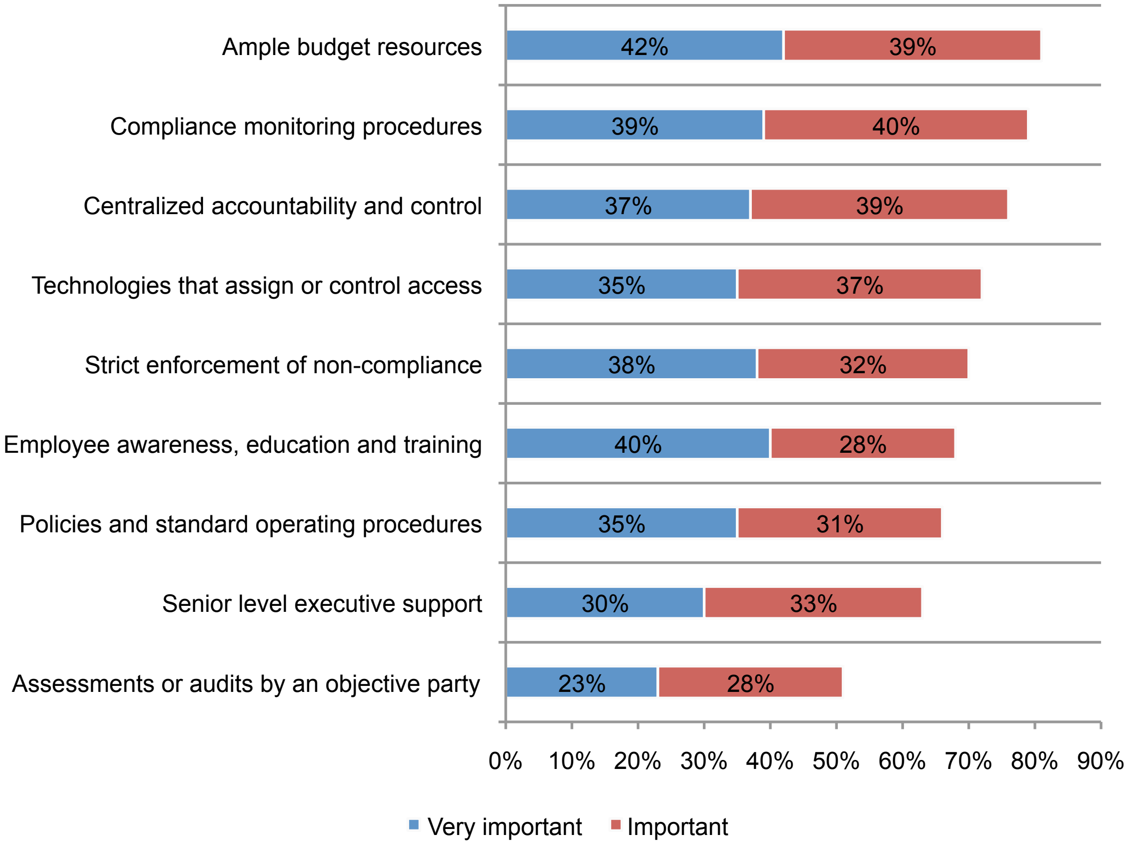
Figure 16. Scorecard ranking of governance procedures



