Ponemon INSTITUTE

Achieving Security in Workplace File Sharing

Sponsored by Axway

Independently conducted by Ponemon Institute LLC

Publication Date: January 2014

Achieving Security in Workplace File Sharing

January 2014

Part 1. Introduction

Sponsored by Axway Corporation, we are pleased to present the findings of *Achieving Security in Workplace File Sharing*. The study focuses on the practice of public cloud file sharing in the workplace, threats to corporate information and features most desirable in achieving security in the sharing of files and documents.

We surveyed 621 IT and IT security practitioners with involvement in setting IT security priorities, managing IT security budgets, selecting vendors and contractors and evaluating program performance. Sixty-two percent of respondents have a very high or high level of involvement in these activities.

File sharing is growing in popularity as a productive and efficient way for employees to exchange or share documents in the workplace. According to most participants in this research, file sharing will substantially increase or increase over the next 24 months. However, using this technology makes the organization vulnerable to risks such as malware and viruses, exposure of sensitive or confidential information and cyber attacks. Sixty-two percent of IT respondents in this study concur and rate the risk of file sharing as very high or high.

Key takeaways from this research

- What is the most convincing reason for organizations to invest in secure file sharing tools? According to 80 percent of respondents, it is the need to secure documents and files containing intellectual property. Respondents in this study consider the loss of intellectual property to be the most negative consequence as a result of employees using insecure file sharing tools.

- Data breaches involving company data stored in a public cloud environment are likely to go undetected. Only 11 percent of respondents say they would be very likely to know if sensitive or confidential information was lost or stolen as a result of a data breach.

- Employees' decisions to use certain file sharing tools are made without guidance or oversight from the organization. Fifty percent of respondents say their organizations do not have policies that inform employees about the approved use of file sharing tools. If they do have policies, 48 percent say they are not enforced. Moreover, 69 percent of respondents are not likely to know whether employees are using unapproved and risky file sharing tools.

- While almost half of the respondents in this study (48 percent) believe popular cloud-sharing services are not suitable for business use, they would worry less about the security of confidential documents if they were encrypted with their own encryption keys (security at rest) and storage was segregated and not shared with other tenants.

- Corporate culture is a barrier to achieving security in workplace file sharing. Fifty-eight percent of respondents say the organization places more importance on employees' productivity than they do on the security of corporate data. Many of the respondents believe the use of file sharing tools increases worker productivity and efficiency.

- To minimize the risk, one solution would be to provide an approved file sharing tool. Sixty-two percent of respondents believe providing an approved file sharing tool would reduce employees' use of a public cloud.

Part 2. Key findings

In this section, we present an analysis of the research findings. The complete audited findings are presented in the appendix of this report. We have organized the report according to the following topics:

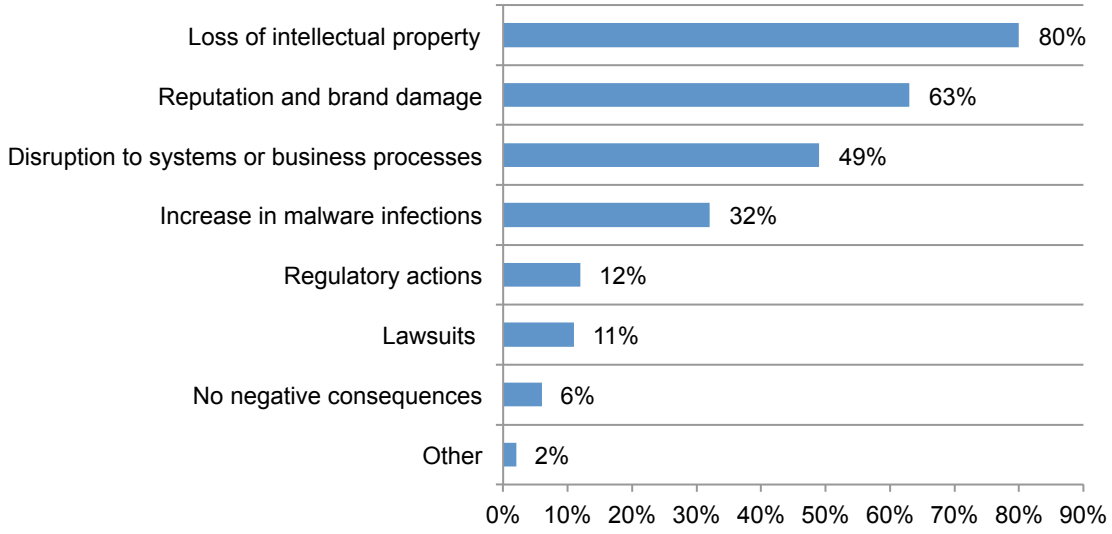
- The risk of insecure workplace file sharing
- Barriers to achieving secure file sharing
- Solutions for secure file sharing

The risk of insecure workplace file sharing

The sharing of corporate data using public cloud file sharing tools puts intellectual property and reputation at risk. Sixty-two percent of respondents rank file sharing as a high or very high risk to their organizations. Only 18 percent of respondents say the risk is low.

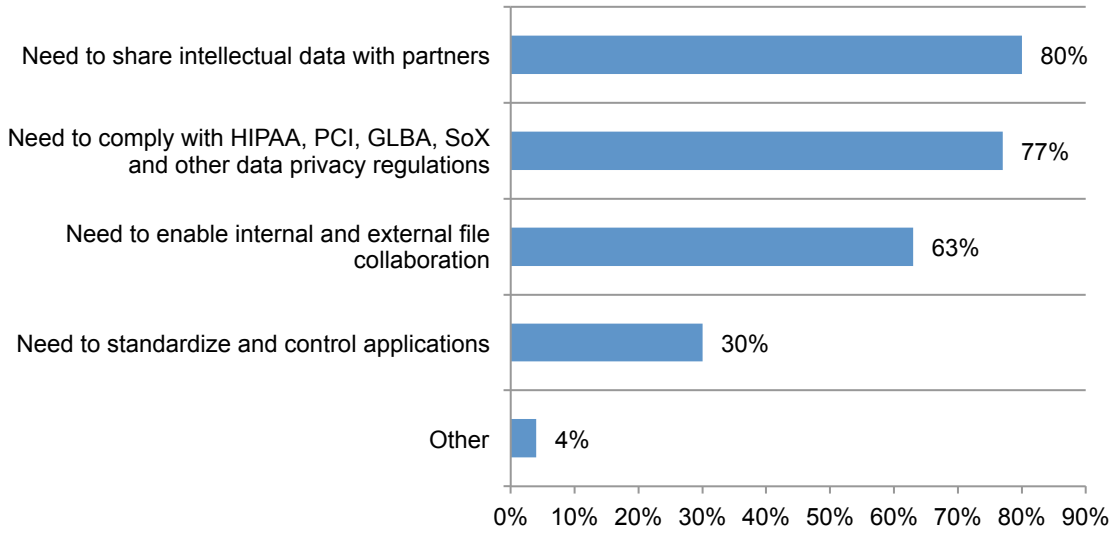
As shown in Figure 1, the most negative consequences are loss of intellectual property (80 percent of respondents) and reputation and brand damage (63 percent of respondents). Only 6 percent say there would be no negative consequences due to the use of insecure file sharing tools.

