# Secure File Sharing & Content Collaboration for Users, IT & IT Security

## Sponsored by Axway Syncplicity

Independently conducted by Ponemon Institute LLC

Publication Date: November 2018

**Secure File Sharing & Content Collaboration for Users, IT & IT Security**
Presented by Ponemon Institute, November 2018

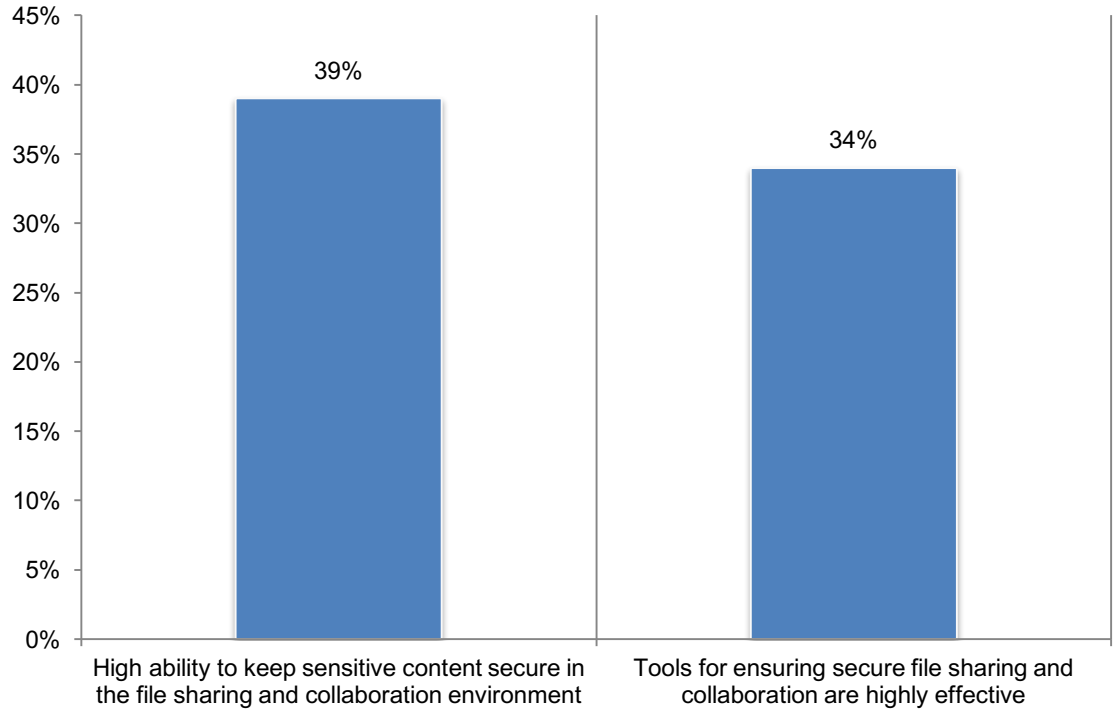
## Part 1. Introduction

The ability to securely and easily share files and content in the workplace is essential to employees' productivity, compliance with the EU's General Data Protection Regulation (GDPR) and digital transformation. However, a lack of visibility into how users are accessing sensitive data and the file applications they are using is putting organizations at risk for a data breach. In fact, 63 percent of participants in this research believe it is likely that their companies had a data breach in the past two years because of insecure file sharing and content collaboration.

According to the findings, an average of 44 percent of employees in organizations use file sharing and collaboration solutions to store, edit or share content in the normal course of business. As a result of this extensive use, most respondents (72 percent) say that it is very important to ensure that the sensitive information in these solutions is secure.

Despite their awareness of the risks, only 39 percent of respondents rate their ability to keep sensitive contents secure in the file sharing and collaboration environment as very high, as shown in Figure 1. Only 34 percent of respondents rate the tools used to support the safe use of sensitive information assets in the file sharing and collaboration environment as very effective.