Critical success factors and security solutions

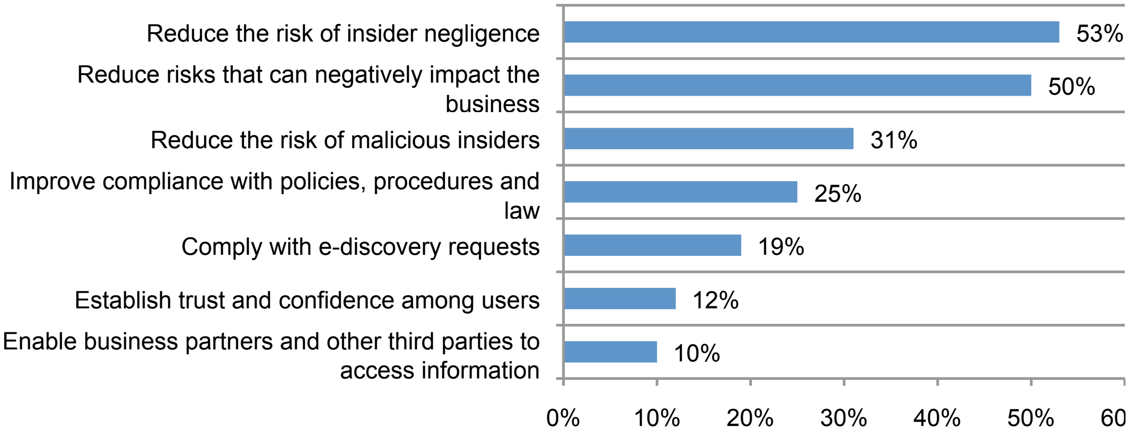
Critical success factors to achieving good internal controls and governance procedures focus on budget, monitoring and access technologies. In order to succeed in the implementation of governance and control practices and improve the scorecard, respondents say they need the funding, compliance monitoring procedures, centralized accountability and control, technologies that assign or control access and strict enforcement of non-compliance (Figure 17).

Figure 17. Critical success factors for implementing control practices



Document-centric security is important to reducing the risk of insider negligence and negative consequences to the organization. We asked the IT practitioners in our study why document-centric security is important. They believe, as shown in Figure 18, that document-centric security is critical to addressing the insider threat to their confidential documents and unstructured data. Reducing the risks that can negatively impact the business is the second most important reason.

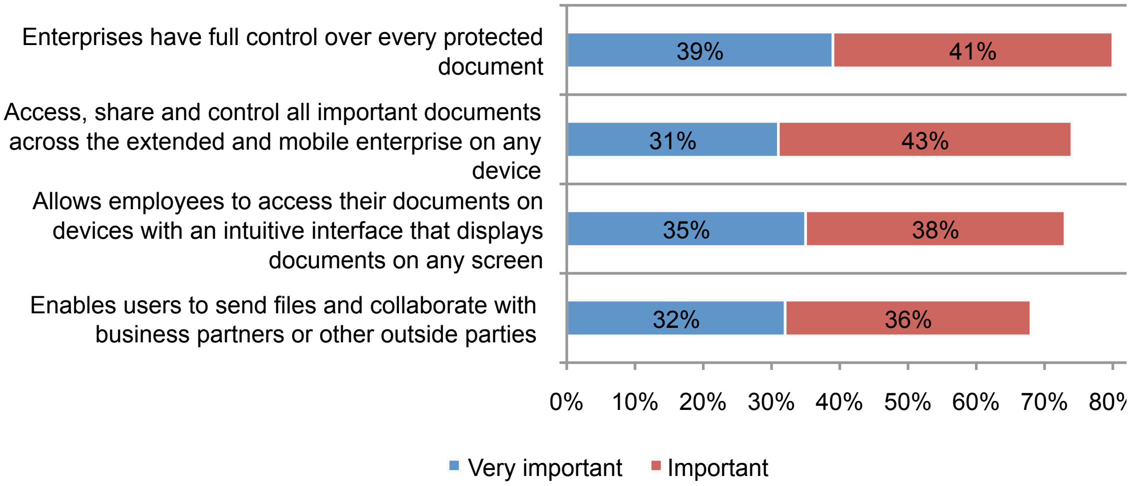
Figure 18. Why document-centric security is important
Two choices permitted



To achieve an optimum level of security, Figure 19 shows the features that are most critical. The most important feature of a document-centric security solution is giving enterprises full control over every protected document so that printing, copying, forwarding and watermarking or wiping the document can be done.

Also important is the ability for enterprises to easily and effectively access, share and control all important documents across the extended and mobile enterprise on any device—even those beyond the IT organization's control. Finally, it is the ability to easily access their corporate documents on PC and mobile devices with an intuitive interface that displays documents perfectly on any screen.

Figure 19. Critical features of document-centric security



Part 3. Conclusion

This research spotlights the pervasive risk to an organization's confidential business information contained in documents, spreadsheets, presentations, email attachments, mobile devices and more. Virtually all organizations in this study have experienced the leakage of these documents. The majority of respondents also believe such commonplace practices as downloading and sharing documents will result in them ending up in the wrong hands.