Figure 1. Negative consequences from employees' use of insecure file sharing tools
More than one response permitted



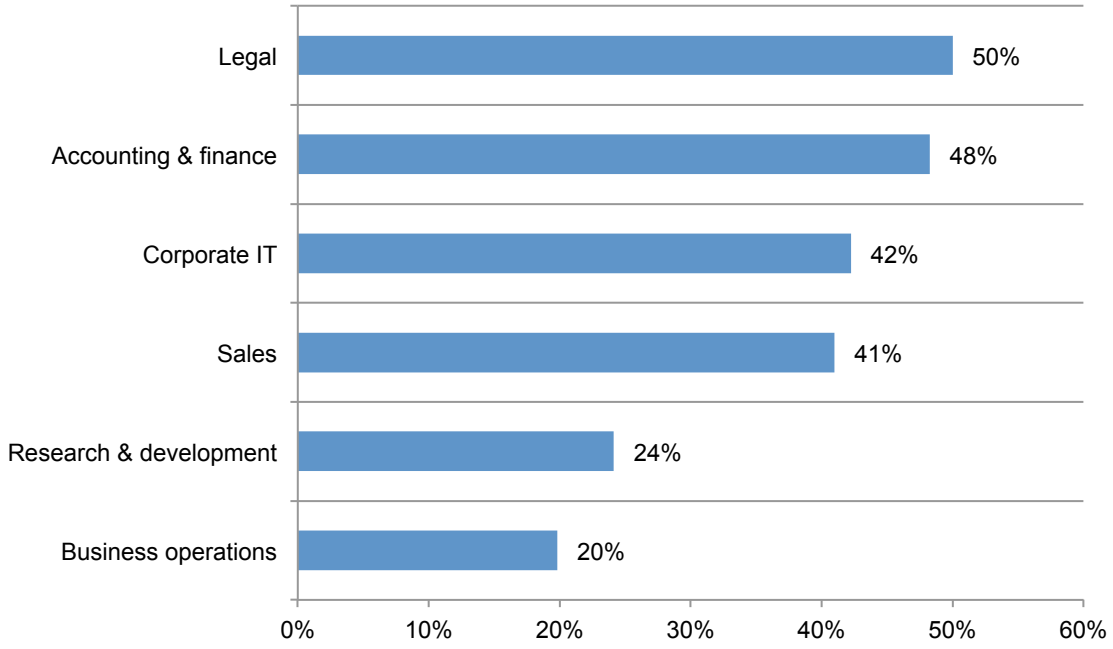
What is the most convincing case for investing in secure file sharing solutions? Figure 2 reveals that 80 percent of respondents claim that the need to share intellectual data with partners best illustrates the need for a secure file sharing solution. This is followed by the need for compliance with data privacy regulations (77 percent of respondents).

Figure 2. Reasons for investing in secure file sharing solutions



Certain departments and functions in an organization are more in need of secure file sharing tools than others. As shown in Figure 3, the most at risk for insecure file sharing are legal and the accounting and finance functions (50 percent and 48 percent of respondents, respectively).

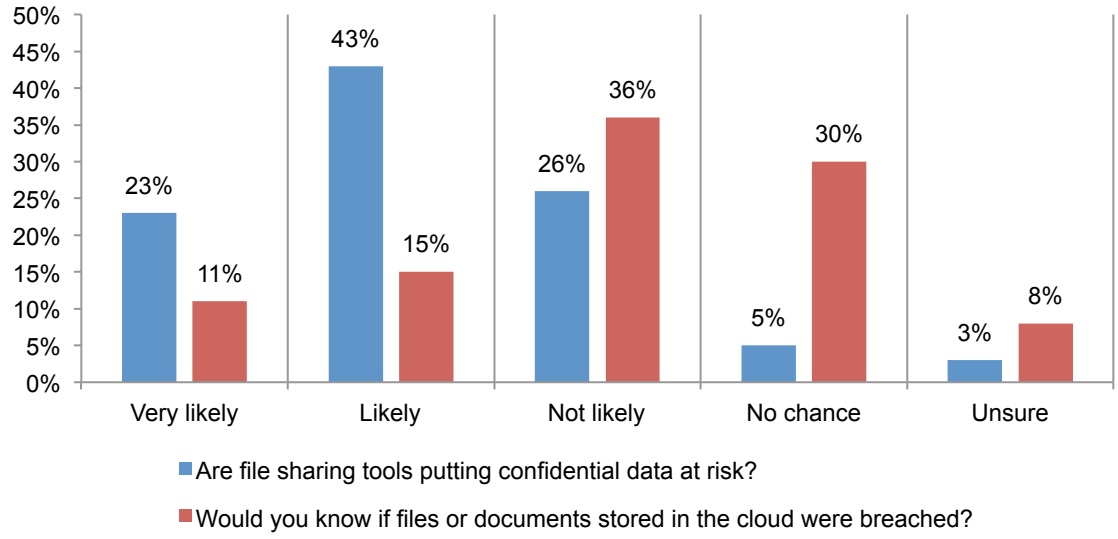
Figure 3. Who needs secure file sharing tools the most?
Three choices permitted



Organizations do not understand the extent of the file sharing risk. Respondents recognize that employees throughout the organization are using unapproved public file sharing tools for business purposes and expect them to continue to proliferate throughout the enterprise. However, they have difficulty in measuring and addressing the risk because they do not know specifically how many and what types of unapproved file sharing tools are in use.

As a result of their inability to control the use of insecure file sharing, most respondents (66 percent) say that it is very likely or likely that this practice is putting sensitive and confidential information at risk, according to Figure 4. Further, only 26 percent are confident that they would likely know if the company's files or documents stored in a public cloud environment were breached.