**Figure 1. The ability to keep sensitive content secure with current solutions**
7+ responses on a scale of 1 = no ability to 10 = high ability
7+ responses on a scale of 1 =low effectiveness to 10 = high effectiveness.



## Part 2. Key findings

Sponsored by Axway Syncplicity, the purpose of this research is to understand file sharing and content collaboration practices in organizations and what practices should be taken to secure the data without impeding the flow of information. Ponemon Institute surveyed 1,371 IT and IT security practitioners in North America, United Kingdom, Germany and France. All respondents are familiar with content collaboration solutions and tools. Further, their job function involves the management, production and protection of content stored in files.

This section presents an analysis of the key findings. The complete audited findings are presented in the Appendix of this report. Following are key themes in this research.

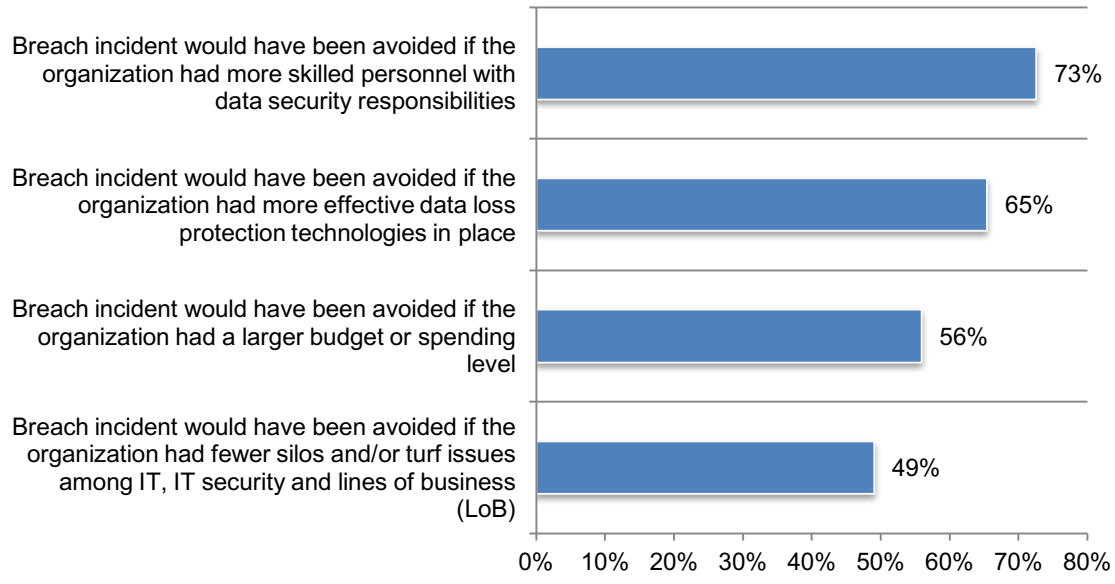
- Risks in the file sharing and collaboration environment
- Governance practices and technologies used to secure sensitive data
- Features that improve the file sharing and collaboration environment
- Conclusion: Achieving secure file sharing & content collaboration

### Risks in the file sharing and content collaboration environment

**Data breaches in the file sharing and content collaboration environment are likely.** Sixty-three percent of respondents say it was likely that their organizations experienced the loss or theft of sensitive information in the file sharing and collaboration environment in the past two years.