Organizations should consider an approach that involves the following:

- Identifying information that needs to be secure and protected at all times and enabling full control over every protected document
- Preventing documents from being accidentally or maliciously forwarded
- Accessing, sharing and controlling all important documents across the extended and mobile enterprise on any device
- Allowing employees to access their documents on devices with an intuitive interface that displays documents on any screen
- Enabling users to send files and collaborate with business partners or other outside parties
- Keeping third parties from transmitting documents to other third parties
- Removing access to documents at any time even from an unsecured PC or mobile device

The solution to mitigating the risk is not to stop sharing and collaboration, which is essential to a productive workplace. Rather it is putting solutions in place that will keep these documents secure without requiring draconian end-user security measures that will stifle productivity.

Part 4. Methods

A random sampling frame of 19,190 IT and IT security practitioners located in all regions of the United States were selected as participants to this survey. As shown in Table 1, 708 respondents completed the survey. After removing 86 surveys that failed reliability checks, the final sample was 622 surveys (or a 3.2 percent response rate).

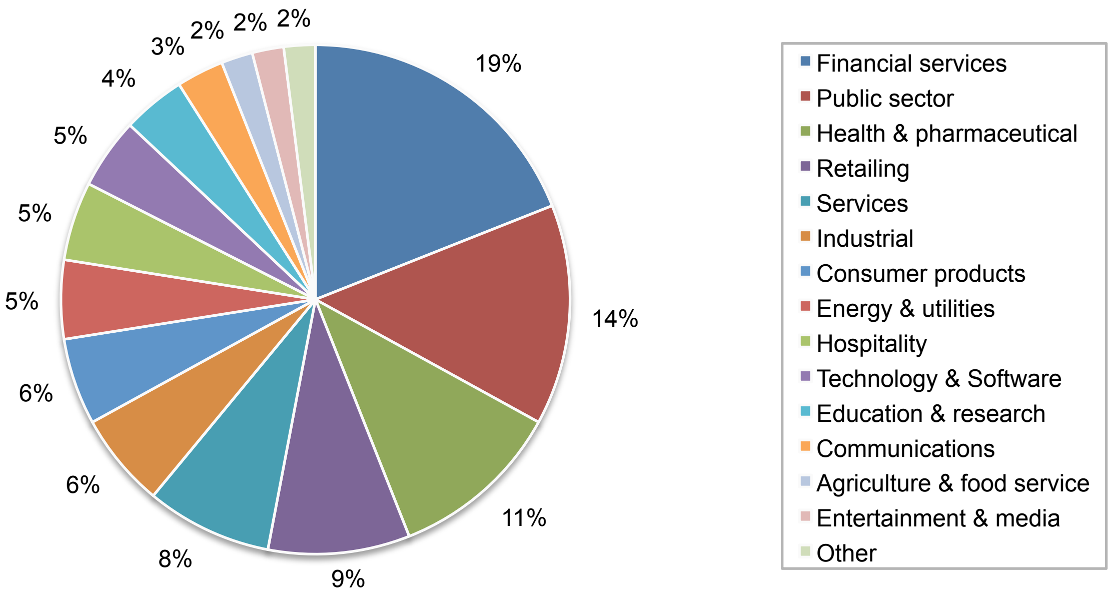
Table 1. Sample response	Freq.	Pct%
Total sampling frame	19,190	100.0%
Total returns	708	3.7%
Rejected returns	86	0.4%
Final sample	622	3.2%

As noted in Table 2, the respondents' average (mean) experience in IT, IT security or related fields is 11.60 years.