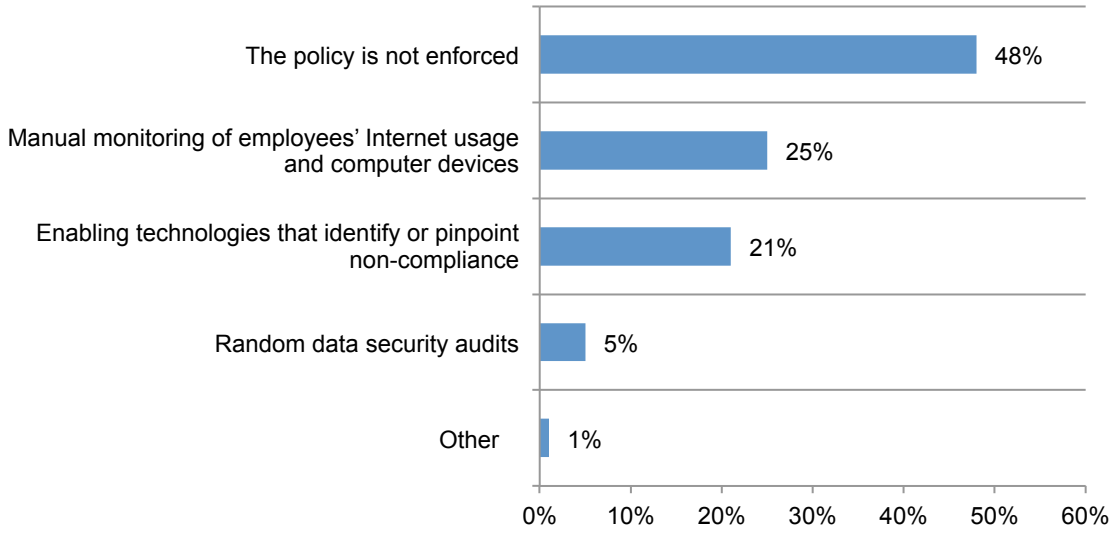
Figure 4. Do file sharing tools put data at risk and would you know if a breach occurred?



Barriers to achieving secure file sharing

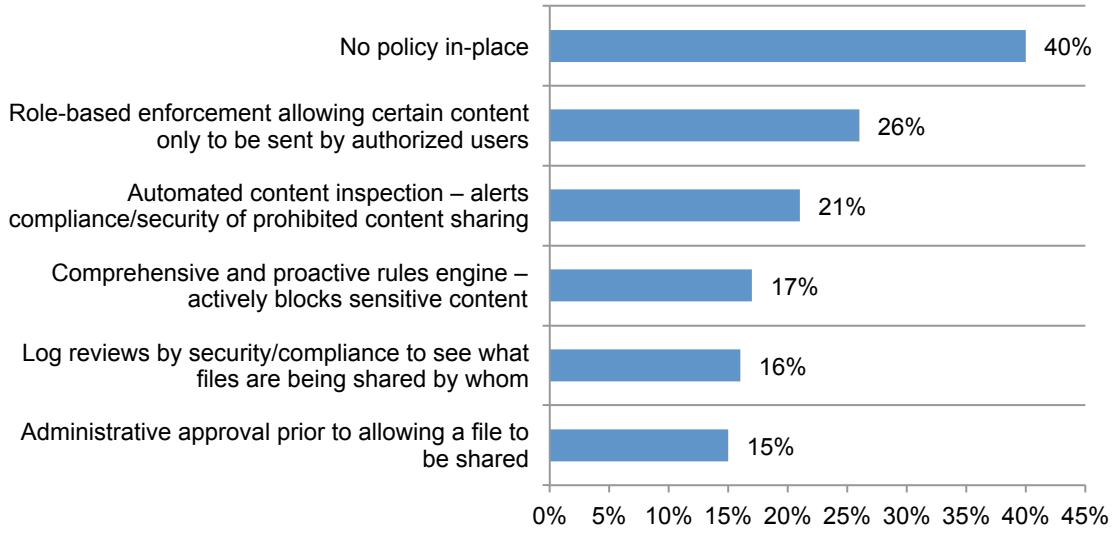
Employees are not given guidance on the acceptable use of file sharing tools. As discussed previously, respondents admit they are uncertain as to the extent employees are using file sharing tools. Creating policies in such an uncertain environment may be difficult and 50 percent of respondents say no policies exist and 7 percent are not sure. If they do have policies, 48 percent of respondents say there is no enforcement. Only 21 percent use technologies that would identify or pinpoint non-compliance, as shown in Figure 5.

Figure 5. How file sharing policies are enforced



Policy enforcement process for file sharing is weak in most organizations. According to Figure 6, 40 percent have no policy in place for detecting employees' use of unapproved file sharing tools. If they do have policy management systems, it is most likely to be a role-based enforcement allowing certain content only to be sent by authorized users.

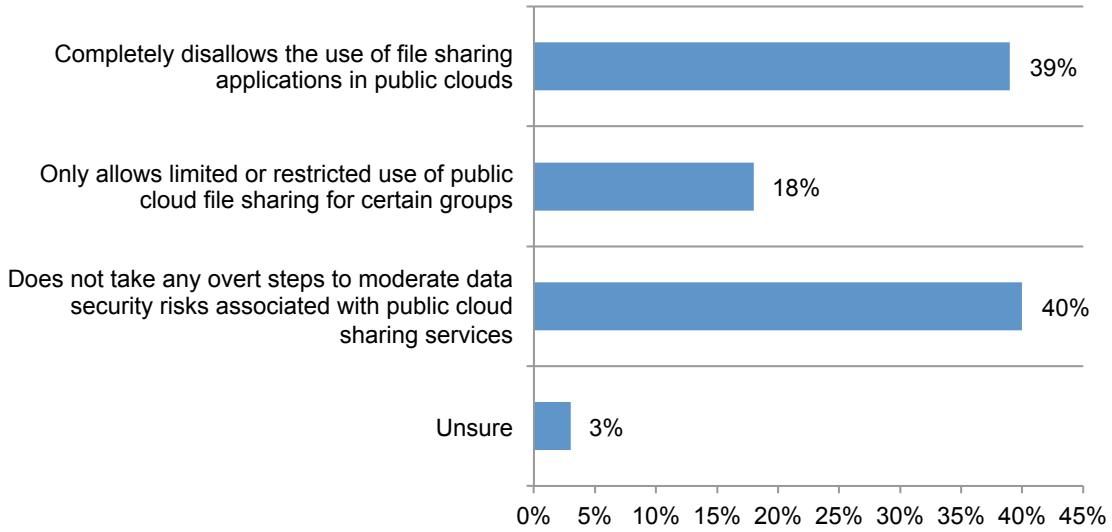
Figure 6. Policy management systems
Two choices permitted



Stronger security practices are needed to reduce data security risks created by employees' use of public cloud file sharing services. Figure 7 reveals that 40 percent of respondents do not take any overt steps to moderate data security risks associated with public cloud sharing services. This is not a satisfactory approach to the risk because it is unrealistic to completely disallow the use of file sharing applications in public clouds.