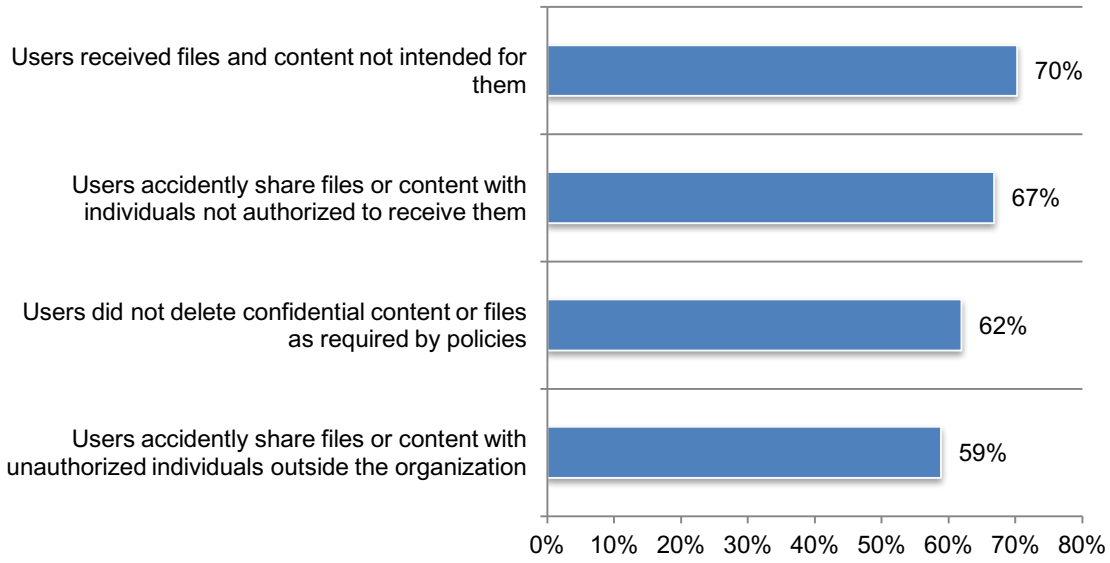
As shown in Figure 2, the best ways to avoid a data breach is to have skilled personnel with data security responsibilities (73 percent of respondents), more effective data loss protection technologies in place (65 percent of respondents), more budget (56 percent of respondents) and fewer silos and/or turf issues among IT, IT security and lines of business (49 percent of respondents).

**Figure 2. Factors most likely to reduce a data breach**
Very likely and Likely responses combined



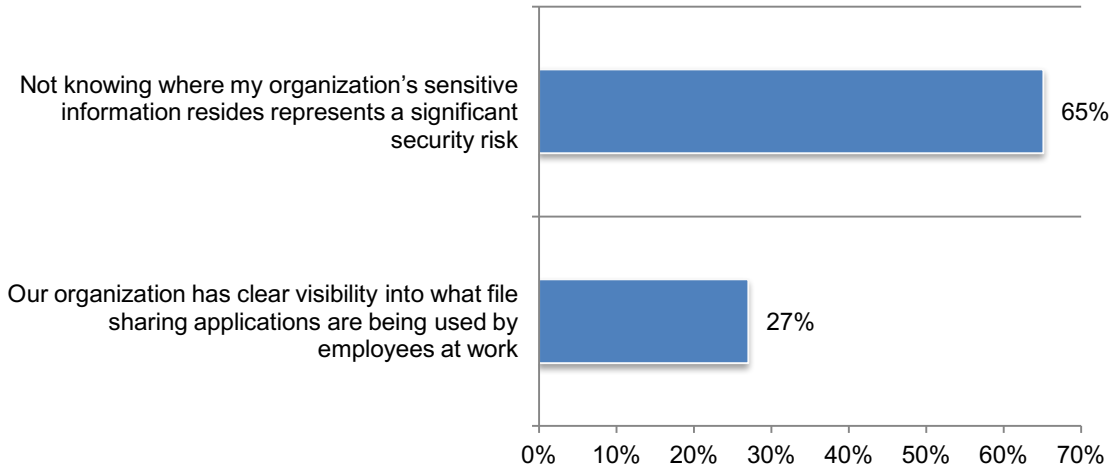
**Data breaches are likely because of risky user behavior.** As shown in Figure 3, 70 percent of respondents say they have received files and content not intended for them. Other risky events include: accidently sharing files or contents with individuals not authorized to receive them, not deleting confidential contents or files as required by policies and accidently sharing files or content with unauthorized individuals outside the organization, according to 67 percent, 62 percent and 59 percent of respondents, respectively.