Table 2. Other characteristics of respondents	Mean
Total years of IT or IT security experience	11.60
Total years in your current position	5.90

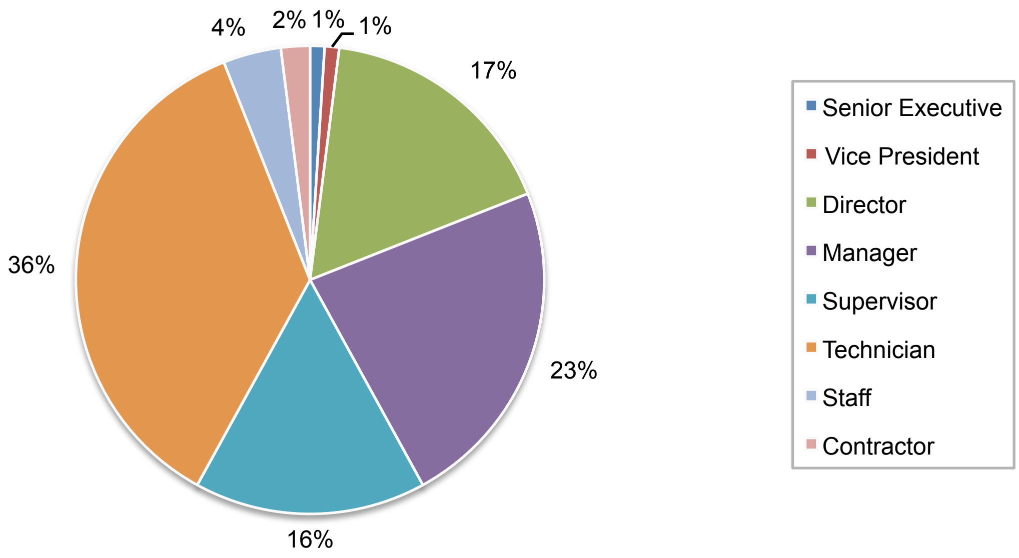
Pie Chart 1 reports the industry segments of respondents' organizations. This chart identifies financial services (19 percent) as the largest segment, followed by public sector (14 percent) and health and pharmaceutical (11 percent).

Pie Chart 1. Industry distribution of respondents' organizations



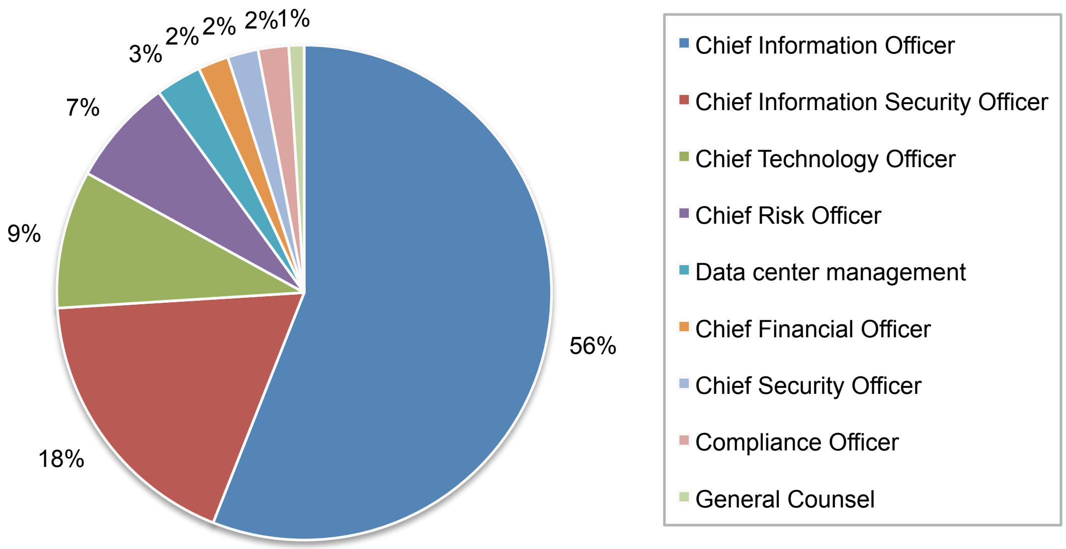
Pie Chart 2 reports the respondent's organizational level within participating organizations. By design, 58 percent of respondents are at or above the supervisory levels.

Pie Chart 2. What organizational level best describes your current position?