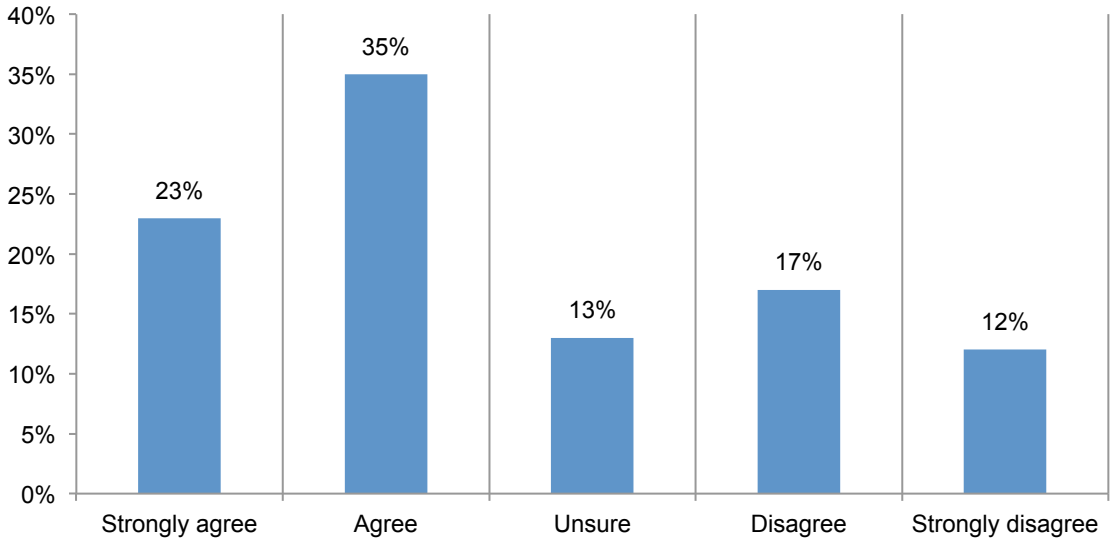
The department most responsible for regulating or curtailing employees' use of public cloud file sharing services is the business unit followed by corporate IT.

Figure 7. Steps taken to reduce the risk of public cloud file sharing



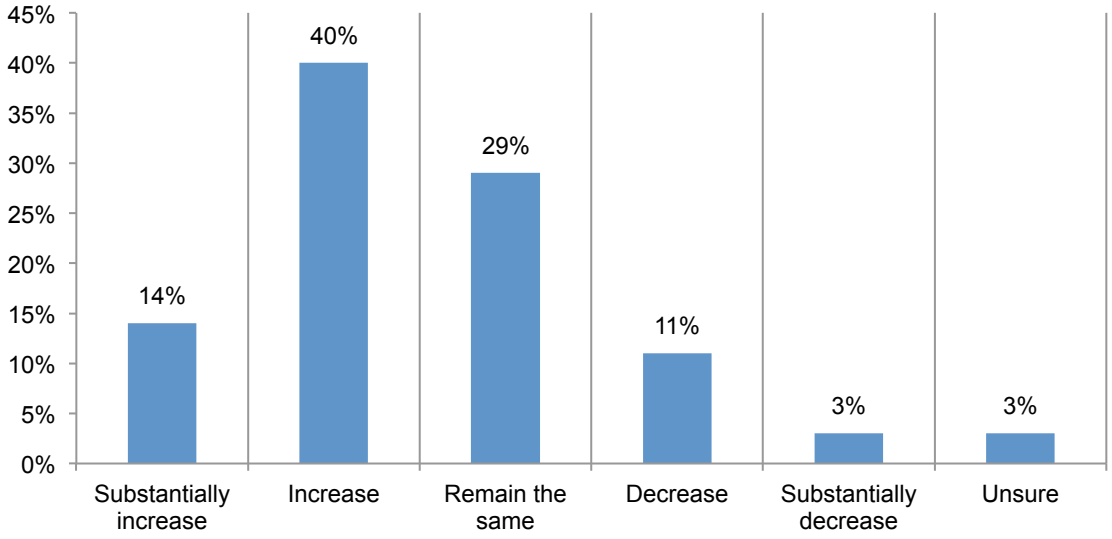
Security is often sacrificed for productivity. Corporate culture can be a barrier to strengthening the security of file sharing. According to Figure 8, 58 percent of respondents strongly agree or agree that their organizations will sometimes place more importance on employees' productivity than they will on security of corporate data. Most respondents (54 percent) also believe file sharing tools improve productivity.

Figure 8. Willingness to sacrifice security for employee productivity



Employees' use of file sharing services is expected to increase. According to Figure 9, 54 percent of respondents expect the use of these services to increase. If nothing is done to mitigate the risk, this increase will seriously jeopardize the security of confidential or sensitive corporate data.

Figure 9. Will employees' use of file sharing services change over the next 24 months?

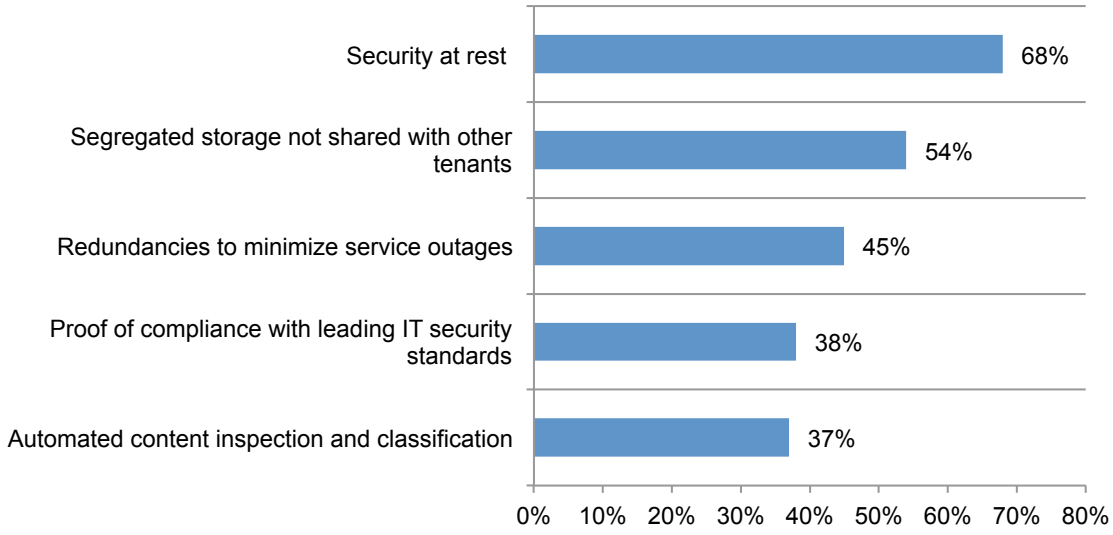


Solutions for secure file sharing

Encryption and segregated storage would reduce IT concerns about the security of confidential files and documents. While almost half of respondents (48 percent) do not believe popular public cloud-sharing services are suitable for business use, there are measures that can be taken to ease some of the worries about their use.

