Ponemon INSTITUTE

Breaking Bad: The Risk of Unsecure File Sharing

Sponsored by Intralinks

Independently conducted by Ponemon Institute LLC

Publication Date: October 2014

Breaking Bad: The Risk of Unsecure File Sharing

Ponemon Institute, October 2014

Part 1. Introduction

*Data leakage and loss from negligent file sharing and information collaboration practices is becoming just as significant a risk as data theft***.**

Just like malicious threats from hackers and others, data leakage through the routine and insecure sharing of information is a major threat to many organizations. Being able to securely share valuable corporate data is a critical requirement for all organizations, but especially regulated companies like financial services and life sciences firms.

Many companies have few provisions in place – process, governance, and technology – to adequately protect data. Yet, more and more sensitive information is being shared outside the organization, often without the knowledge or approval of CIOs or GRC professionals who are arguably losing control. Employees are 'behaving badly' – they acknowledge risky behavior and in turn experience the consequences of risky behavior regularly.

For the first time, the study *Breaking Bad: The Risk of Unsecure File Sharing* explores the link between organizational and individual behavior when using increasingly popular file sync-and-share solutions. As shown in this research, organizations are not responding to the risk of ungoverned files-sharing practices among employees as well as with external parties, such as business partners, contractors, vendors and other stakeholders.

Consumer grade file-sharing cloud applications are popular with both employees and organizations because they make it possible for busy professionals to work efficiently together. However, the findings in this report identify the holes in document and file level security in part caused by their expanded use. The goal is to provide solutions to reduce the risk of created by employees' document and file sharing practices.

More than 1,000 IT and IT security practitioners were surveyed in the United States, United Kingdom and Germany. The majority of respondents are at the supervisor level or above with expertise and understanding of their organization's use of file-sharing solutions and overall information security and data privacy policies and strategies.

Following are the key takeaways from this study:

Organizations are vulnerable to data loss and non-compliance. Weak process control, the inability to govern how data is shared and weak file-sharing technology creates the perfect environment for data loss and non-compliance. Seventy percent of respondents say their organization has not conducted an audit or assessment to determine if document and file-sharing activities are in compliance with laws and regulations. Only 9 percent of respondents say their organization is compliant with ISO 27001 (the international standard for process-based security).

Safeguards and GRC mandates are often inadequate. As a result, organizations experience the consequences of lax information security on a regular basis. About half of respondents (between 48 percent and 56 percent of respondents as shown below) are unsure or do not agree that their organizations have the following governance and security practices in place:

- A clear policy for the adoption and use of cloud-based file sharing/file sync-and-share applications (48 percent).
- Clear visibility into the file sharing/file sync and share applications used by employees at work (49 percent).
- The ability to manage and control user access to sensitive documents and how they are shared (50 percent).
- Sufficiently educates individuals annually of the risks of data loss and data theft (56 percent).

Employees behave badly when it comes to data sharing and collaboration.

Employees throughout the organization are often negligent when it comes to data sharing and collaboration. A clear majority of respondents (more than 60 percent) confess they have often or frequently done the following:

- Used their personal file-sharing/file sync-and-share apps in the workplace.
- Sent unencrypted emails.
- Failed to delete confidential documents or files as required by policies.
- Accidentally forwarded files or documents to individuals not authorized to see them.

IT has lost control of decision-making and their company's data.

Only 54 percent of respondents say the organization's IT department is involved in the adoption of new technologies for end users such as cloud, mobile and big data analytics. However, the following practices diminish their ability to control the risk of unsecured file sharing:

- Less than half (46 percent) of respondents say the CISO and CIO have ultimate authority and responsibility for securing document collaboration and file-sharing activities.
- More than 26 percent of applications are being used by various business functions without the IT department's approval or knowledge.
- The primary technology used in the file-sharing environment is white listing and/or black listing tools.

Cross-tabulations by industry, country sample and respondents' position level revealed significant differences.

- Respondents in regulated industries (e.ge financial services, life sciences and healthcare) provide consistently higher ratings for effectiveness and safety of their companies' file sharing practices than respondents in unregulated industries. Nevertheless, almost half of respondents working in regulated industries express concern about their organizations file sharing.

- German country-level results show consistently higher ratings for effectiveness and safety of file sharing practices than respondents in the UK and US country samples, respectively. The UK lags other countries represented in this research. These results may reflect the effectiveness of tighter regulatory regimes.

- Senior-level respondents (i.e., those at or above the director position level) provide consistently higher ratings for effectiveness and safety of their companies' file sharing practices than respondents who are rank-and-file employees (i.e., those below the supervisory level). Consistent with other Ponemon Institute research, executive responses may reflect their convictions rather than the practical realities expressed by senior respondents.

Part 2. Key findings

Information sharing and collaborating is more pervasive than ever due to increased employee mobility, changing work patterns, BYOD, and the competitive advantages that come with being able to work across groups and with partners, suppliers and customers in real-time. Yet, the enhanced ability to readily share company information also potentially exposes organizations to greater risks of data leakage and loss.

In this section, we provide the analysis of the key findings. The complete audited findings are presented in the appendix of this report. The report is organized according to the following themes:

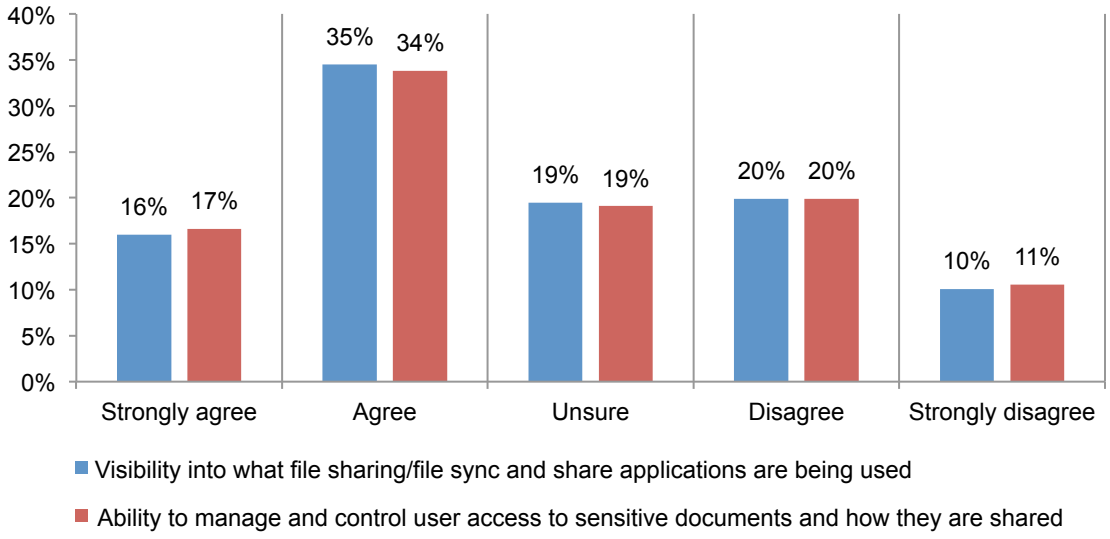
- Organizations are vulnerable to data loss and non-compliance
- Employees behave badly when it comes to data sharing and collaboration
- IT has lost control of decision-making and their company's data

Organizations are vulnerable to data loss and non-compliance.

Many respondents are not confident they can deal with risky file sharing practices. As shown in Figure 1**,** 49 percent of respondents (19 percent + 20 percent + 10 percent) do not agree or are unsure they have clear visibility into employees' use of file sharing/file sync and share applications used in the workplace.

Similarly, 50 percent of respondents (19 percent + 20 percent + 11 percent) do not agree or are unsure their organizations have the ability to manage and control user access to sensitive documents and how they are shared.

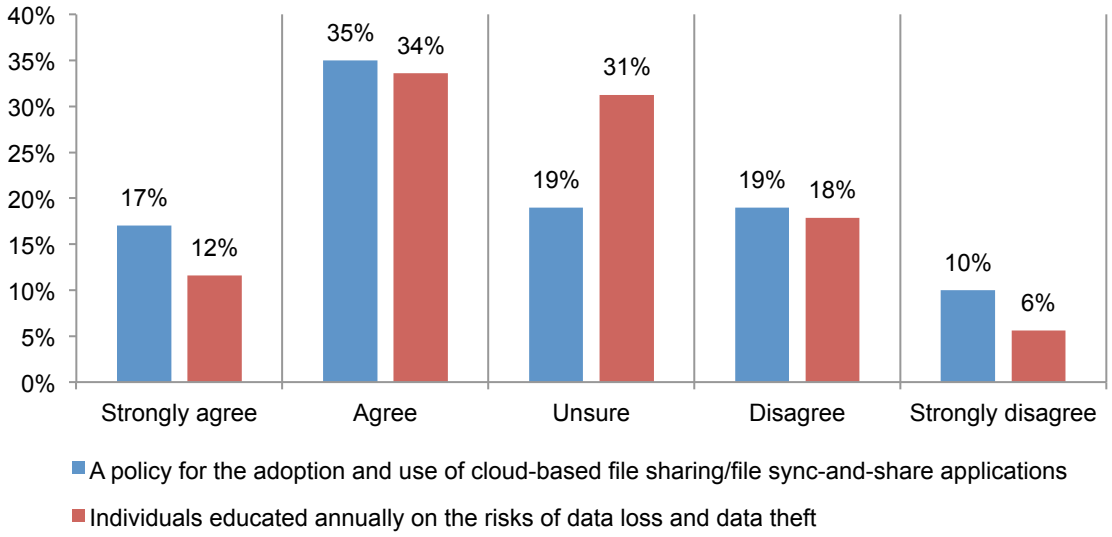
Figure 1. Our organization has visibility into and the ability to manage file-sharing practices



Policies for safeguarding data when using file-sharing applications exist in most organizations but efforts to communicate those policies are lagging. The majority of the organizations represented in this research have policies for managing and controlling data sharing, but often these policies are not being communicated to employees. As a consequence, a majority of respondents are putting sensitive data at risk with poor file-sharing practices.

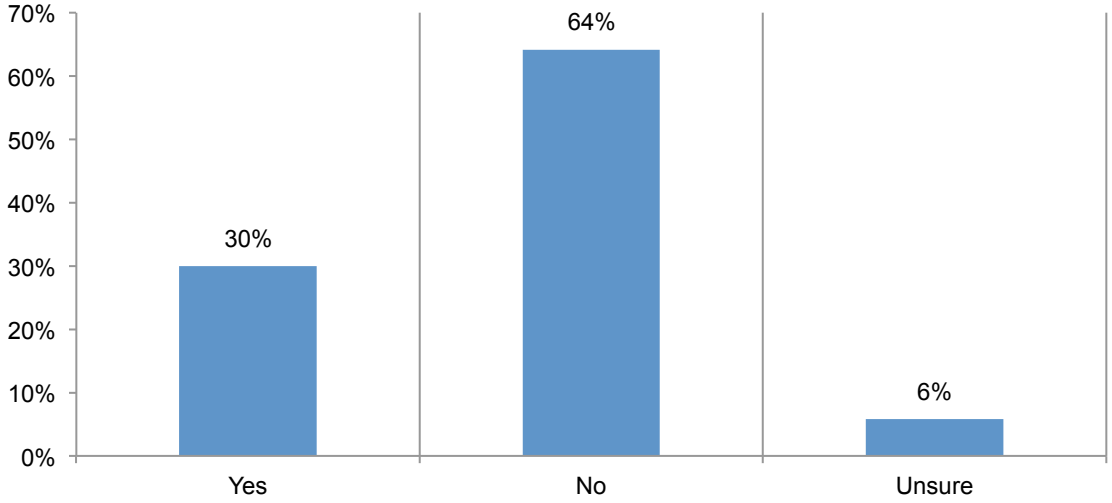
As shown in Figure 2, more than half of respondents (52 percent) say their organizations have a clear policy for the adoption and use of cloud-based file sharing/file sync-and-share applications. But less than half (46 percent) says their organizations have yearly training programs on the risks of data loss and theft. In fact, 31 percent of respondents say they are unsure if such training exists.