**Figure 3. How frequently do risky events happen?**
Very frequently and Frequently responses combined



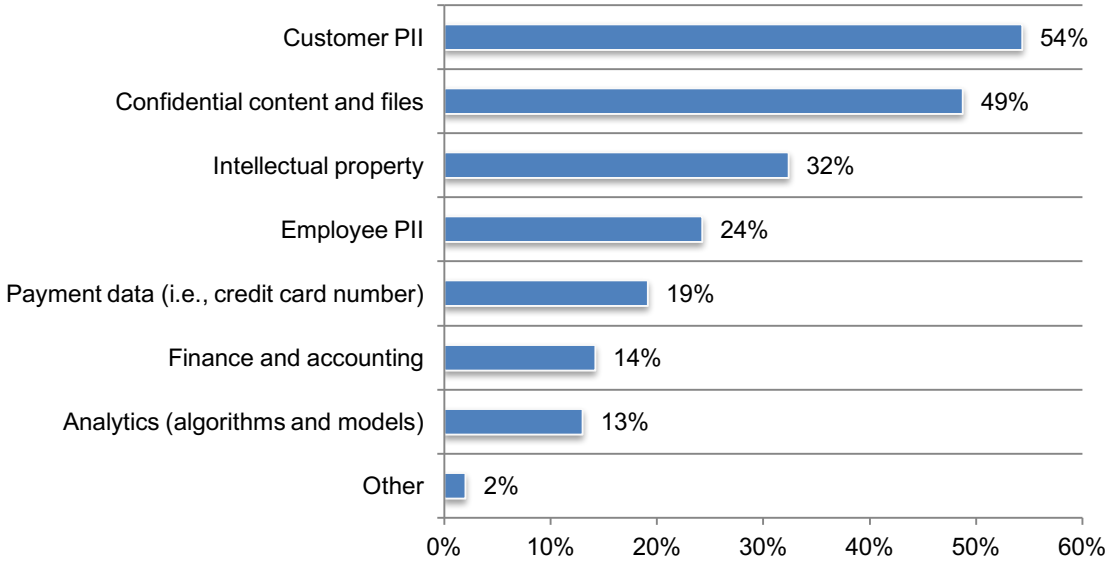

**A lack of visibility into users' access puts sensitive information at risk**. Only 31 percent of respondents are confident in having visibility into users' access and file sharing applications. As shown in Figure 4, 65 percent of respondents recognize that not knowing where sensitive data is a significant security risk. Only 27 percent of respondents say their organization has clear visibility into what file sharing applications are being used by employees at work. A consequence of not having visibility is the inability for IT leadership to know if lines of business are using file sharing applications without informing them (i.e. shadow IT).

**Figure 4. Risks in the file sharing and collaboration environment**
Strongly agree and Agree responses combined



**Customer PII and confidential contents and files are the types of sensitive information at risk.** According to Figure 5, the most sensitive types of data shared with colleagues and third parties is customer PII and confidential documents and files. Hence, these need to be most protected in the file sharing and collaboration environment.