Figure 10 reveals the security features in a public cloud environment that would give companies more confidence. Security at rest (encryption with their own encryption keys) and segregated storage not shared with other tenants would provide respondents with greater assurance that confidential files or data is adequately secured.

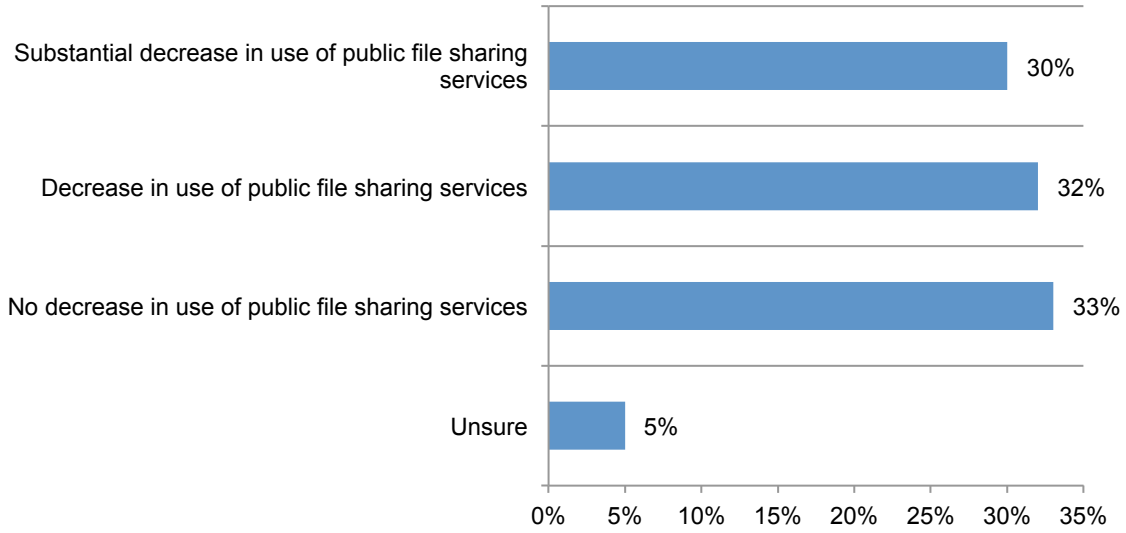
Figure 10. Public cloud features that create confidence about data security
More than one response permitted



One security solution would be to provide an approved file sharing tool. Currently, only 26 percent of respondents say their organizations have a sanctioned tool for all employees and 39 percent are considering the implementation of secure file sharing alternatives.

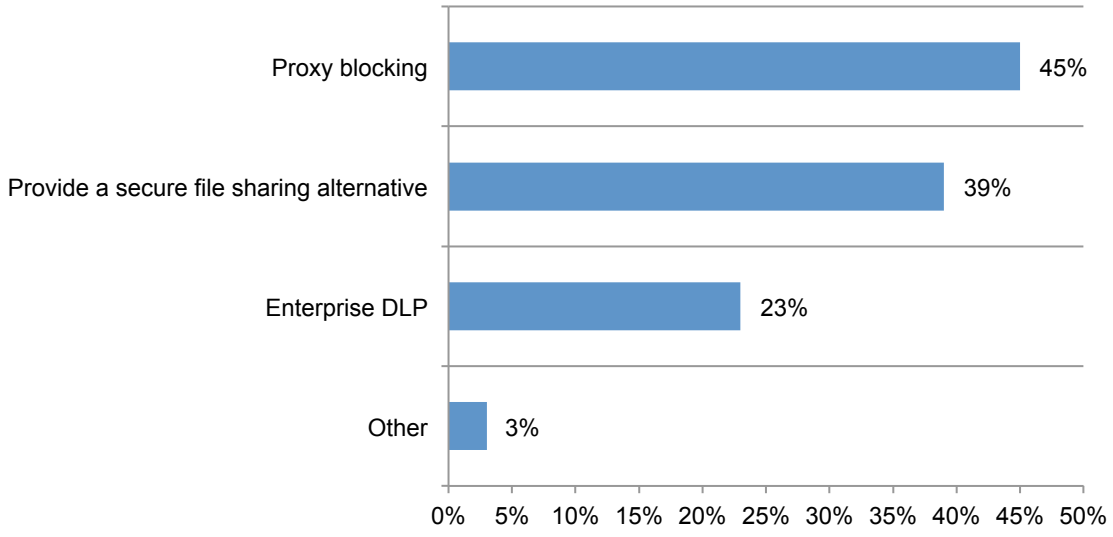
Figure 11 shows that providing such tools might have an effect on the use of file sharing services. Sixty-two percent of respondents believe that giving employees a secure file sharing alternative would decrease to some degree the use. However, 33 percent believe employees would continue to use public file sharing services despite having an alternative provided by the employer.

Figure 11. Would a secure file sharing alternative decrease the use of public file sharing services?