Figure 2. Our organization has policies for the secure use of file sharing applications and training programs



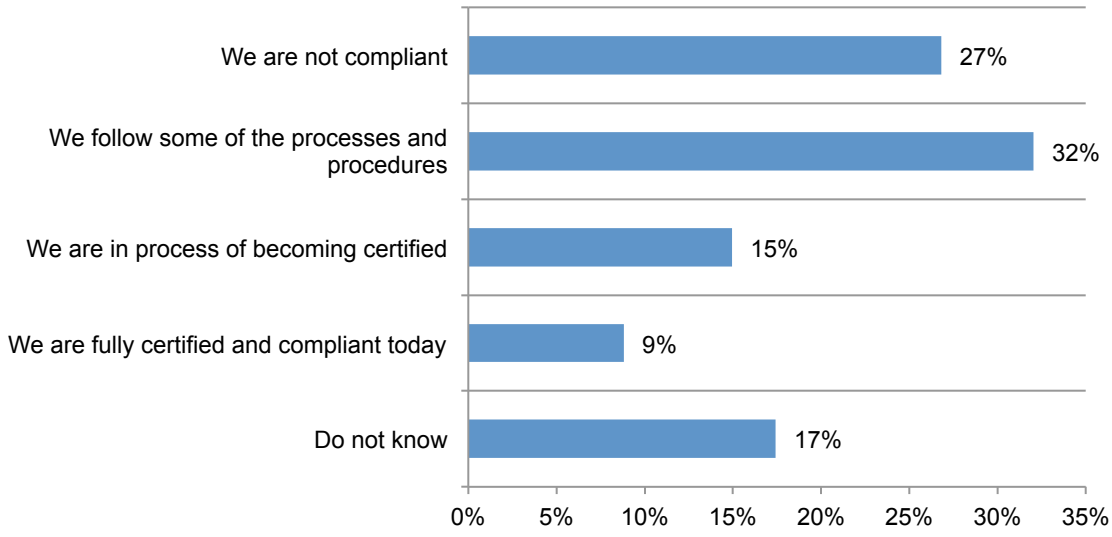
Companies are not conducting audits or assessments to determine if their file-sharing activities are in compliance. Despite the risk, 64 percent of respondents say their organizations are in the dark about whether or not file-sharing activities are in compliance with laws and regulations, as shown in Figure 3. They have not conducted audits or assessment in the past 24 months.

Figure 3. Are audits or assessments conducted to determine if document and file sharing activities are in compliance with laws and regulations?



As shown in Figure 4, only 9 percent of respondents say their organizations are certified and fully compliant today with ISO 27001 (the international standard for process-based security.

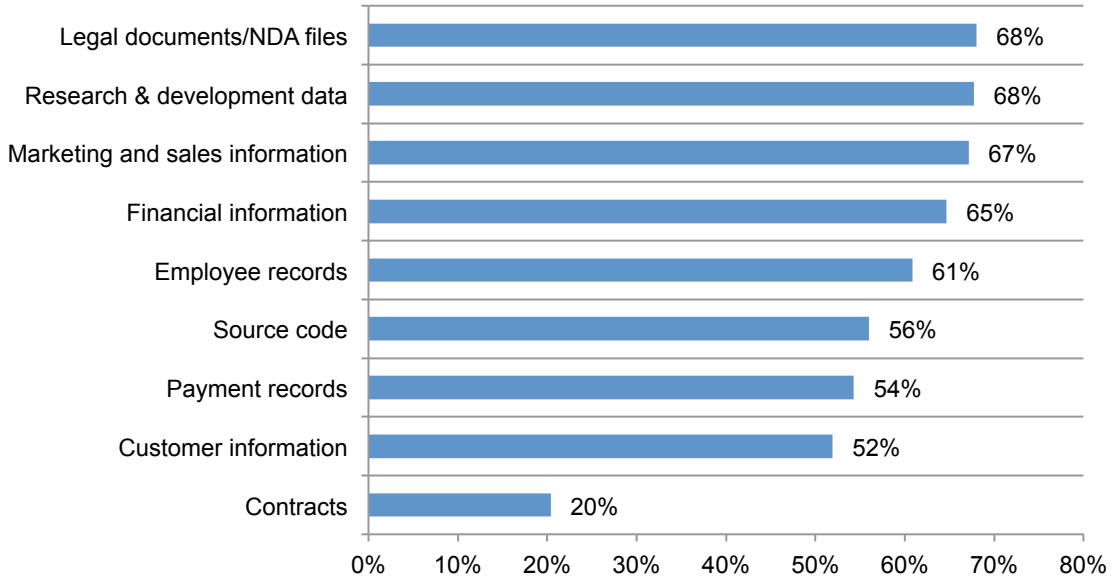
Figure 4. Compliance with ISO 27001



Companies restrict sensitive documents from being shared with third parties. Fifty percent of respondents say that more than half of their organization's documents containing sensitive or confidential information are exchanged with third parties.

As shown in Figure 5, documents such as confidential financial information, research & development data, legal documents/NDA files, and marketing and sales information are restricted by about two-thirds of respondents. However, only slightly more than half of respondents (52 percent) restrict customer information that is subject to regulations. This finding indicates that organizations may be in risk of non-compliance when sharing files.

Figure 5. Types of documents restricted from sharing with third parties
More than one response permitted

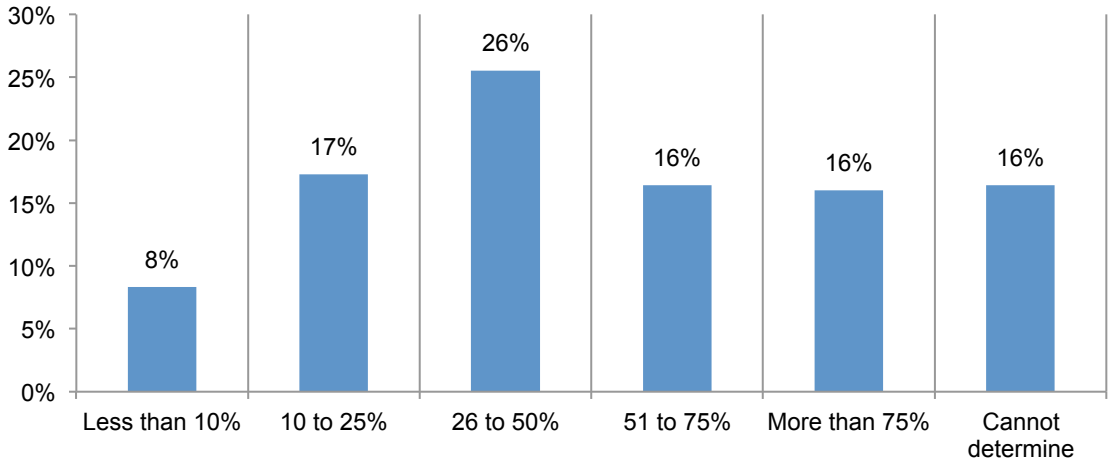


Employees behaving badly put their organizations at risk

Employees throughout the organization behave badly when it comes to data sharing and collaboration. Safeguards and GRC mandates are often inadequate and as a result organizations experience the consequences of lax information security on a regular basis.

Figure 6 reveals that almost one-third of respondents (16 percent + 16 percent) say more than half of employees in their organizations regularly share files outside the company/beyond the firewall. Sixteen percent cannot determine.

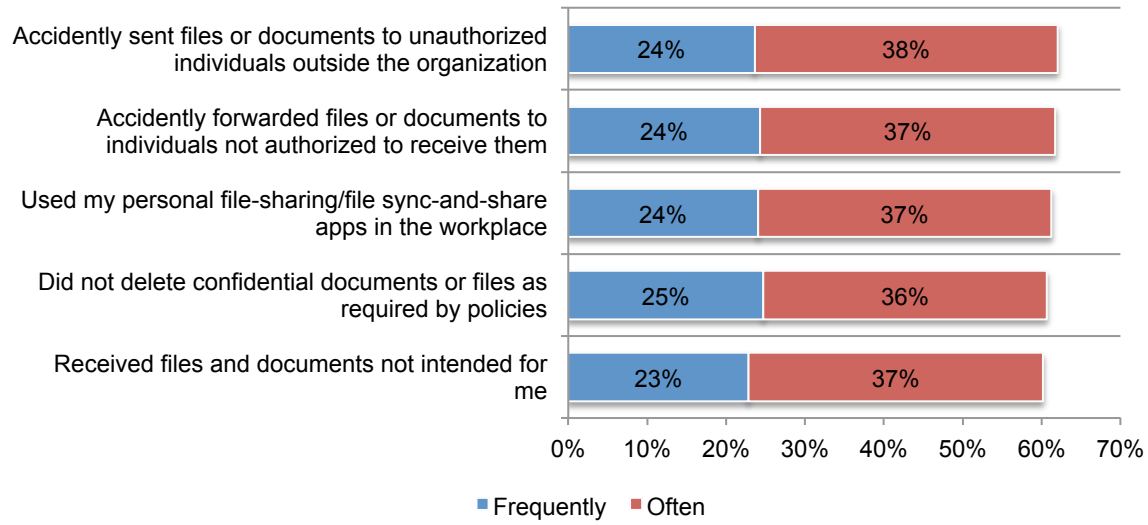
Figure 6. Frequency of employees' sharing files outside the company/beyond the firewall



Risky file sharing practices are occurring with high frequency in organizations represented in this study. According to Figure 7, employees are putting their organizations at risk through negligence and ignoring policies. The following practices are happening frequently or often in the majority of organizations:

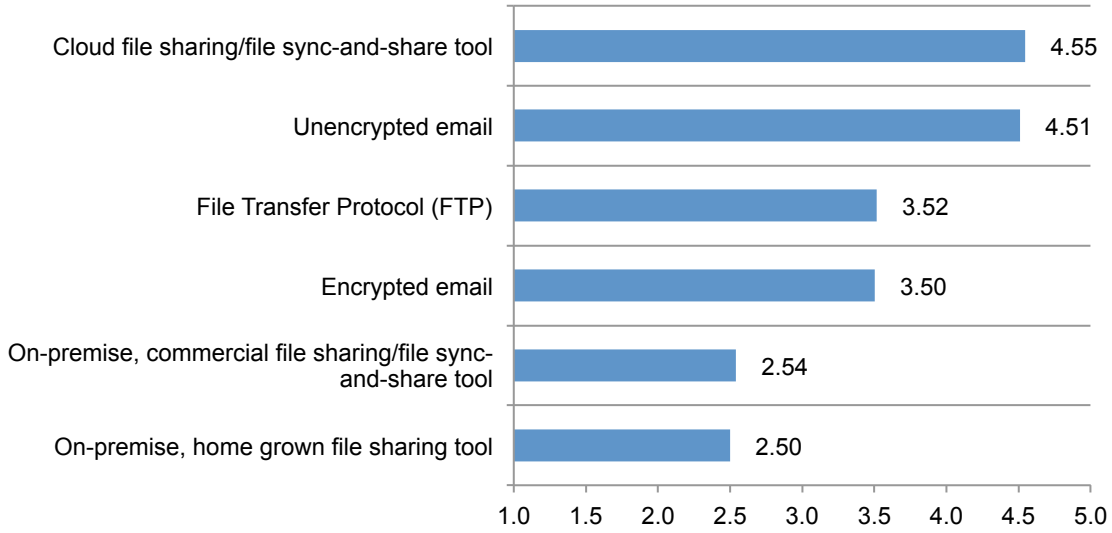
- Receives files and documents not intended for the recipient (60 percent)
- Ignores policies and does not delete confidential documents or files (61 percent)
- Accidently forwards files or documents to individuals not authorized to receive them (61 percent)
- Accidently sent files or documents to unauthorized individuals outside the organization (62 percent)
- Uses their personal file-sharing/file sync-and-share apps in the workplace (62 percent)

Figure 7. Risky practices by employees
Frequently and often responses combined



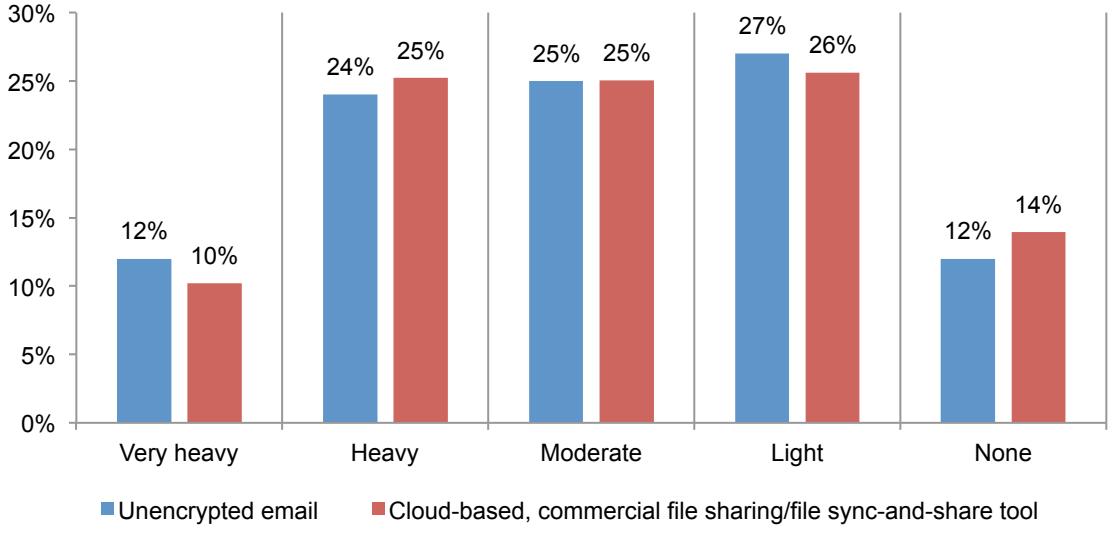
Respondents rank cloud file sharing and unencrypted email as the two most risky file sharing technologies in use. Respondents were asked to rank the level of risk certain file-sharing technologies pose to the organization. According to Figure 8, the use of cloud applications leads in risk followed by unencrypted email.