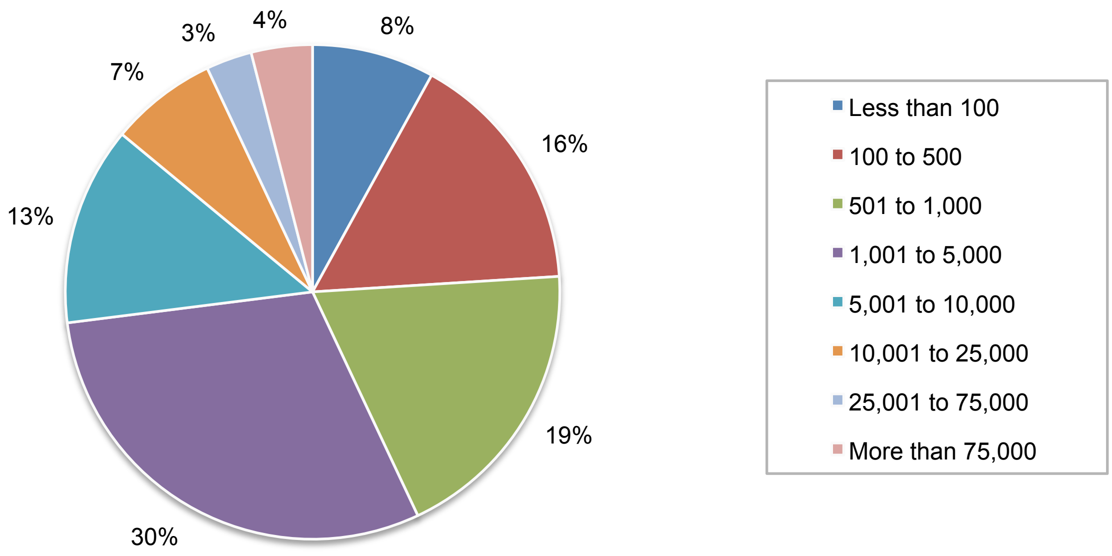
According to Pie Chart 3, 56 percent of respondents report directly to the Chief Information Officer and 18 percent report to the Chief Information Security Officer.

Pie Chart 3. The primary person the IT or IT security practitioner reports to within the organization



More than half of the respondents (57 percent) are from organizations with a global headcount of over 1,000 employees, as shown in Pie Chart 4.

Pie Chart 4. Global headcount



Part 5. Caveats

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 IT or IT 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.

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.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in May 2012.

Survey response	Freq	Pct%
Sample frame	19,190	100.0%
Total returns	708	3.7%
Rejected surveys	86	0.4%
Final sample	622	3.2%

Part 1. General Questions

Each statement is rated using the five-point scale from strongly agree to strongly disagree. Strongly agree and agree response presented.	Strongly agree	Agree
Q1a. In my organization, confidential or sensitive documents are fully secured and protected.	15%	22%
Q1b. In my organization, there is little risk that sensitive or confidential documents would end up in the hands of unauthorized parties (such as a business competitor).	14%	21%
Q1c. In my organization, protecting sensitive or confidential documents is a business priority.	21%	29%
Q1d. In my organization, controlling sensitive or confidential documents is less difficult than controlling records in databases.	13%	16%
Q1e. In my organization, documents accessed by mobile data-bearing devices such as smart phones and tablets do not present a significant security risk.	15%	15%

Q2a. Does your organization have a method for classifying the confidentiality of particular documents?	Pct%
Yes	67%
No	33%
Total	100%

Q2b. If yes, how many levels of confidentiality or sensitivity does your organization use in its classification schema?	Pct%
Two	26%
Three	31%
Four	24%
Five	13%
Six	4%
Seven	1%
More than seven	1%
Total	100%

Q3. What types of information do you consider to be most at risk because of document-level insecurity? Please select your top two choices.	Pct%
Customer/consumer	50%
Employee	47%
Legal & compliance	26%
Research & development	23%
Sales	21%
Finance & accounting	12%
Executive/board	7%
Internal communications	6%
Marketing	5%
Logistics/supply chain	4%
Total	200%

Q4a. Did your organization experience the leakage or loss of sensitive or confidential documents sometime over the past 12-month period?	Pct%
Yes, with certainty	35%
Yes, most likely	55%
No	10%
Total	100%