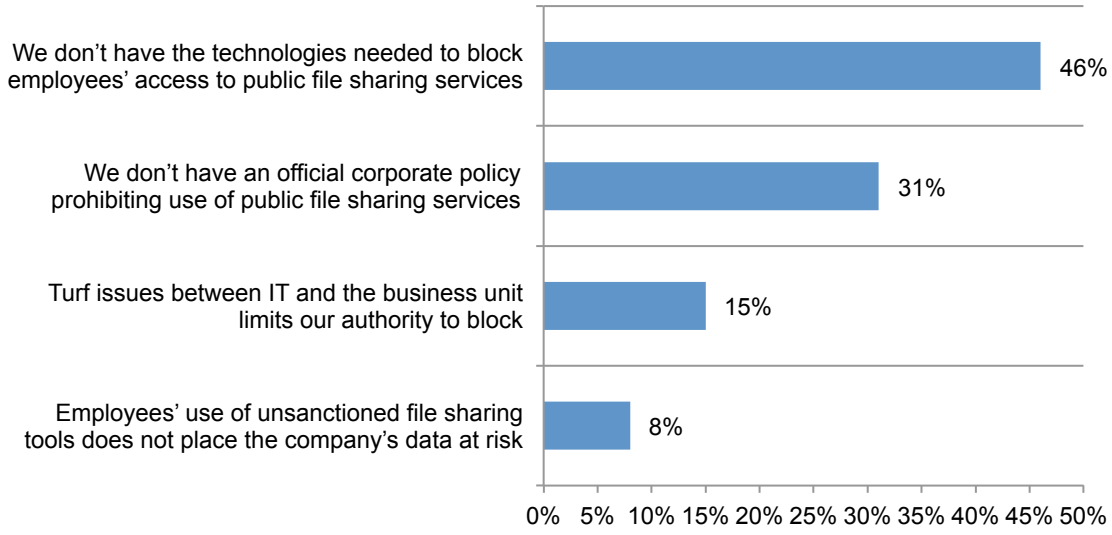
While 50 percent are not pursuing the adoption of tools to prevent employees from using insecure public cloud services, other respondents are considering proxy blocking or a secure file sharing alternative to decrease employees' use of public file sharing services, according to Figure 12.

Figure 12. Features to decrease employees' use of public file sharing services



Organizations lack the technologies needed to block employees' access to public file sharing services. Most respondents (56 percent) do not block access to certain "high risk" file sharing services. The primary reason, as shown in Figure 13, is not having the technologies to take such steps. Another reason is not having an official corporate policy prohibiting use of public file sharing services (31 percent of respondents).

Figure 13. Reasons for not blocking employees' access to "high risk" file sharing services
More than one choice permitted



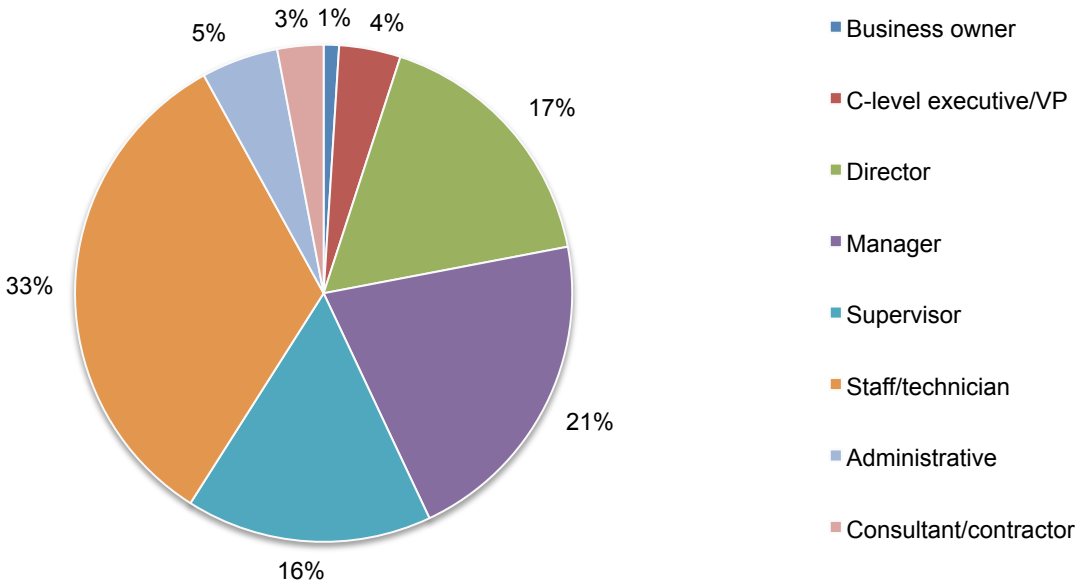
Part 3. Methods

A sampling frame of 19,703 IT and IT security practitioners with involvement in setting IT security priorities, managing IT security budgets, selecting vendors and contractors and evaluating program performance were selected to complete the survey. All participants were located in the United States. As shown in Table 1, 735 respondents completed the survey. Screening and failed reliability checks removed 114 surveys resulting in a final sample 621 completed surveys (or a 3.2 percent response rate).

Table 1. Sample response	Freq.	Pct%
Total sampling frame	19,703	100.0%
Total returns	735	3.7%
Rejected and screened surveys	114	0.6%
Final sample	621	3.2%

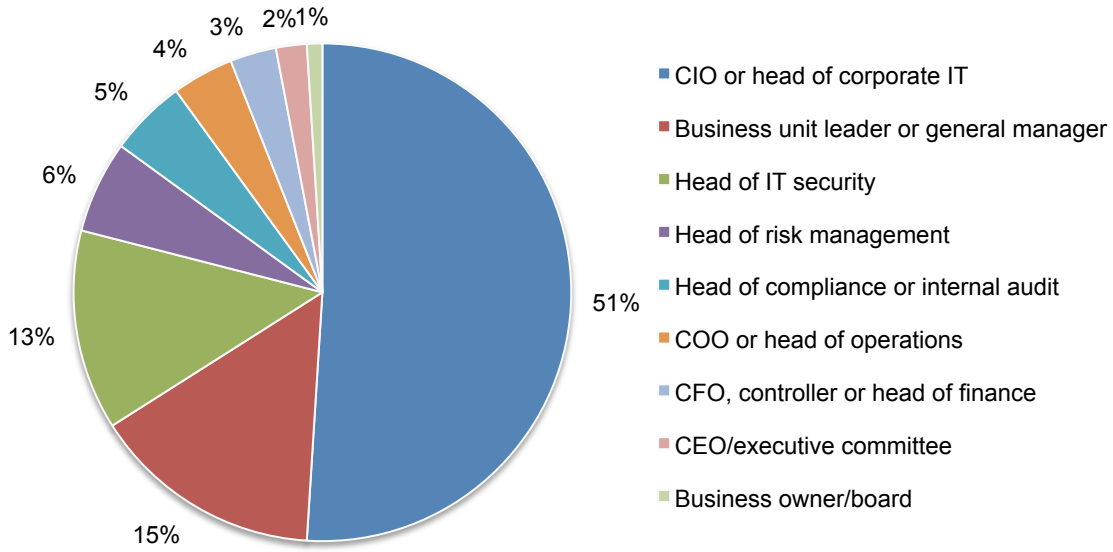
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, 59 percent of respondents are at or above the supervisory levels.