Figure 8. File sharing technologies ranked based on their level of information security risk
6 = highest risk to 1 = lowest risk



How heavy is the usage of these more risky file-sharing technologies? As shown in Figure 9, Thirty-five percent of respondents (10 percent + 25 percent) say there is heavy usage of commercial cloud-based file sharing and 36 percent (12 percent + 24 percent) say usage of unencrypted email sharing is very heavy or heavy. Based on these findings, use of file sync and share is as ubiquitous as email.

Figure 9. How heavy is the use of risky file-sharing technologies?

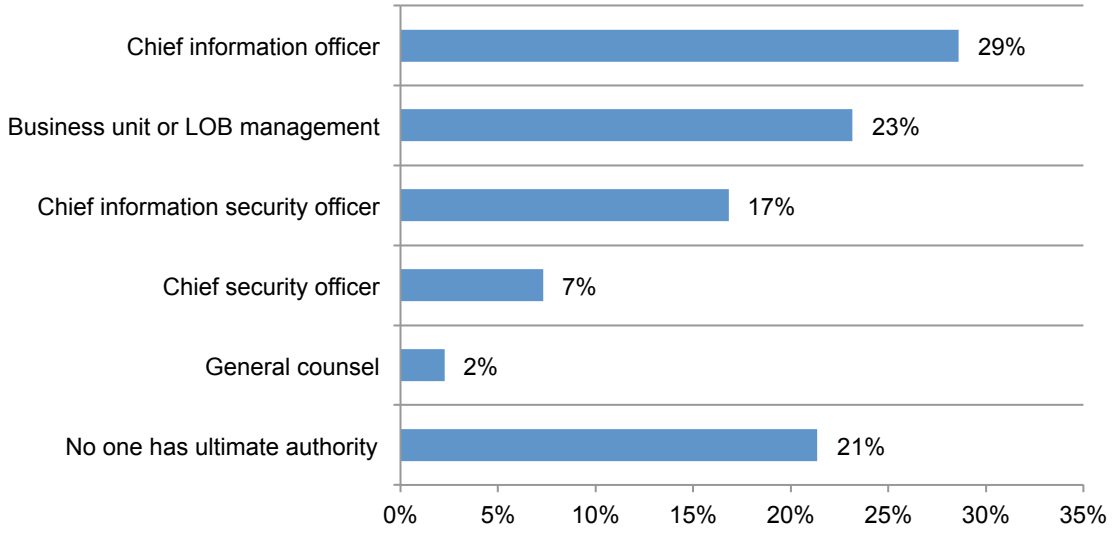


IT has lost control of decision-making and their company's data

Fifty-four percent of respondents say the organization's IT department is involved in the adoption of new technologies for end users such as cloud, mobile and big data analytics. However, their ability to control the risk of unsecured file sharing has been diminished by the increasing influence of business units in how file sharing and collaboration applications are used.

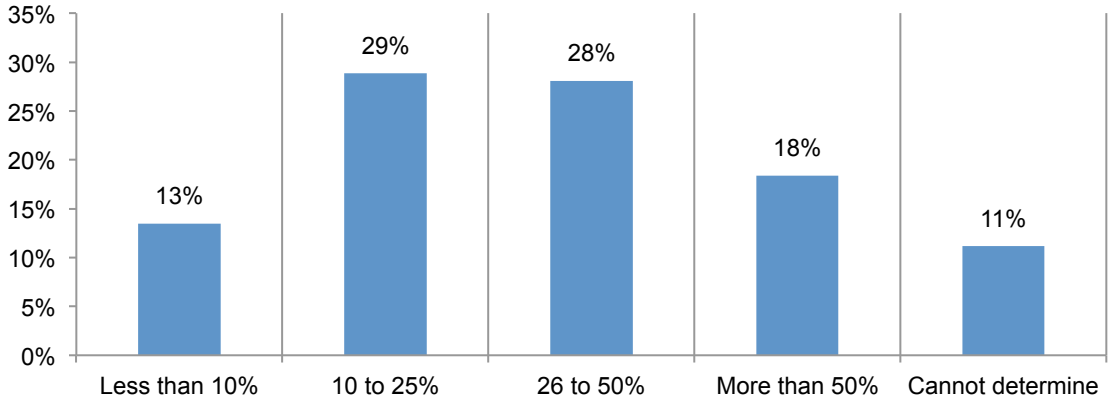
The majority of respondents say the organization's IT department is involved in making sure documents that are shared are secure. However, several respondents (21 percent) say no one has the ultimate authority to ensure safeguards are in place. Forty-six percent of respondents (29 percent + 17 percent) say the CISO and CIO have ultimate authority and responsibility for securing document collaboration and file-sharing activities, according to Figure 10.

Figure 10. Who has ultimate authority and responsibility for securing document collaboration and file sharing activities?



According to Figure 11, 46 percent of respondents say more than 26 percent of applications are being used by various business functions without the IT department's approval or knowledge and 11 percent cannot determine

Figure 11. Applications used without IT's approval or knowledge



Companies are less likely to control mobile devices and laptops. According to Figure 12, technologies most often used in the file-sharing environment are: white listing and/or black listing tools (63 percent of respondents) and identity and access management tools (51 percent of respondents).

Least used are mobile device management (MDM) to lock down mobile devices or laptops and remotely erase them (27 percent of respondents) and ability to obtain data location when using cloud services (24 percent of respondents).

Figure 12. Technologies used in the file-sharing environment
More than one response permitted

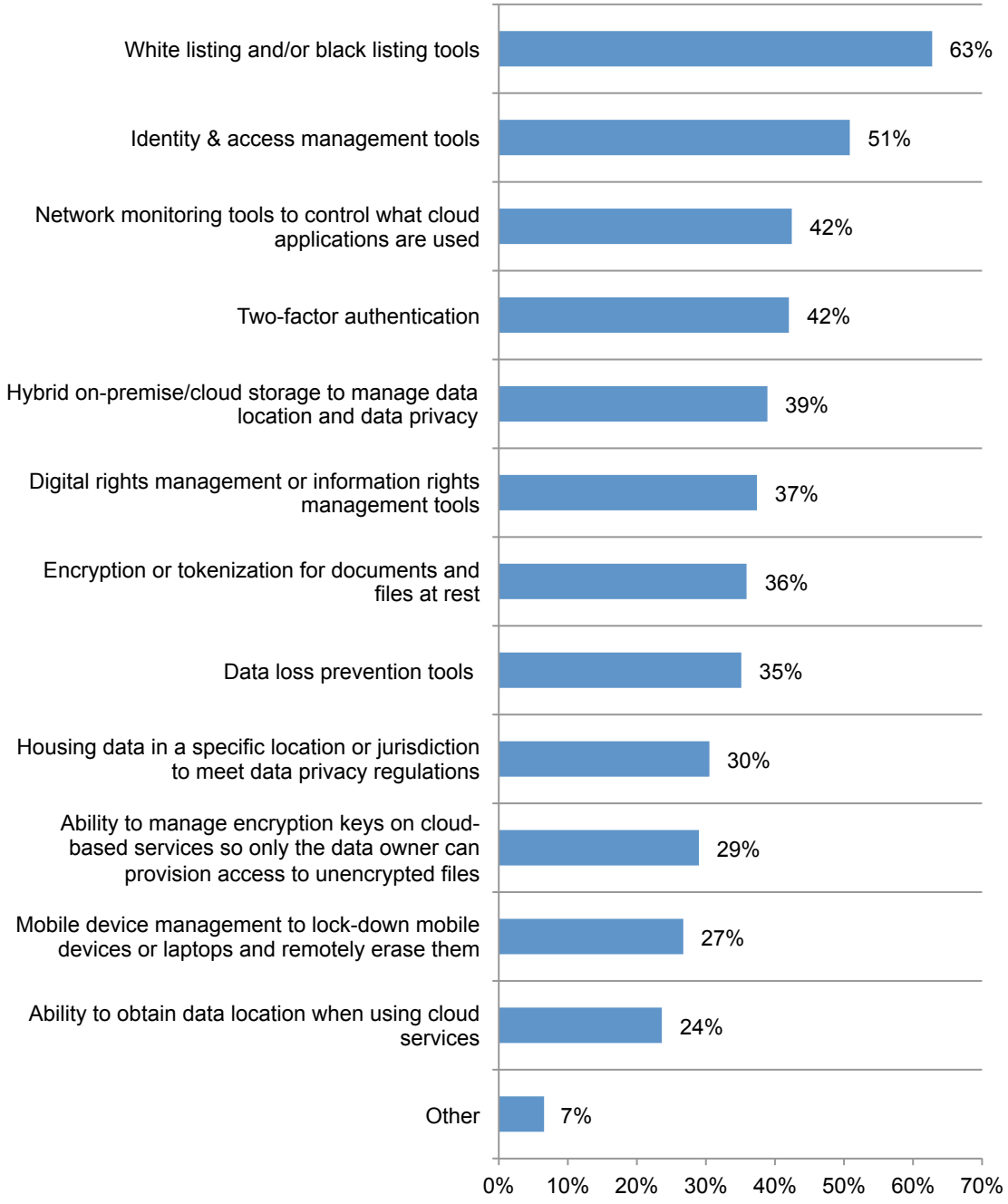
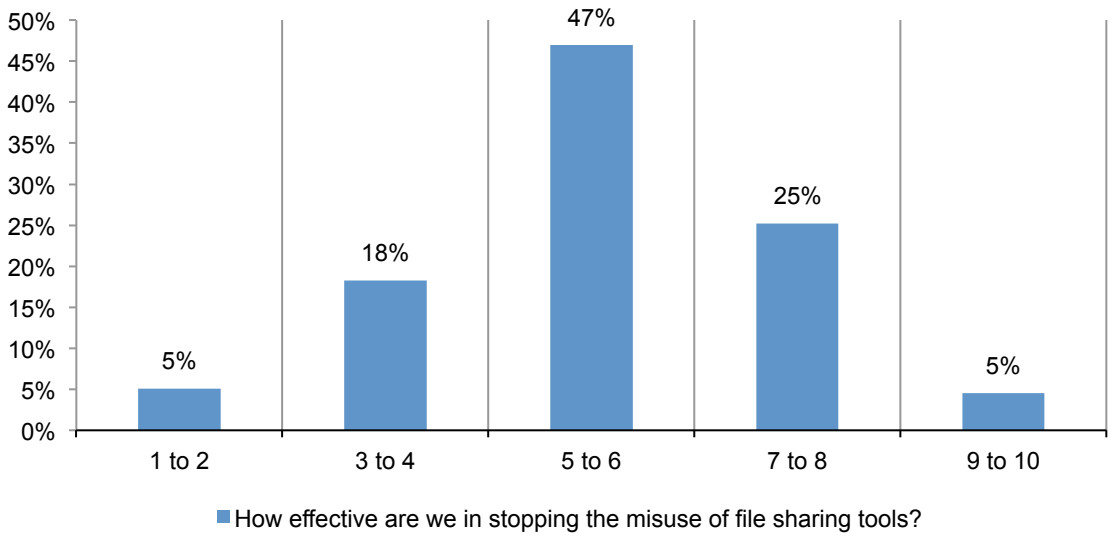


Figure 13 reveals perceptions about organizations' effectiveness in setting permissions to access sensitive or confidential documents and files, stopping the use of unapproved file sharing tools and stopping the misuse of file sharing tools as average. A large number of respondents rate their effectiveness level at or below average (70 percent). The consolidated average rating is 5.61.