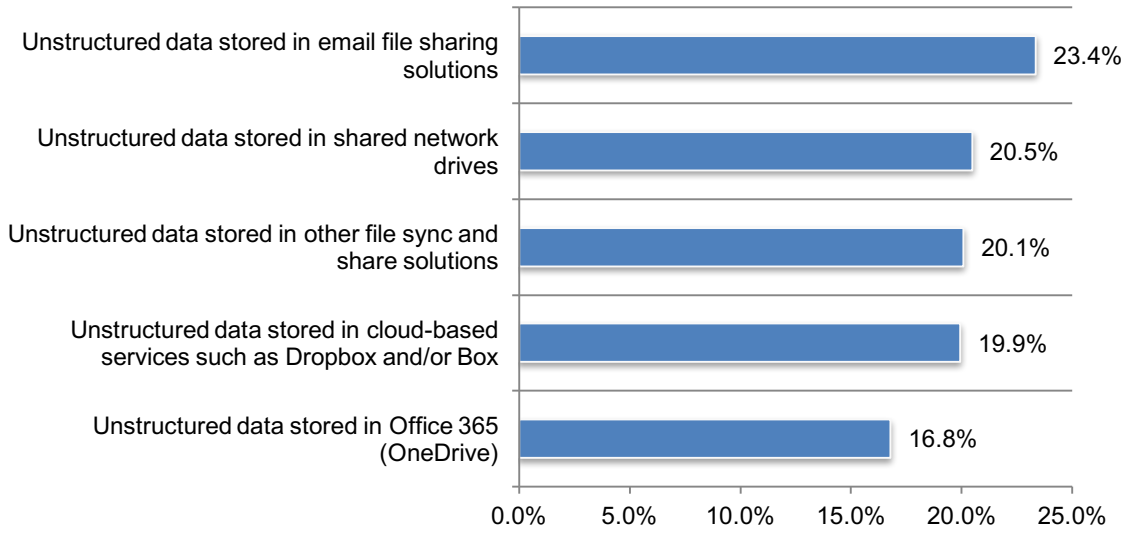
**Figure 5. The types of sensitive information most at risk in your organization**
Two responses permitted



**The plethora of unstructured data makes managing the threats to sensitive information difficult.** As defined in the research, unstructured data is information that either does not have a pre-defined data model or is not organized in a pre-defined manner. Unstructured information is typically text-heavy, but may contain data such as dates, numbers, and facts as well. An average of 53 percent of organizations' sensitive data is unstructured and organizations have an average of almost 3 petabytes of unstructured data.

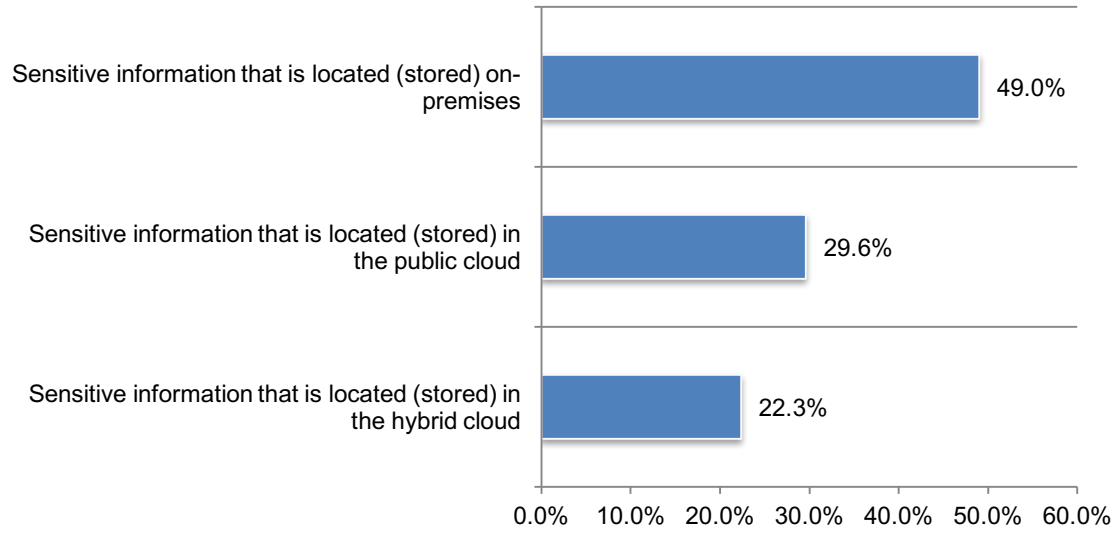
As shown in Figure 6, most unstructured data is stored in email file sharing solutions. Respondents estimate an average of 20.5 percent is stored in shared network drives and 20 percent is stored in other file sync and share solutions. Almost half (49 percent of respondents) are concerned about storing unstructured data in the cloud. As shown below, only about 20 percent of unstructured data is stored in cloud-based services such as Dropbox or Box (20 percent) and Office 365 (17 percent).