Pie Chart 1. What organizational level best describes your current position?



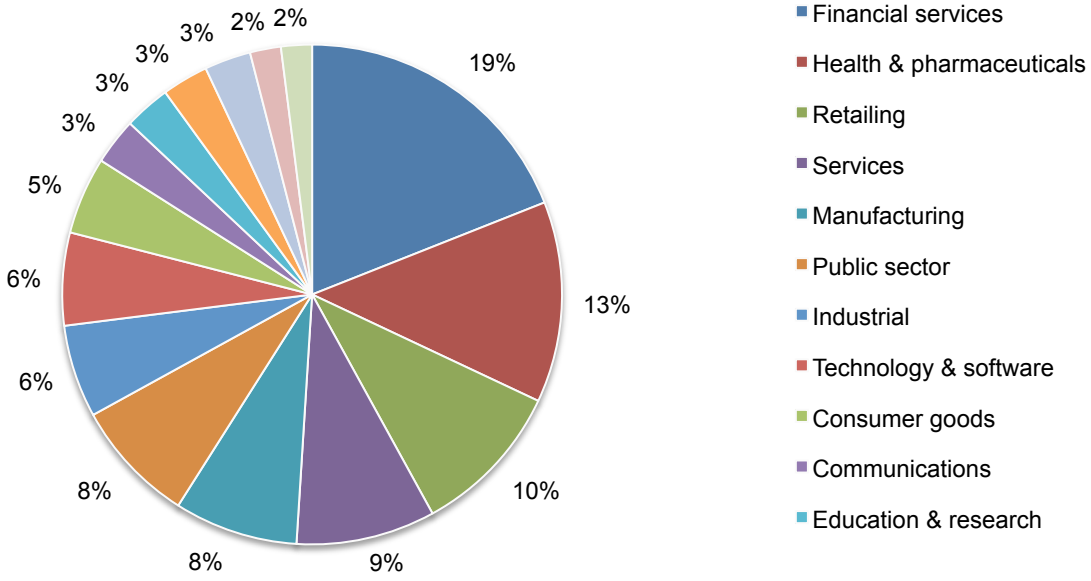
As shown in Pie Chart 2, 51 percent of respondents indicated that they or their immediate supervisor reports directly to the CIO or head of corporate IT. This is followed by 15 percent who report directly to the business unit leader or general manager.

Pie Chart 2. Functional area you or your immediate supervisor reports to within the organization



Pie Chart 3 reports the primary industry classification of respondents' organizations. This chart identifies financial services (19 percent) as the largest segment, followed by health & pharmaceuticals (13 percent) and retailing (10 percent).

Pie Chart 3. Primary industry classification



Part 4. 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 October 2013.

Sample response	Freq	Pct%
Total sampling frame	19,703	100.0%
Total returns	735	3.7%
Rejected or screened surveys	114	0.6%
Final sample	621	3.2%

Part 1. Screening

S1. What range best describes the full-time employee headcount of your organization?	Pct%	
501 to 1,000	25%	
1,001 to 5,000	21%	
5,001 to 10,000	23%	
10,001 to 25,000	15%	
25,001 to 75,000	11%	
More than 75,000	5%	Headcount
Total	100%	14,668

S2. What best describes your role in managing the IT security function or activities within your organization? Check all that apply.	Pct%
Setting IT security priorities	67%
Managing IT security budgets	59%
Selecting vendors and contractors	55%
Determining IT security strategy	40%
Evaluating program performance	52%
Average	273%

S3. How do you rate your level of involvement in the evaluation, selection, and/or implementation of IT services in your organization?	Pct%
Very high level of involvement	29%
High level of involvement	33%
Moderate level of involvement	38%
Total	100%

Part 1. General questions

Q1. Drawing upon your knowledge and experience, rate the data security risks associated with the sharing of corporate data using public cloud file sharing tools. Please use the following 10-point scale from 1 = low risk to 10 = high risk.	Pct%	
1 to 2	5%	
3 to 4	13%	
5 to 6	20%	
7 to 8	21%	
9 to 10	41%	Mean value
Total	100%	7.10

Q2. What specific negative consequences does your company face due to the use of insecure file sharing tools? Please select all that apply.	Pct%
Regulatory actions	12%
Lawsuits	11%
Loss of intellectual property	80%
Reputation and brand damage	63%
Increase in malware infections	32%
Disruption to systems or business processes	49%
No negative consequences	6%
Other	2%
Total	255%

Q3. What step does your company take to moderate the data security risks associated with public cloud file sharing services? Please select only one choice.	Pct%
Completely disallows the use of file sharing applications in public clouds	39%
Only allows limited or restricted use of public cloud file sharing for certain groups	18%
Does not take any overt steps to moderate data security risks associated with public cloud sharing services	40%
Unsure	3%
Total	100%

Q4. [For those NOT allowing use] Who within your company regulates or curtails employees' use of public cloud file sharing services? Please select all that apply.	Pct%
Corporate IT	36%
Compliance	18%
IT security	19%
Risk management	11%
Internal audit	5%
Business unit (line of business)	57%
No one (employees choose freely)	29%
Other	1%
Total	176%

Q5. Does your company know if employees are using unapproved public file sharing tools for business purposes?	Pct%
Yes, in all instances	10%
Yes, in most instances	21%
Yes, in some instances	28%
No	41%
Total	100%

Q6. What is the likelihood that public cloud-based file sharing tools are putting your company's sensitive or confidential information at risk today?	Pct%
Very likely	23%
Likely	43%
Not likely	26%
No chance	5%
Unsure	3%
Total	100%

Q7. If your company's files or documents stored in a public cloud environment were breached, would your company know about it?	Pct%
Very likely	11%
Likely	15%
Not likely	36%
No chance	30%
Unsure	8%
Total	100%

Q8. What is your company's preferred file sharing platform today?	Pct%
Public cloud-based applications	33%
Private cloud-based applications	25%
On-premise applications	29%
Unsure	12%
Other	1%
Total	100%

Q9. In your opinion, how will employees' use of file sharing services change over the next 24 months?	Pct%
Substantially increase	14%
Increase	40%
Remain the same	29%
Decrease	11%
Substantially decrease	3%
Unsure	3%
Total	100%

Q10a. Does your company block employees' access to certain "high risk" file sharing services?	Pct%
Yes	32%
No	56%
Unsure	12%
Total	100%

Q10b. If no, why not? Please select only one choice.	Pct%
Employees' use of unsanctioned file sharing tools does not place the company's data at risk	8%
We don't have the technologies needed to block employees' access to public file sharing services	46%
We don't have an official corporate policy prohibiting use of public file sharing services	31%
Turf issues between IT and the business unit limits our authority to block	15%
Total	100%