Figure 13. The effectiveness in setting permissions and stopping the use/misuse of file sharing tools

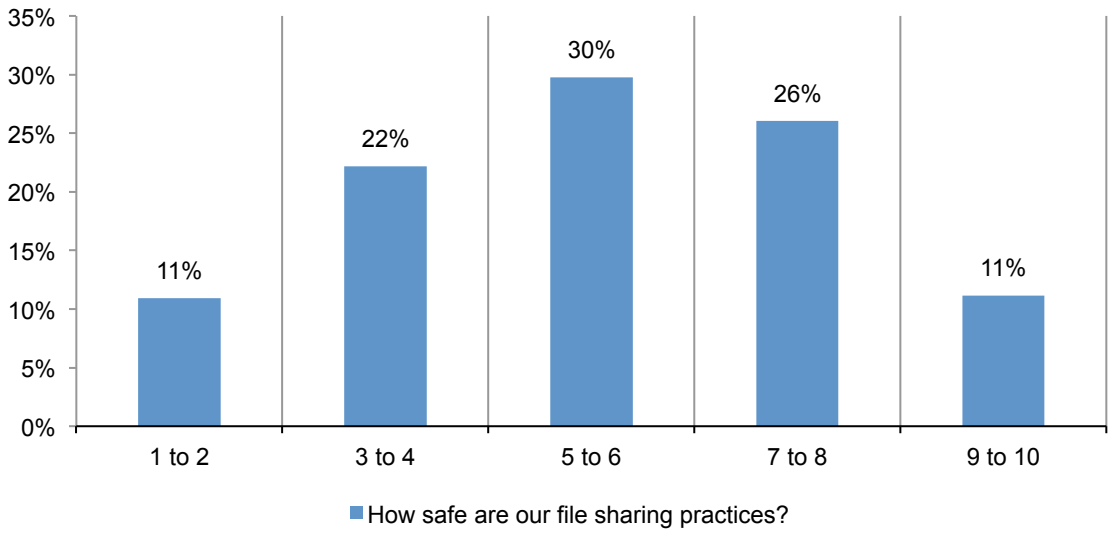
1 = not effective to 10 = very effective



The safety of file-sharing approaches is rated at average. Respondents were asked to rate the safety of their organizations' various file-sharing practices. Figure 14 shows their perceptions about four different aspects of file-sharing: the process, procedures and technologies, approach to file sharing among peer organizations, personal approach to file sharing and employees' approach to file sharing. The consolidated average safety risk is 5.59.

Figure 14. How safe are the file-sharing practices in organization?

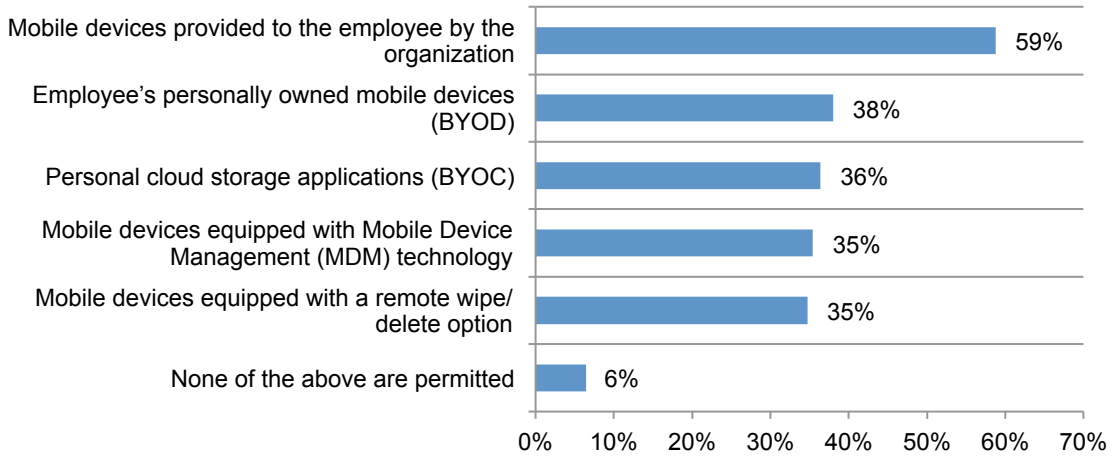
1 = not safe to 10 = very safe



BYOD is not preferred if mobile devices are to be used for file sharing or document collaboration. Fifty-nine percent of respondents say they allow employees to share or collaborate on documents if the company provides the mobile device, according to Figure 15.

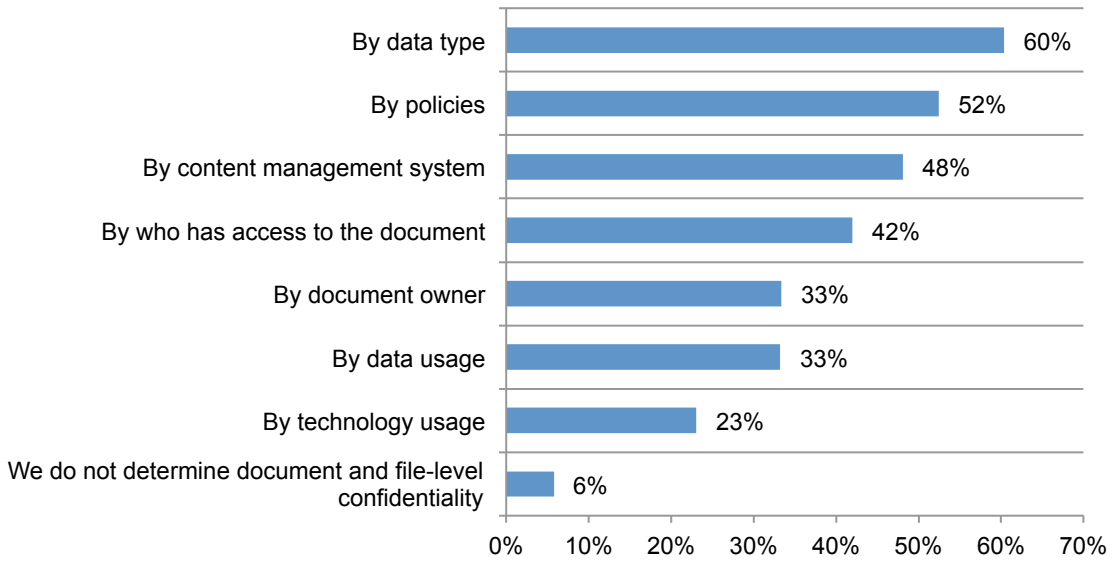
However, organizations put information at risk when they allow personal devices or personal cloud storage for file sharing and collaboration. As shown, 38 percent of respondents allow BYOD and 36 percent allow BYOC.

Figure 15. Which mobile devices are permitted for file sharing or document collaboration
More than one response permitted



Determining document and file-level confidentiality is mostly made by data type and policies. Figure 16 reveals that 60 percent of respondents determine document and file-level confidentiality by data type and 52 percent by policies. Less than half (48 percent) use a content management system to determine confidentiality.

Figure 16. How organizations determine document and file-level confidentiality



Part 3. Industry differences

In this section we analyze survey differences between two industry groups: regulated and unregulated companies. Approximately, 55 percent of the total sample represents regulated industries and the remaining 45 percent represent unregulated companies.

Companies regulated by specific data protection legislation include:

- Financial services
- Public sector
- Healthcare
- Energy & utilities
- Communications,
- Life sciences
- Education & research

Companies not regulated by industry-specific data protection laws include:

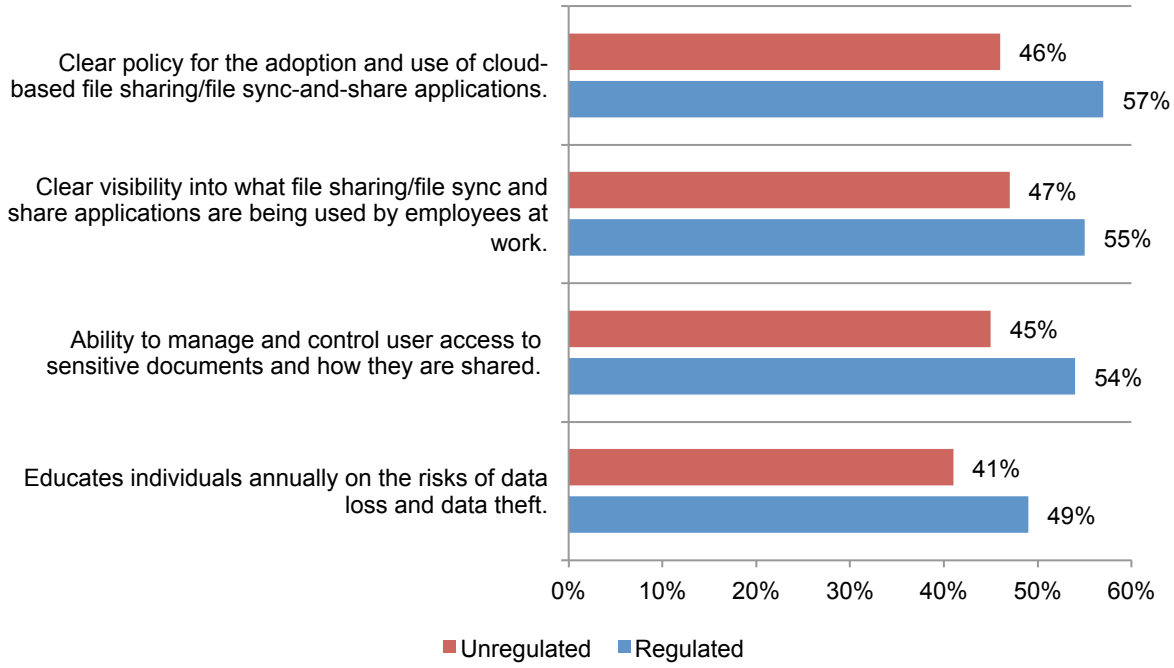
- Retail
- Technology
- Consumer products t
- Transportation
- Hospitality
- Entertainment & media
- Agriculture & food services
- Defense & aerospace.

In Figure 17, we summarize responses to four attributions for two industry groups. The attributions, which were rated from strongly agree to strongly disagree, are stated precisely as follows in the survey instrument:

- **Attribution 1**. Our organization has a clear policy for the adoption and use of cloud-based file sharing/file sync-and-share applications.
- **Attribution 2**. Our organization has clear visibility into what file sharing/file sync and share applications are being used by employees at work.
- **Attribution 3**. Our organization has the ability to manage and control user access to sensitive documents and how they are shared.
- **Attribution 4**. Our organization educates individuals annually on the risks of data loss and data theft.