Q4b. If yes, what percent of your organization's sensitive or confidential documents **inadvertently** leaked to unauthorized parties because of carelessness or internal control issues? Your best guess is welcome.	Pct%
Less than 1%	2%
1 to 10%	9%
11 to 20%	15%
21 to 30%	23%
31 to 40%	21%
41 to 50%	17%
More than 50%	13%
Total	100%

Q4c. What percent of your organization's sensitive or confidential documents **deliberately** leaked to unauthorized parties because of malicious or criminal insiders? Your best guess is welcome.	Pct%
Less than 1%	12%
1 to 10%	14%
11 to 20%	34%
21 to 30%	18%
31 to 40%	16%
41 to 50%	5%
More than 50%	1%
Total	100%

Q5. How often (frequently) do employees, contractors or business partners have access to sensitive or confidential documents even though access to this information is not a job or role-related requirement?	Pct%
Very frequently	29%
Frequently	41%
Not frequently	20%
Never	10%
Total	100%

Q6a. Who is **most** responsible for managing and controlling access to sensitive or confidential information at the document, file and volume levels, respectively? Please check only one most responsible party per stored information category.			
Responsible parties	Volume	File	Document
Information technology department	36%	26%	17%
Information security department/function	14%	14%	16%
Legal, risk or compliance department	10%	9%	6%
Business unit managers	18%	25%	32%
Application or data owners	19%	23%	29%
Human resource department	3%	3%	0%
Other	0%	0%	0%
Total	100%	100%	100%

Q6b. In your opinion, where is your biggest threat to the security of stored sensitive or confidential information? Please check one choice only.	Pct%
At the volume level	11%
At the file level	33%
At the document level	37%
All levels are approximately equal	19%
Total	100%

Each statement is rated using the five-point scale from "the control is very effective" to "the control does not exist." Very effective and effective response presented.	Very effective	Effective
Q7a. Your organization's control process for monitoring employees, contractors and other insiders who access sensitive or confidential documents.	19%	22%
Q7b. Your organization's control process for assigning privilege to employees, contractors and other insiders whose job or role requires access to sensitive or confidential documents.	16%	21%
Q7c. Your organization's control process for preventing or limiting the transfer of sensitive or confidential documents from one storage or computing device to other devices?	16%	18%

Q8. How well does your organization govern privilege and access to sensitive or confidential documents? Please grade each one of the following governance tasks or procedures using the following scale: 1 = excellent, 2 = good, 3 = fair, 4 = poor, 5 = task is not performed. Excellent and good response presented.	Excellent	Good
Remove sensitive or confidential documents from storage or computing devices when this information is no longer necessary	20%	30%
Meet regulatory compliance objectives and provide evidence of compliance	23%	25%
Educate end-users about access control policies and procedures	19%	27%
Segregate documents based on their level of confidentiality	21%	23%
Monitor privileged user access to sensitive or confidential documents	17%	20%
Assign access rights to specific documents based on job function or role	15%	20%
Enforce access policies to sensitive or confidential documents	15%	17%
Prevent employees from transferring sensitive or confidential documents from one computing device to others.	14%	15%
Implement identity and roles management technologies at the document level	12%	14%
Map user business roles to document-level entitlements	11%	12%

Q9. How confident are you that your organization has visibility to all users of sensitive and confidential documents and their use of these resources?	Pct%
Very confident	12%
Confident	17%
Somewhat confident	20%
Not confident	51%
Total	100%

Q10. What are the critical success factors for implementing governance and control practices over sensitive or confidential documents? Please rate the following success factors using the following scale: 1 = Very important, 2 = important, 3 = sometimes important, 4 = not important, 5 = irrelevant. Very important and important response presented	Very important	Important
Ample budget resources	42%	39%
Compliance monitoring procedures	39%	40%
Centralized accountability and control	37%	39%
Technologies that assign or control access	35%	37%
Strict enforcement of non-compliance	38%	32%
Employee awareness, education and training	40%	28%
Policies and standard operating procedures	35%	31%
Senior level executive support	30%	33%
Assessments or audits by an objective party	23%	28%