**Figure 6. How much unstructured data exists in various locations?**
Extrapolated values



**On average, almost half of an organization's sensitive data is stored on-premises**. According to Figure 7, an average of almost half (49 percent) of organizations' sensitive information is stored on-premises and approximately 30 percent is located in the public cloud. An average of 22 percent of sensitive information is stored in the hybrid cloud. Hybrid cloud is a cloud computing environment that uses a mix of on-premises, private cloud and third-party, public cloud services with orchestration between the two platforms.

**Figure 7. Where sensitive information is stored or located**
Extrapolated values

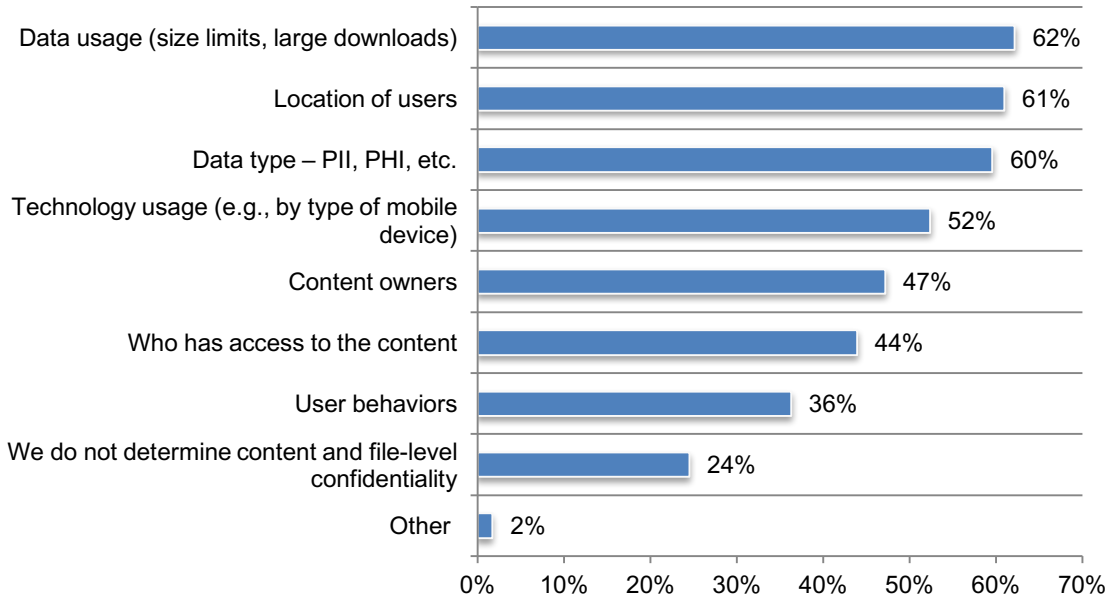


**Governance practices and technologies used to secure sensitive contents**

**Companies are challenged to keep sensitive content secure in the file sharing and collaboration environment.** As mentioned earlier in the report, respondents are aware of the threats to their sensitive information, but admit their governance practices and technologies should be more effective. According to respondents, on average, about one-third of the data in the file sharing and collaboration environment is considered sensitive.