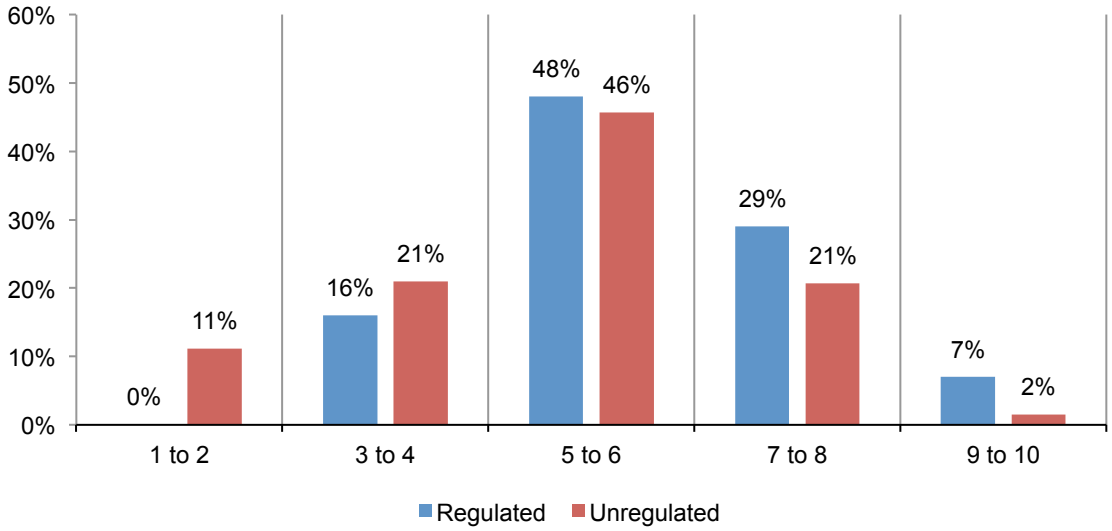
Results are fairly consistent for all attributions – that is, respondents in regulated industries provide a higher rate of agreement than those in unregulated industries. The largest difference between industry groups concerns the existence of a clear policy (Diff = 11 percent) and the ability to manage and control user access to sensitive documents (Diff = 9 percent).

Figure 17. Four attributions about the organization's file sharing practices by industry
Strongly agree and agree responses combined



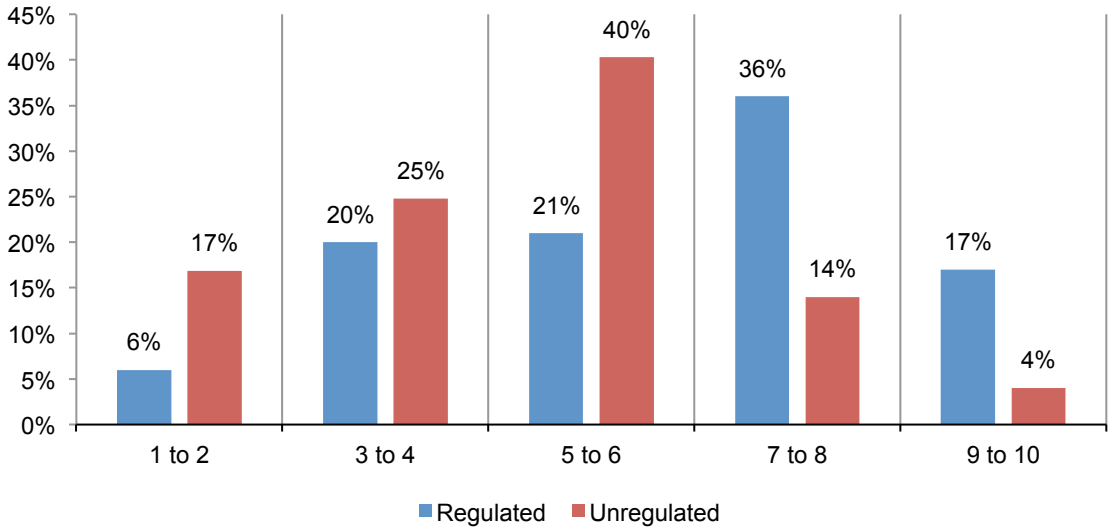
As shown in Figure 18, respondents in regulated industries believe their companies are more effective in stopping the misuse of file sharing tools than respondents in unregulated industries. The extrapolated average rating for regulated companies on a 10-point effectiveness scale is 6.04. In contrast, unregulated companies had an average rating of 5.11 – which is below the mean of 5.5.

Figure 18. How effective are we in stopping the misuse of file sharing tools by industry groups?
1 = not effective to 10 = very effective



Similar to the above industry group differences, Figure 19 shows respondents in regulated industries believe their companies achieve a higher level of safety with respect to file sharing practices than those in unregulated industries. The extrapolated average rating for regulated companies on a 10-point safety scale is 6.26. In contrast, unregulated companies had an average rating of 4.77 – which is below the mean of 5.5.

Figure 19. How safe are our file sharing practices by industry groups?
1 = not safe to 10 = very safe



Part 4. Country sample differences

In this section we analyze possible differences among three country samples: United States (US), United Kingdom (UK) and Germany (DE). In Figure 20, we summarize responses to four attributions about file sharing practices, which were rated from strongly agree to strongly disagree. For purposes of simplicity, we show the strongly agree and agree response combined.

Results show that German respondents provide the highest rate of agreement to the four attributions about file sharing practices. In contrast, respondents in the UK provide the lowest rate of agreement to these four attributions. At 56 percent agreement for German respondents, the highest rating concerns a clear policy on the adoption and use of cloud-based file sharing/file sync-and-share applications. At 43 percent agreement for UK respondents, the lowest rating concerns educating individuals on the risks of data loss and data theft.

Figure 20. Four attributions about the organization's file sharing practices by country sample
Strongly agree and agree responses combined

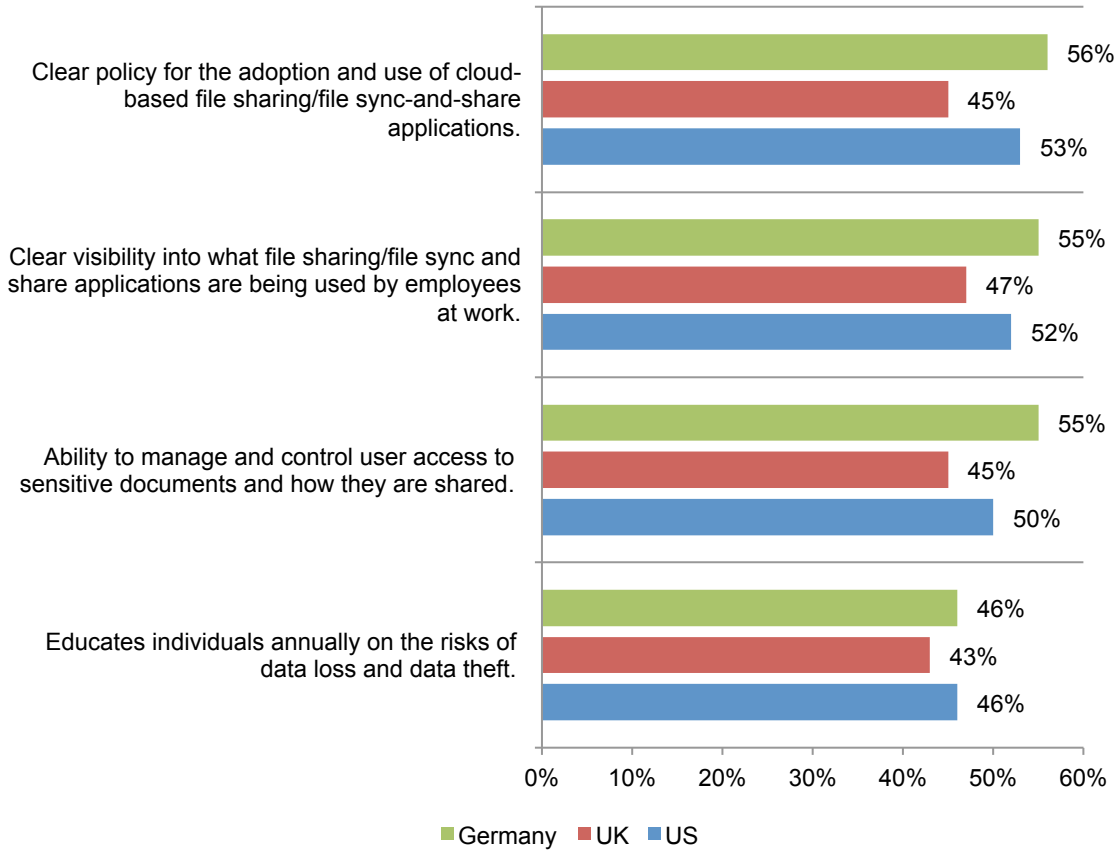
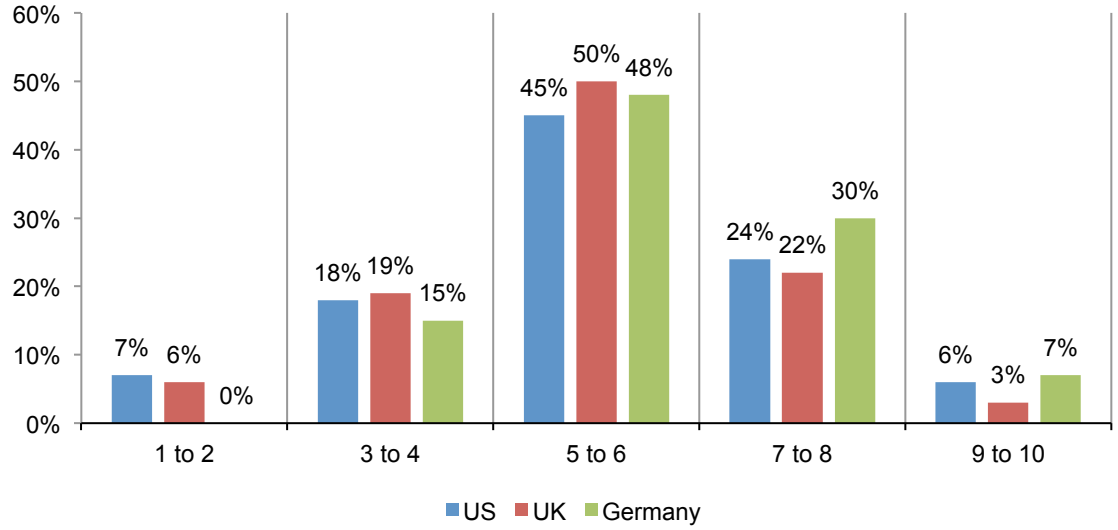


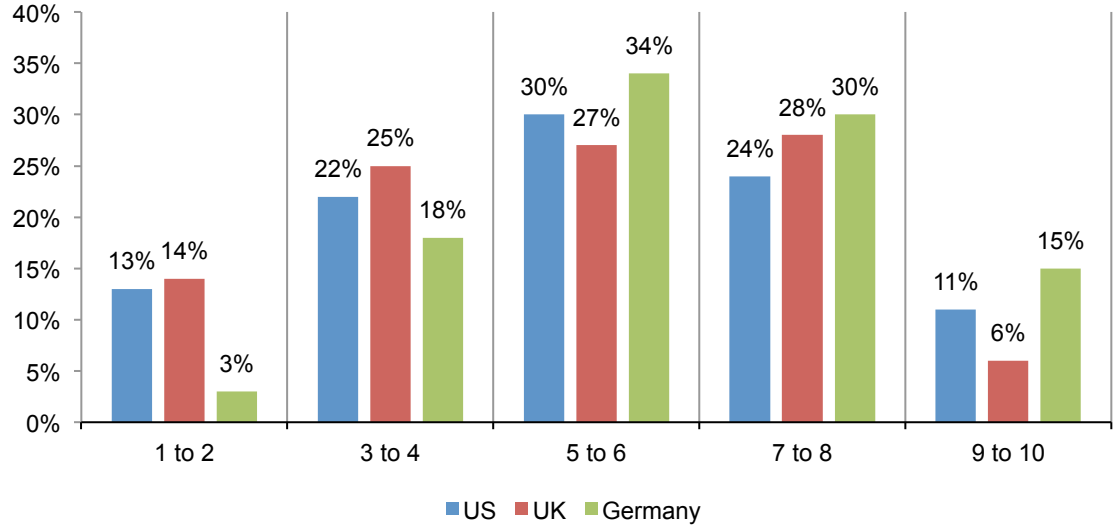
Figure 21 shows German respondents achieve a higher effectiveness rating with respect to stopping the misuse of file sharing tools than respondents in the UK and US. The extrapolated average rating for German respondents on a 10-point effectiveness scale is 6.08. In contrast, UK respondents had an average rating of 5.44 – which is below the mean of 5.5.