	Very frequently	Frequently
Q11a. How frequently does this situation happen in your organization? Very frequently & frequently combined.	33%	35%

	Very Likely	Likely
Q11b. How likely does this situation result in the loss or theft of confidential documents? Very likely & likely combined.	31%	40%

	Very frequently	Frequently
Q12a. How frequently does this situation happen in your organization? Very frequently & frequently combined.	32%	33%

	Very Likely	Likely
Q12b. How likely does this situation result in the loss or theft of confidential documents? Very likely & likely combined.	30%	38%

	Very frequently	Frequently
Q13a. How frequently does this situation happen in your organization? Very frequently & frequently combined.	29%	31%

	Very Likely	Likely
Q13b. How likely does this situation result in the loss or theft of confidential documents? Very likely & likely combined.	28%	29%

	Very frequently	Frequently
Q14a. How frequently does this situation happen in your organization? Very frequently & frequently combined.	29%	33%

	Very Likely	Likely
Q14b. How likely does this situation result in the loss or theft of confidential documents? Very likely & likely combined.	23%	33%

	Very frequently	Frequently
Q15a. How frequently does this situation happen in your organization? Very frequently & frequently combined.	26%	29%

	Very Likely	Likely
Q15b. How likely does this situation result in the loss or theft of confidential documents? Very likely & likely combined.	24%	27%

Q16. How many browser-based filesharing tools are used by employees in your organization? Examples of these tools include: Yousendit!, Dropbox, Box.net and/or others.	Pct%
None	15%
1 to 2	23%
3 to 5	22%
More than 5	6%
Don't know	34%
Total	100%

Q17a. **Today**, what percent of your organization's employees use one or more browser-based filesharing tools such as Yousendit, Dropbox, Box.net and/or others. Your best guess is welcome.	Pct%
None	15%
Less than 1%	1%
1 to 10%	3%
11 to 25%	5%
26 to 50%	21%
51 to 75%	16%
76 to 100%	4%
Don't know	35%
Total	100%

Q17b. **In the next 12-24 months**, what percent of your organization's employees will use one or more browser-based filesharing tools such as Yousendit, Dropbox, Box.net and/or others. Your best guess is welcome.	Pct%
None	11%
Less than 1%	1%
1 to 10%	1%
11 to 25%	4%
26 to 50%	20%
51 to 75%	18%
76 to 100%	8%
Don't know	37%
Total	100%

Q18. What steps is your organization taking to mitigate or reduce the risk of document loss or leakage when using browser-based filesharing tools? Please select all that apply.	Pct%
Manual monitoring and controls	47%
None of the above	40%
Employee training and awareness	41%
Policies and standard operating procedures	39%
Enabling security technologies	23%
Access governance technologies	20%
Non-disclosure agreements	13%
Other	2%
Total	225%

Q19a. In your opinion, how will the importance of securing and protecting the sensitive or confidential documents in browser-based filesharing tools change over time?	Pct%
It will become more important for my organization	50%
It will stay the same in terms of importance for my organization	36%
It will become less important for my organization	14%
Total	100%

Q19b. If you believe that the security of browser-based filesharing tools will become "more important," why do you feel this way? Please select all that apply.	Pct%
Increase in the access requirements for users because of mobility	68%
Increase in the volume of documents	63%
Managing user access at the document level will become more complex	61%
Increase in the need to share documents for purposes of collaboration	56%
Increase in cyber criminal attacks	48%
More privacy and data security regulations to comply with	43%
Cost of non-compliance will increase	39%
Other	3%
Total	381%

Following are features of a document-centric security solution. Please rate the importance of each feature in the context of securing or protecting sensitive or confidential documents within your organization today using a five-point scale from very important to irrelevant. Very important and important response presented.	Very important	Important
Q20a. A solution that allows enterprise organizations to easily and effectively access, share and control all important documents across the extended and mobile enterprise on any device – even those beyond the IT organization's control.	31%	43%
Q20b. A solution that allows employees to easily access their corporate documents on PC and mobile devices with an intuitive interface that displays documents perfectly on any screen.	35%	38%
Q20c. A solution that enables users to easily and safely send files and collaborate with business partners or other outside parties. This solution ensures that shared files remain protected even as business partners use their own corporate or personal mobile devices.	32%	36%
Q20d. A solution that gives enterprises full control over every protected document. The platform provides granular capabilities such as controlling printing, copying and forwarding, as well as the ability to watermark or wipe the document.	39%	41%