Q11. In your opinion, which of the following public cloud-sharing services are suitable for business use within your company?	Pct%
Dropbox	40%
Box	39%
Hightail (previously Yousendit)	40%
Any of them	33%
Other	5%
None of the above	48%
Total	205%

Q12. What security features in a public cloud environment would give you the added confidence that your company's sensitive or confidential files or data were adequately secured?	Pct%
Proof of compliance with leading IT security standards	38%
Segregated storage not shared with other tenants	54%
Security at rest (encryption with my own encryption keys)	68%
Automated content inspection and classification	37%
Redundancies to minimize service outages	45%
Other	1%
Total	243%

Q13. What best describes the policy enforcement process as it relates to the use of file sharing within your company? Please select no more than two choices.	Pct%
Comprehensive and proactive rules engine – actively blocks sensitive content	17%
Automated content inspection – alerts compliance/security of prohibited content sharing	21%
Role-based enforcement allowing certain content only to be sent by authorized users	26%
Administrative approval by a human prior to allowing a file to be shared	15%
Log reviews by security/compliance to see what files are being shared by whom	16%
No policy in-place	40%
Other	0%
Total	135%

Q14. In the context of public cloud services, my organization is sometimes willing to sacrifice security for employee productivity?	Pct%
Strongly agree	23%
Agree	35%
Unsure	13%
Disagree	17%
Strongly disagree	12%
Total	100%

Q15. What features or functionality is IT looking to implement in order to prevent employees from using insecure public cloud services?	Pct%
Enterprise DLP	23%
Proxy blocking	45%
Provide a secure file sharing alternative	39%
Other	3%
None of the above	50%
Total	160%

Q16. Does your company provide an approved (sanctioned) file sharing tool for employees' use?	Pct%
Yes, all employees have access to this tool	26%
Yes, only some employees have access to this tool	16%
No	58%
Total	100%

Q17. In your opinion, how do file sharing tools impact employees' productivity?	Pct%
Substantial increase in productivity	16%
Increase in productivity	38%
No impact on productivity	16%
Decrease in productivity	21%
Substantial decrease in productivity	6%
Unsure	3%
Total	100%

Q18. If your company provided a secure file sharing alternative, would employees decrease their use of public file sharing services? In other words, does providing a secure file sharing alternative improve or worsen the rogue employee problem?	Pct%
Substantial decrease in use of public file sharing services	30%
Decrease in use of public file sharing services	32%
No decrease in use of public file sharing services	33%
Unsure	5%
Total	100%

Q19a. Does your organization currently offer an official policy on the acceptable use of file sharing tools?	Pct%
Yes	43%
No	50%
Unsure	7%
Total	100%

Q19b. If yes, how does your company enforce this policy?	Pct%
The policy is not enforced	48%
Manual monitoring of employees' Internet usage and computer devices	25%
Random data security audits	5%
Enabling technologies that identify or pinpoint non-compliance	21%
Other	1%
Total	100%

Q20. Is your company presently looking for a secure file sharing tool?	Pct%
Yes	45%
No	43%
Unsure	12%
Total	100%

Q22. Drawing upon your knowledge and experience, please rate four product features in terms of their importance in ensuring secure file sharing services within your company. Please use the following 10-point scale from 1 = low importance to 10 = high importance provided below each item.

Q21a. Private cloud with segregated data and private encryption keys	Pct%	
1 to 2	4%	
3 to 4	10%	
5 to 6	13%	
7 to 8	40%	
9 to 10	33%	Mean value
Total	100%	7.26

Q21b. Encryption of files and documents	Pct%	
1 to 2	3%	
3 to 4	11%	
5 to 6	13%	
7 to 8	30%	
9 to 10	43%	Mean value
Total	100%	7.48

Q21c. Auditability of file sharing activity and chain of custody	Pct%	
1 to 2	7%	
3 to 4	12%	
5 to 6	25%	
7 to 8	25%	
9 to 10	31%	Mean value
Total	100%	6.72

Q21d. Ability to enforce compliance with data privacy policies (i.e., HIPAA, PCI, GLBA, SoX,) through automated inspection and classification of file content	Pct%	
1 to 2	2%	
3 to 4	6%	
5 to 6	12%	
7 to 8	25%	
9 to 10	55%	Mean value
Total	100%	8.00

Q22. What use cases or factors best illustrate the need for secure file sharing solutions by your company? Please select all that apply.	Pct%
Need to comply with HIPAA, PCI, GLBA, SoX and other data privacy regulations	77%
Need to share intellectual data with partners	80%
Need to enable internal and external file collaboration	63%
Need to standardize and control applications	30%
Other	4%
Total	254%

Q23. What function within your company is most likely to need a secure file sharing tool? Please select your three top choices.	Pct%
Accounting & finance	48%
Business operations	20%
C-level senior executives	14%
Compliance	16%
Corporate communications	6%
Corporate IT	42%
Human resources	19%
Information security	13%
Legal	50%
Manufacturing operations	3%
Marketing	3%
Research & development	24%
Sales	41%
Total	300%

Q24. What team within your organization is responsible for selecting secure or public file sharing tools?	Pct%
Messaging team	16%
Enterprise architects	23%
Email security team	5%
Networking team	32%
Security team	13%
General IT infrastructure	6%
Other	5%
Total	100%

Part 3. Role & Organizational Characteristics

D1. What best describes your position level within the organization?	Pct%
Business owner	1%
C-level executive/VP	4%
Director	17%
Manager	21%
Supervisor	16%
Staff/technician	33%
Administrative	5%
Consultant/contractor	3%
Other	0%
Total	100%

D2. Which of the following functional areas do you or your leaders report to within your company?	Pct%
Business owner/board	1%
CEO/executive committee	2%
COO or head of operations	4%
CFO, controller or head of finance	3%
CIO or head of corporate IT	51%
Business unit leader or general manager	15%
Head of compliance or internal audit	5%
Head of risk management	6%
Head of IT security	13%
Other	0%
Total	100%

D3. What best describes your organization's primary industry classification?	Pct%
Aerospace & defense	1%
Agriculture & food services	1%
Communications	3%
Consumer goods	5%
Education & research	3%
Entertainment, media and publishing	2%
Financial services	19%
Health & pharmacueticals	13%
Industrial	6%
Logistics and distribution	3%
Manufacturing	8%
Public sector	8%
Retailing	10%
Services	9%
Technology & software	6%
Transportation	3%
Other	0%
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.