Figure 21. How effective are we in stopping the misuse of file sharing tools by country samples?
1 = not effective to 10 = very effective



According to Figure 22, German respondents say their companies achieve a higher of level of safety than UK and US companies with respect to file sharing. The extrapolated average rating for German respondents on a 10-point safety scale is 6.22. In contrast, UK respondents had an average rating of 5.24 – which is below the mean of 5.5.

Figure 22. How safe are our file sharing practices by country samples?
1 = not safe to 10 = very safe

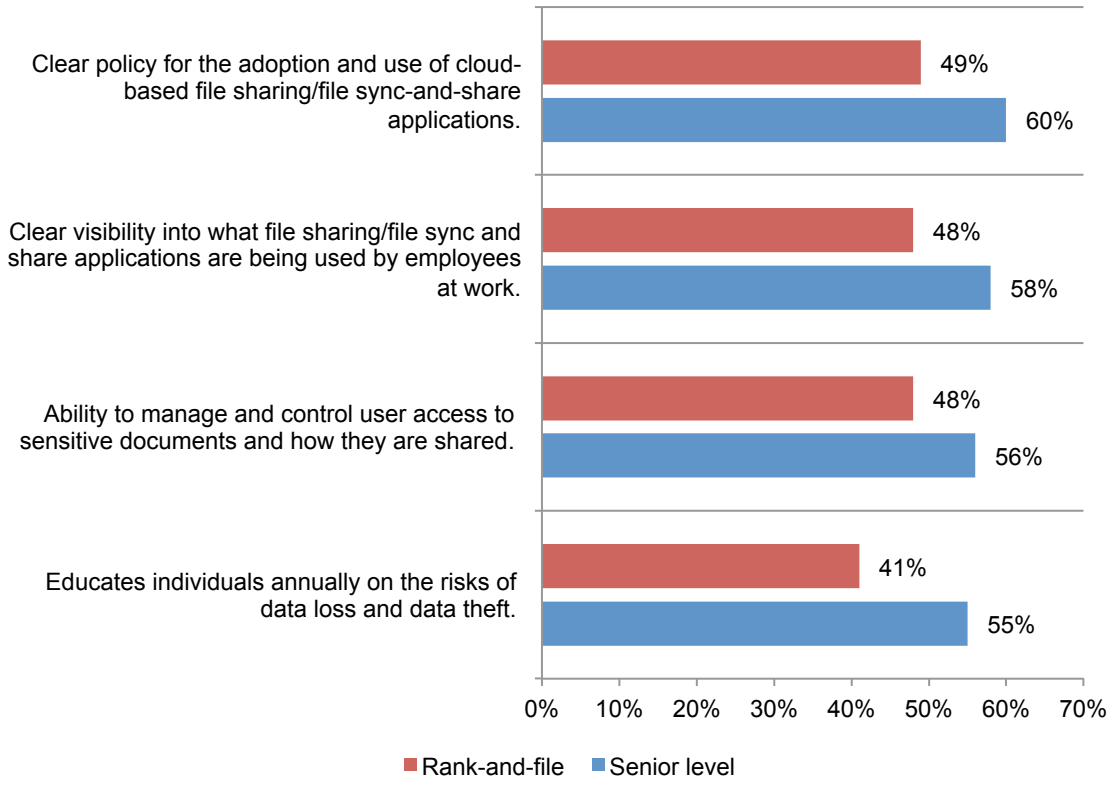


Part 5. Position-level differences

In this section we analyze survey differences between two groups: senior-level respondents and rank-and-file respondents. We define senior-level respondents as those who are at or above the director position level. Rank-and-file respondents are technicians, associates or staff-level employees.[1]

Once again, results are fairly consistent – that is, senior-level respondents provide a higher rate of agreement than rank-and-file respondents. The largest differences between these position-level groups concern educating individuals on the risks of data loss (Diff = 14 percent) and the existence of a clear policy (Diff = 11 percent).

Figure 23. Four attributions about the organization's file sharing practices by respondents' position level
Strongly agree and agree responses combined



[1]A total of 431 respondents at the manager or supervisor level was removed from the revised sample. Of the remaining 580 respondents, 175 are at or above the director level and 405 are below the supervisor level.

Figure 24 shows senior-level respondents rate their companies at a higher level of effectiveness with respect to stopping the misuse of file sharing tools than unregulated companies. The extrapolated average rating for senior-level respondents on a 10-point effectiveness scale is 6.32. The average effectiveness rating for rank-and-file respondents is 5.27 – which is below the mean of 5.5.

Figure 24. How effective are we in stopping the misuse of file sharing tools by position level?
1 = not effective to 10 = very effective

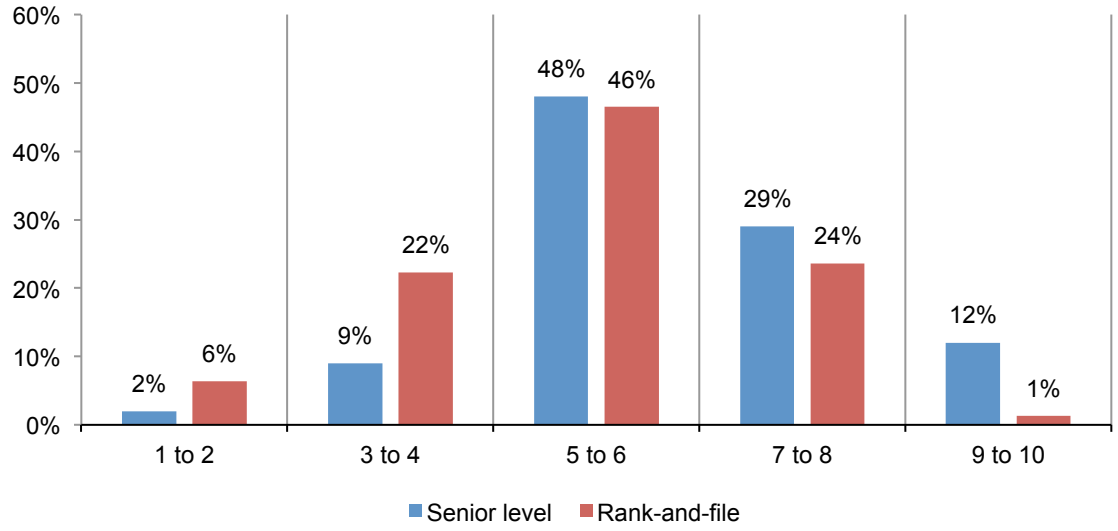
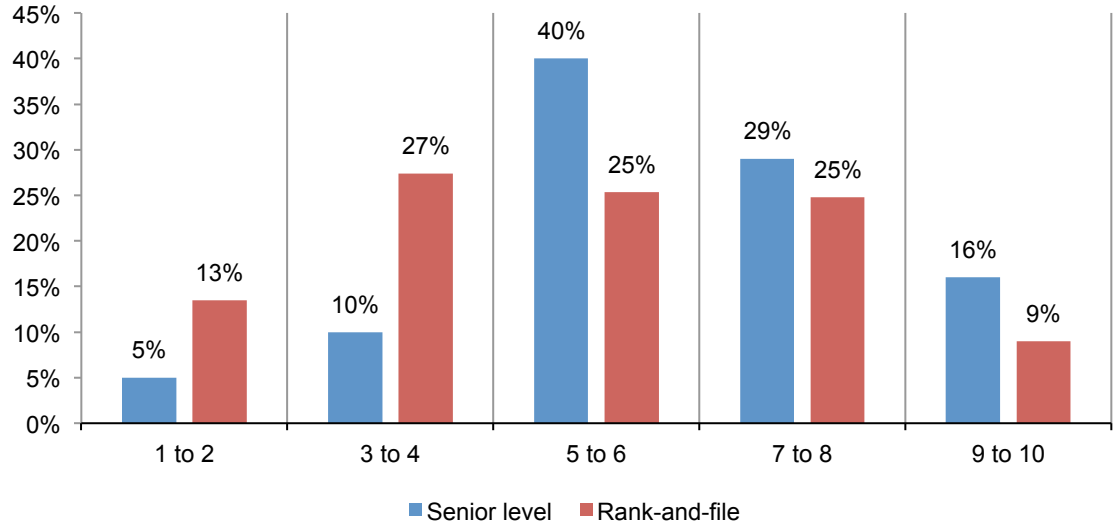


Figure 25 shows senior-level and rank-and-file respondents' rating with respect to the safety of their companies' file sharing practices. Once again, senior-level respondents provide higher ratings, on average, than rank-and-file respondents. The extrapolated average rating from senior-level respondents on a 10-point safety scale is 6.30. In contrast, rank-and-file respondents had an average rating of 5.32 – which is below the mean of 5.5.

Figure 25. How safe are our file sharing practices by position level?
1 = not safe to 10 = very safe



Part 6. Conclusion

File sync-and-share applications are popular because of their ability to make individuals more productive. Employees' ability to work across groups and with partners, suppliers and customers in real-time can be a competitive advantage for organizations. However, the benefits created need to be supported by security policies and enabling technologies.

What is the extent of the risk of data loss due to unsecured file sharing? As shown in the study, employees are regularly sending unencrypted emails, not deleting confidential documents or files as required by policies, accidentally forwarding files or documents to individuals not authorized to see them and using their personal file-sharing/file sync-and-share apps in the workplace.

However, despite the financial loss and damage to reputation when data is lost, organizations are not responding appropriately to the risk. Seventy percent of respondents say their organization has not conducted an audit or assessment to determine if document and file-sharing activities are in compliance with laws and regulations. Only 9 percent of respondents say their organization is compliant with ISO 27001 (the international standard for process-based security).

The following are key considerations for secure information sharing in the collaborative environment:

- Recognize that employees are already using unmanaged file-sharing solutions that are putting your corporate data at risk.
- Tools often employed by IT to control the adoption of unsecure file sharing and cloud services, for example blacklisting, aren't always effective and can be circumvented by employees.
- IT needs to provision alternative collaboration services that keeps employees productive but meets security and GRC requirements.
- Have a clear policy for the adoption and use of cloud-based file sharing/file sync-and-share applications. This should reduce the risks created when various business functions use these applications without the IT department's approval or knowledge.
- Establish regular training and awareness programs to make sure employees and other insiders understand the risks of data loss and data theft, especially when in engaging in document sharing and collaboration.
- Centralize the ultimate authority and responsibility for securing document collaboration and file-sharing activities with those who have the expertise, namely IT and IT security practitioners.
- Conduct regular audits and assessments to ensure document sharing and collaboration practices are in compliance with regulations.
- Improve the organizations ability to have clear visibility into the file sharing/file sync and share applications used by employees at work.
- Deploy identity and access management tools to manage and control user access to sensitive documents and how they are shared.
- Adopt solutions that employ new information right management technology that provide lifetime control of files, even after they have been shared. IRM guards against even accidental mishandling of files by being able to revoke access on demand.
- Adopt technologies that target the risk created by employees behaving badly.

Companies need to take steps to understand how data is being shared and distributed, and take steps to adequately protect data wherever it travels. This will require a combination of education, process control, governance, and technology. Failure to take action is resulting in data loss, with consequential loss of reputation, competitive advantage and potential regulatory fines.