Q21. In your opinion, why is document-centric security most important in your organization? Please select your top two reasons.	Pct%
To reduce the risk of insider negligence	53%
To reduce risks that can negatively impact the business	50%
To reduce the risk of malicious insiders	31%
To Improve compliance with policies, procedures and law	25%
To comply with e-discovery requests	19%
To establish trust and confidence among users	12%
To enable business partners and other third parties to access information	10%
Total	200%

Part 2. Budget

Q22a. Are you responsible for managing all or part of your organization's IT security budget?	Pct%
Yes	54%
No (Go to Part 3)	46%
Total	100%

Q22b. Approximately, what is the dollar range that best describes your organization's IT security budget in the present year? Your best guess is welcome.	Pct%
Less than $1 million	9%
$1 to 2 million	15%
$2 to $3 million	27%
$3 to $5 million	21%
$5 to $10 million	11%
$10 to $15 million	6%
$15 to $20 million	5%
$20 to $30 million	2%
$35 to $40 million	1%
$45 to $50 million	1%
Over $50 million	2%
Total	100%

Q22c. Approximately, what percentage of the current IT security budget will go to data protection activities? Your best guess is welcome.	Pct%
Less than 1%	0%
1% to 5%	4%
6% to 10%	8%
11% to 20%	21%
21% to 30%	24%
31% to 40%	18%
41% to 50%	11%
51% to 60%	8%
61% to 70%	3%
71% to 80%	2%
81% to 90%	1%
91% to 100%	0%
Total	100%

Q22d. Approximately, what percentage of the budget for data protection activities will be allocated to the protection of sensitive or confidential documents? Your best guess is welcome.	Pct%
Less than 1%	0%
1% to 5%	5%
6% to 10%	12%
11% to 20%	32%
21% to 30%	28%
31% to 40%	13%
41% to 50%	6%
51% to 60%	1%
61% to 70%	1%
71% to 80%	0%
81% to 90%	1%
91% to 100%	1%
Total	100%

Part 3. Role and organization characteristics

D1. What organizational level best describes your current position?	Pct%
Senior Executive	1%
Vice President	1%
Director	17%
Manager	23%
Supervisor	16%
Technician	36%
Staff	4%
Contractor	2%
Other	0%
Total	100%

D2. Check the **Primary Person** you or your IT security leader reports to within the organization.	Pct%
Chief Information Officer	56%
Chief Information Security Officer	18%
Chief Technology Officer	9%
Chief Risk Officer	7%
Data center management	3%
Chief Financial Officer	2%
Chief Security Officer	2%
Compliance Officer	2%
General Counsel	1%
Other	0%
Total	100%

D3. Experience	Mean	Median
D3a. Total years of IT or IT security experience	11.60	11.50
D3b. Total years in present position	5.90	6.00

D4. What industry best describes your organization's industry focus?	Pct%
Financial services	19%
Public sector	14%
Health & pharmaceutical	11%
Retailing	9%
Services	8%
Industrial	6%
Consumer products	6%
Energy & utilities	5%
Hospitality	5%
Technology & Software	5%
Education & research	4%
Communications	3%
Agriculture & food service	2%
Entertainment & media	2%
Defense	1%
Other	1%
Total	100%

D5. Where are your employees located? (Please check all that apply):	Pct%
United States	100%
Canada	71%
Europe	68%
Middle East & Africa	43%
Asia-Pacific	58%
Latin America (including Mexico)	56%

D6. What is the worldwide headcount of your organization?	Pct%
Less than 100	8%
100 to 500	16%
501 to 1,000	19%
1,001 to 5,000	30%
5,001 to 10,000	13%
10,001 to 25,000	7%
25,001 to 75,000	3%
More than 75,000	4%
Total	100%

Ponemon Institute

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.