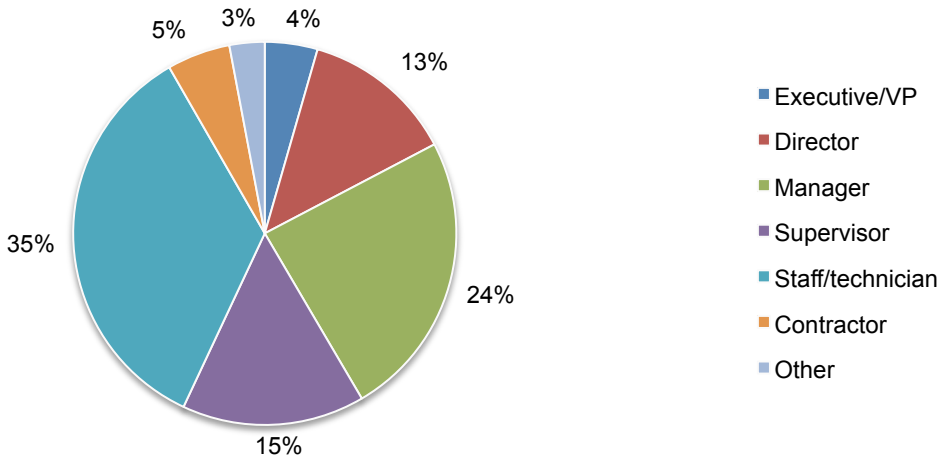
Part 7. Methods

A sampling frame composed of 29,987 IT and IT security practitioners located within the United States, United Kingdom and Germany was selected for participation in this survey. As shown in the following table, 1,196 respondents completed the survey. Screening removed 185 surveys. The final sample was 1,011 surveys (or a 3.4 percent response rate).

Table 1. Sample response	Freq	Pct%
Total sampling frame	29,987	100.0%
Returns	1,196	4.0%
Rejected and screened surveys	185	0.6%
United States	495	1.7%
United Kingdom	262	0.9%
Germany	254	0.8%
Total sample	1,011	3.4%

Pie Chart 1 reports the organizational level for survey participants. In total, 56 percent of respondents are at or above the supervisory level.

Pie Chart 1. Position level within the organization



As shown in Pie Chart 2, over half of the respondents (62 percent) have business operations in more than six countries.

Pie Chart 2. Number of countries the organization has business operations in

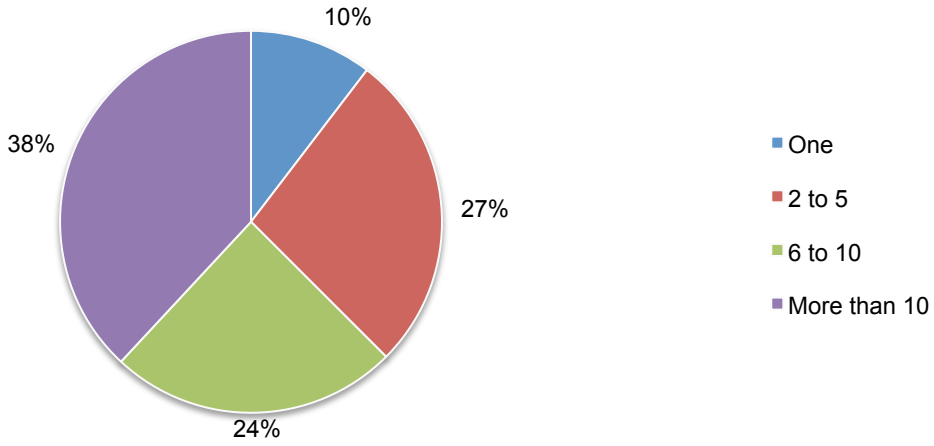
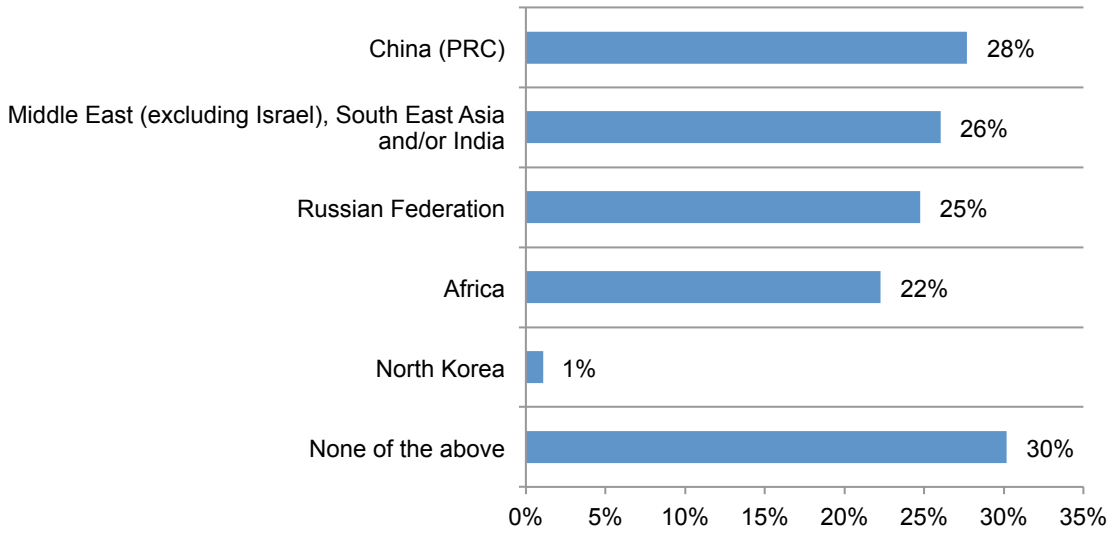


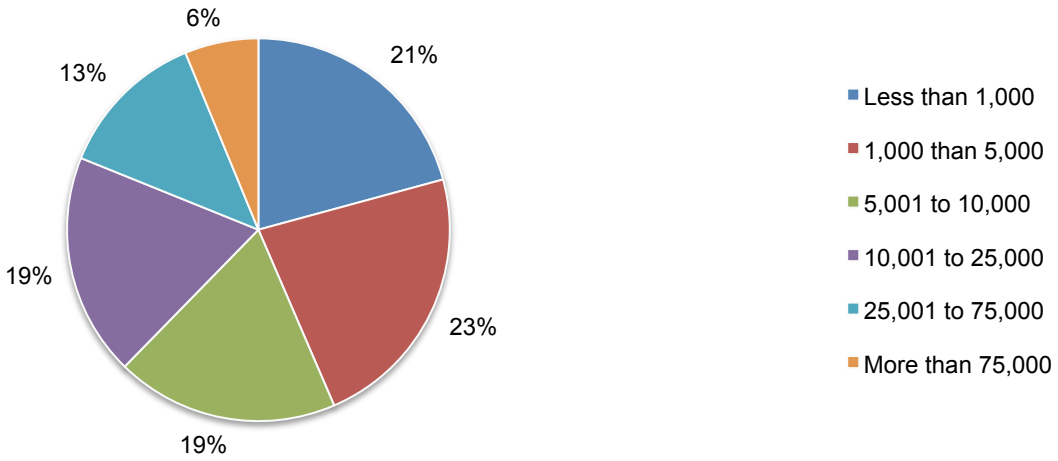
Figure 26 reveals that 28 percent of respondents indicated they have direct operations, sales presence or direct suppliers in China, 26 percent responded Middle East (excluding Israel), South East Asia and/or India. Twenty-two percent indicated they have a business presence in Africa.

Figure 26. Does you organization have direct operations, sales presence or direct suppliers in any of the following countries?
More than one response permitted



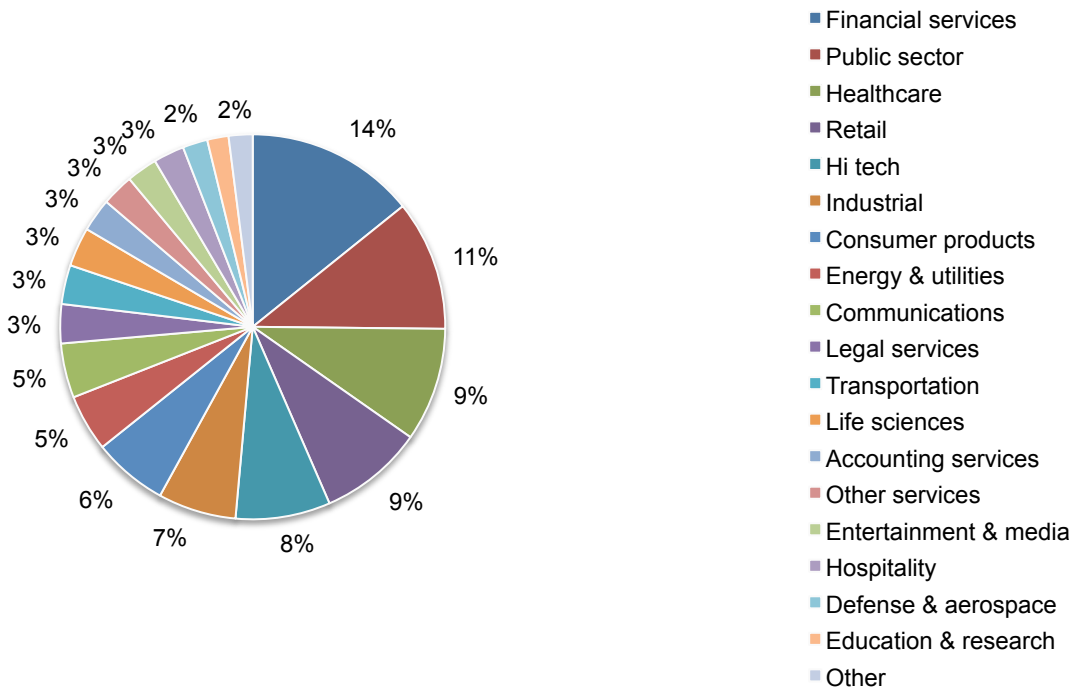
According to Pie Chart 3, more than half of the respondents (57 percent) are from organizations with a full-time global headcount of over 5,000 employees.

Pie Chart 3. Full-time headcount of the global organization



Pie Chart 4 reports the primary industry focus of respondents' organizations. This chart identifies financial services (14 percent) as the largest segment, followed by public sector (11 percent) and healthcare and retail, both at nine percent.

Pie Chart 4. Primary industry classification



Part 8. 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 in various organizations in the United States, United Kingdom and Germany. 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 specified time 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 accurate responses.

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 July 2014.

Sample response	**Freq**	**Pct%**
Total sampling frame	29,987	100.0%
Returns	1,196	4.0%
Rejected and screened surveys	185	0.6%
United States	495	1.7%
United Kingdom	262	0.9%
Germany	254	0.8%
Total sample	1,011	3.4%

Part 1. Screening

S1. What best describes your organization's use of file sharing solutions?	Freq	Pct%
Very heavy	152	15%
Heavy	278	27%
Moderate	298	29%
Light	258	26%
No	25	2%
Total	1,011	100%

S2. What best describes your familiarity with your organization's overall information security and data privacy policy and strategy	Freq	Pct%
Very familiar	124	12%
Familiar	299	30%
Somewhat familiar	293	29%
Not familiar	270	27%
No knowledge	25	2%
Total	1,011	100%

Part 2. Role & organizational characteristics

D1. What best describes your position level within the organization?	Freq	Pct%
Executive/VP	45	4%
Director	130	13%
Manager	245	24%
Supervisor	156	15%
Staff/technician	351	35%
Contractor	54	5%
Other	30	3%
Total	1,011	100%

D2. Approximately how many countries does your organization have business operations?	Freq	Pct%
One	105	10%
2 to 5	274	27%
6 to 10	247	24%
More than 10	385	38%
Total	1,011	100%

D3. Does you organization have direct operations, sales presence or direct suppliers in any of the following countries? Please check all that apply.	Freq	Pct%
China (PRC)	280	28%
Russian Federation	250	25%
North Korea	11	1%
Middle East (excluding Israel), South East Asia and/or India	263	26%
Africa	225	22%
None of the above	305	30%
Total	1,334	

D4. What range best describes the full-time headcount of your global organization?	Freq	Pct%
Less than 1,000	210	21%
1,000 than 5,000	230	23%
5,001 to 10,000	190	19%
10,001 to 25,000	190	19%
25,001 to 75,000	128	13%
More than 75,000	63	6%
Total	1,011	100%

D5. What best describes your organization's primary industry classification?	Freq	Pct%
Financial services	143	14%
Public sector	110	11%
Healthcare	96	9%
Retail	88	9%
Hi tech	80	8%
Industrial	66	7%
Consumer products	63	6%
Energy & utilities	48	5%
Communications	46	5%
Legal services	33	3%
Transportation	33	3%
Accounting services	28	3%
Other services	27	3%
Entertainment & media	26	3%
Hospitality	26	3%
Life sciences	33	3%
Education & research	18	2%
Agriculture & food services	15	1%
Defense & aerospace	21	2%
Other	11	1%
Total	1,011	100%

Q1a. Our organization has a clear policy for the adoption and use of cloud-based file sharing/file sync-and-share applications.	Freq	Pct%
Strongly agree	170	17%
Agree	352	35%
Unsure	194	19%
Disagree	196	19%
Strongly disagree	99	10%
Total	1,011	100%

Q1b. Our organization has clear visibility into what file sharing/file sync and share applications are being used by employees at work.	Freq	Pct%
Strongly agree	162	16%
Agree	349	35%
Unsure	197	19%
Disagree	201	20%
Strongly disagree	102	10%
Total	1,011	100%

Q1c. Our organization has the ability to manage and control user access to sensitive documents and how they are shared.	Freq	Pct%
Strongly agree	168	17%
Agree	342	34%
Unsure	193	19%
Disagree	201	20%
Strongly disagree	107	11%
Total	1,011	100%

Q1d. Our organization educates individuals annually on the risks of data loss and data theft.	Freq	Pct%
Strongly agree	117	12%
Agree	340	34%
Unsure	316	31%
Disagree	181	18%
Strongly disagree	57	6%
Total	1,011	100%

Q2. Please estimate the percentage of employees in your organization who regularly share files outside the company/beyond the firewall?	Freq	Pct%
Less than 10%	84	8%
10 to 25%	175	17%
26 to 50%	258	26%
51 to 75%	166	16%
More than 75%	162	16%
Cannot determine	166	16%
Total	1,011	100%

How do employees share files and documents? Please rate the employee's usage level for the following six technologies using the scale provided below each item.		
Q3a. Unencrypted email	Freq	Pct%
Very heavy	118	12%
Heavy	246	24%
Moderate	252	25%
Light	276	27%
None	119	12%
Total	1,011	100%

Q3b. Encrypted email	Freq	Pct%
Very heavy	138	14%
Heavy	243	24%
Moderate	233	23%
Light	268	27%
None	129	13%
Total	1,011	100%

Q3c. File Transfer Protocol (FTP)	Freq	Pct%
Very heavy	126	12%
Heavy	265	26%
Moderate	250	25%
Light	244	24%
None	126	12%
Total	1,011	100%

Q3d. Cloud-based, commercial file sharing/file sync-and-share tool	Freq	Pct%
Very heavy	103	10%
Heavy	255	25%
Moderate	253	25%
Light	259	26%
None	141	14%
Total	1,011	100%

Q3e. On-premise, commercial file sharing/file sync-and-share tool	Freq	Pct%
Very heavy	124	12%
Heavy	279	28%
Moderate	234	23%
Light	228	23%
None	146	14%
Total	1,011	100%

Q3f. On-premise, home grown file sharing tool	Freq	Pct%
Very heavy	125	12%
Heavy	240	24%
Moderate	261	26%
Light	261	26%
None	124	12%
Total	1,011	100%

Q4. Please rank the following list of file sharing technologies based on their level of information security risk to your organization. Let 1 = highest risk to 6 = lowest risk.	Average	Rank
Unencrypted email	2.49	2
Encrypted email	3.50	4
File Transfer Protocol (FTP)	3.48	3
Cloud file sharing/file sync-and-share tool	2.45	1
On-premise, commercial file sharing/file sync-and-share tool	4.46	5
On-premise, home grown file sharing tool	4.50	6
Total	3.48	

Q5. What percent of your organization's employees are part of the mobile workforce?	Freq	Pct%
Less than 10%	139	14%
10 to 25%	235	23%
26 to 50%	245	24%
More than 50%	258	26%
Cannot determine	134	13%
Total	1,011	100%

Q6. Does your organization permit the use of the following mobile devices for file sharing or document collaboration? Please select all that apply.	Freq	Pct%
Mobile devices provided to the employee by the organization	594	59%
Employee's personally owned mobile devices (BYOD)	384	38%
Personal cloud storage applications (BYOC)	368	36%
Mobile devices equipped with a remote wipe/delete option	351	35%
Mobile devices equipped with Mobile Device Management (MDM) technology	358	35%
None of the above are permitted	65	6%
Total	2,120	

Q7. What percent of your organization's documents containing sensitive or confidential information is exchanged with third parties?	Freq	Pct%
Less than 10%	92	9%
11 to 25%	252	25%
26 to 50%	334	33%
More than 50%	174	17%
Cannot determine	159	16%
Total	1,011	100%

Q8. What types of documents are usually restricted from sharing with third parties?	Freq	Pct%
Employee records	615	61%
Contracts	206	20%
Legal documents/NDA files	688	68%
Customer information	525	52%
Research & development data	685	68%
Payment records	549	54%
Source code	566	56%
Financial information	654	65%
Marketing and sales information	679	67%
Total	5,167	

Q9. What best describes the level of involvement of your organization's IT department in the adoption of new technologies such as cloud, mobile platforms, big data analytics and so forth?	Freq	Pct%
Very significant	186	18%
Significant	369	36%
Not significant	340	34%
Minimal	116	11%
Total	1,011	100%

Q10. What percent of applications are used by various business functions without the IT department's approval or knowledge (for instance, cloud computing services or mobile apps)?	Freq	Pct%
Less than 10%	136	13%
10 to 25%	292	29%
26 to 50%	284	28%
More than 50%	186	18%
Cannot determine	113	11%
Total	1011	100%

Have the following incidents happened over the past 12 months by you?		
Q11a. Received files and documents not intended for me.	Freq	Pct%
Never	190	19%
Rarely	213	21%
Often	377	37%
Frequently	231	23%
Total	1,011	100%

Q11b. Did not delete confidential documents or files as required by policies.	Freq	Pct%
Never	187	18%
Rarely	211	21%
Often	363	36%
Frequently	250	25%
Total	1,011	100%

Q11c. Accidently forwarded files or documents to individuals not authorized to receive them.	Freq	Pct%
Never	175	17%
Rarely	212	21%
Often	378	37%
Frequently	246	24%
Total	1,011	100%

Q11d. Accidently sent files or documents to unauthorized individuals outside the organization.	Freq	Pct%
Never	174	17%
Rarely	210	21%
Often	388	38%
Frequently	239	24%
Total	1,011	100%

Q11e. Used my personal file-sharing/file sync-and-share apps in the workplace.	Freq	Pct%
Never	180	18%
Rarely	212	21%
Often	376	37%
Frequently	243	24%
Total	1,011	100%

Q12. Are you using any of the following file sharing software products at work? Please select all that apply.	Freq	Pct%
Amazon	151	15%
Box	542	54%
Dropbox	601	59%
Google Drive	495	49%
Intralinks	169	17%
Sharedox	84	8%
ShareFile	147	15%
Watchdox	162	16%
Accelion	131	13%
HighTail	89	9%
SharePoint/Microsoft	531	53%
None	28	3%
Total	3,130	

Q13. Are "free" cloud storage and file sharing applications used by employees within your organization?	Freq	Pct%
Most likely	165	16%
Likely	343	34%
Not likely	174	17%
No	157	16%
Do not know	172	17%
Total	1,011	100%

Overall, when you think about the safety and risks of file sharing, how would you rate the following?		
Q14a. Your organization's file sharing process, procedures and technologies	Freq	Pct%
1 and 2 (not safe)	106	10%
3 and 4	232	23%
5 and 6	295	29%
7 and 8	277	27%
9 and 10 (very safe)	101	10%
Total	1,011	100%

Q14b. Your industry's overall approach to file sharing among peer organizations	Freq	Pct%
1 and 2 (not safe)	114	11%
3 and 4	232	23%
5 and 6	292	29%
7 and 8	271	27%
9 and 10 (very safe)	102	10%
Total	1,011	100%

Q14c. Your personal approach to file sharing	Freq	Pct%
1 and 2 (not safe)	101	10%
3 and 4	212	21%
5 and 6	303	30%
7 and 8	267	26%
9 and 10 (very safe)	128	13%
Total	1,011	100%

Q14d. Your employees'/colleagues' approach to file sharing	Freq	Pct%
1 and 2 (not safe)	121	12%
3 and 4	220	22%
5 and 6	313	31%
7 and 8	238	24%
9 and 10 (very safe)	119	12%
Total	1,011	100%

Part 3. File sharing policies, governance and control practices

Q15. Over the past 24 months, did your organization experience a data breach caused by the following incidents? Please check all that apply.	Freq	Pct%
Lost or stolen device	303	30%
Employee mishap while file sharing	53	5%
Other employee mistakes	151	15%
Third party mishap	281	28%
System glitches	143	14%
Malicious or criminal insider	94	9%
External cyber attack	103	10%
Do not know	135	13%
None	235	23%
Total	1,498	

Q16. Who within your organization has ultimate authority and responsibility for securing document collaboration and file sharing activities?	Freq	Pct%
Chief information security officer	170	17%
Chief security officer	74	7%
Chief information officer	289	29%
Chief privacy officer	5	0%
General counsel	23	2%
Business unit or LOB management	234	23%
No one has ultimate authority	216	21%
Total	1,011	100%

Q17. How does your organization determine document and file-level confidentiality? Please select all that apply.	Freq	Pct%
By policies	530	52%
By data type	610	60%
By data usage	336	33%
By technology usage	233	23%
By document owner	337	33%
By who has access to the document	424	42%
By content management system	486	48%
We do not determine document and file-level confidentiality	59	6%
Total	3,015	

Q18. How would you rate your organization's effectiveness in determining the appropriate confidentiality of documents and files? Please use the following 10-point scale from 1 = not effective to 10 = very effective.	Freq	Pct%
1 and 2 (not effective)	50	5%
3 and 4	177	18%
5 and 6	464	46%
7 and 8	270	27%
9 and 10 (very effective)	50	5%
Total	1,011	100%

Q19. In the past 12 months, did your organization conduct audits or assessments to determine if document and file sharing activities are in compliance with laws and regulations?	Freq	Pct%
Yes	303	30%
No	649	64%
Unsure	59	6%
Total	1,011	100%

Q20. How would you rate your organization's effectiveness in setting permissions to access sensitive or confidential documents and files? Please use the following 10-point scale from 1 = not effective to 10 = very effective.	Freq	Pct%
1 and 2 (not effective)	51	5%
3 and 4	177	18%
5 and 6	493	49%
7 and 8	248	25%
9 and 10 (very effective)	42	4%
Total	1,011	100%

Q21. How would you rate your organization's effectiveness in stopping the use of unapproved file sharing tools? Please use the following 10-point scale from 1 = not effective to 10 = very effective.	Freq	Pct%
1 and 2 (not effective)	52	5%
3 and 4	200	20%
5 and 6	467	46%
7 and 8	247	24%
9 and 10 (very effective)	45	4%
Total	1,011	100%

Q22. How effective is your organization in stopping the misuse of file sharing tools? Please use the following 10-point scale from 1 = not effective to 10 = very effective.	Freq	Pct%
1 and 2 (not effective)	56	6%
3 and 4	197	19%
5 and 6	454	45%
7 and 8	261	26%
9 and 10 (very effective)	43	4%
Total	1,011	100%

Q23. Does your organization use any of following technologies in the file-sharing environment? Please select all that apply.	Freq	Pct%
Mobile device management (MDM) to lock-down mobile devices or laptops and remotely erase them	270	27%
Ability to obtain data location when using cloud services	239	24%
Ability to manage encryption keys (customer-managed encryption keys) on cloud-based services so only the data owner can provision access to unencrypted files	293	29%
Encryption or tokenization for documents and files at rest	363	36%
Data loss prevention tools (DLP)	355	35%
Digital rights management (DRM) or information rights management (IRM) tools	378	37%
Identity & access management tools	514	51%
Two-factor authentication	425	42%
Hybrid on-premise/cloud storage to manage data location and data privacy	393	39%
Housing data in a specific location or jurisdiction to meet data privacy regulations	308	30%
Network monitoring tools to control what cloud applications are used	429	42%
White listing and/or black listing tools	634	63%
Other	66	7%
Total	4,667	

Q24. Is your organization compliant with ISO 27001 (the international standard for process-based security)?	Freq	Pct%
We are fully certified and compliant today	89	9%
We are in process of becoming certified	151	15%
We follow some of the processes and procedures	324	32%
We are not compliant	271	27%
Do not know	176	17%
Total	1,011	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.