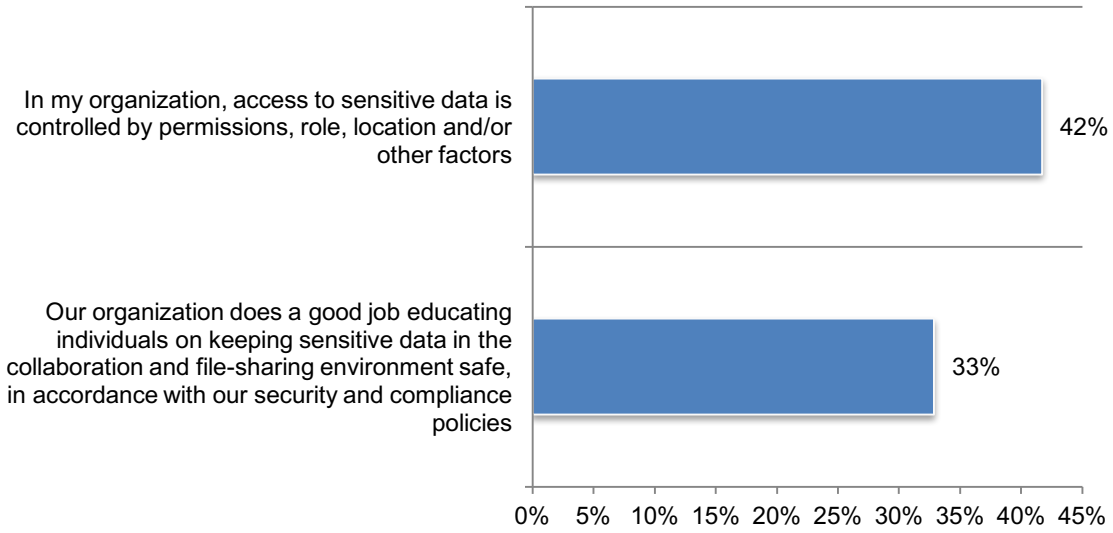
To classify the level of security that is needed, respondents say it is mostly determined by data usage, location of users and sensitivity of data type (62 percent, 61 percent and 60 percent, respectively), as shown in Figure 8. Twenty-four percent of respondents say their companies do not determine content and file-level confidentiality.

**Figure 8. How is file-level confidentiality determined in the file sharing and collaboration environment?**
More than one response permitted



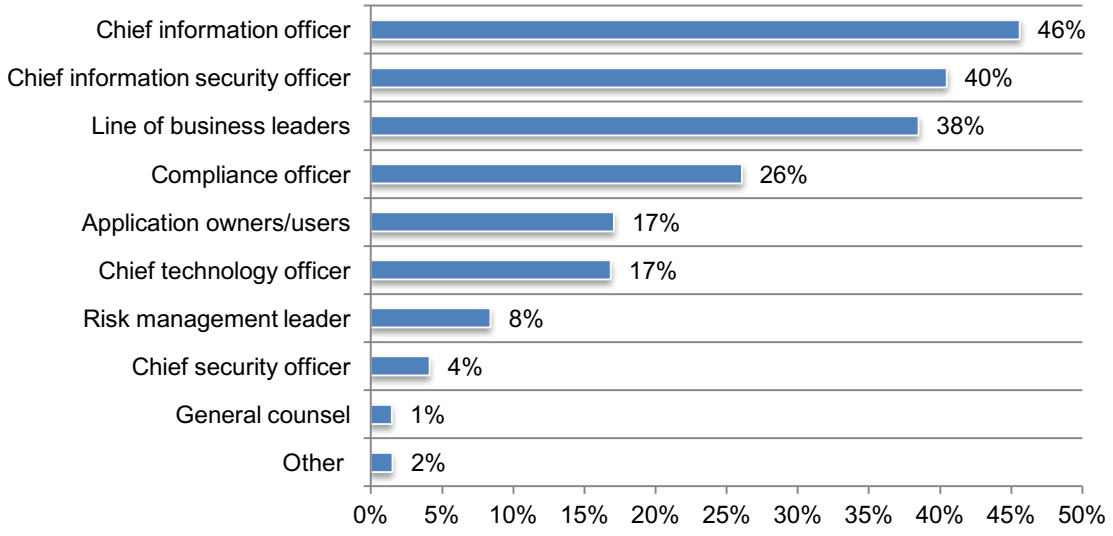
**Controlling access and training users is critical to safeguarding sensitive information.** According to Figure 9, only 42 percent of respondents say their organizations have practices in place to control access to sensitive data by permissions, role, location and/or other factors. Despite the risky user behavior discussed previously, only 33 percent of respondents say their organization does a good job educating individuals to follow their security and compliance policies with respect to content collaboration and file sharing.

**Figure 9. Practices taken to safeguard sensitive data**
Strongly agree and Agree responses combined



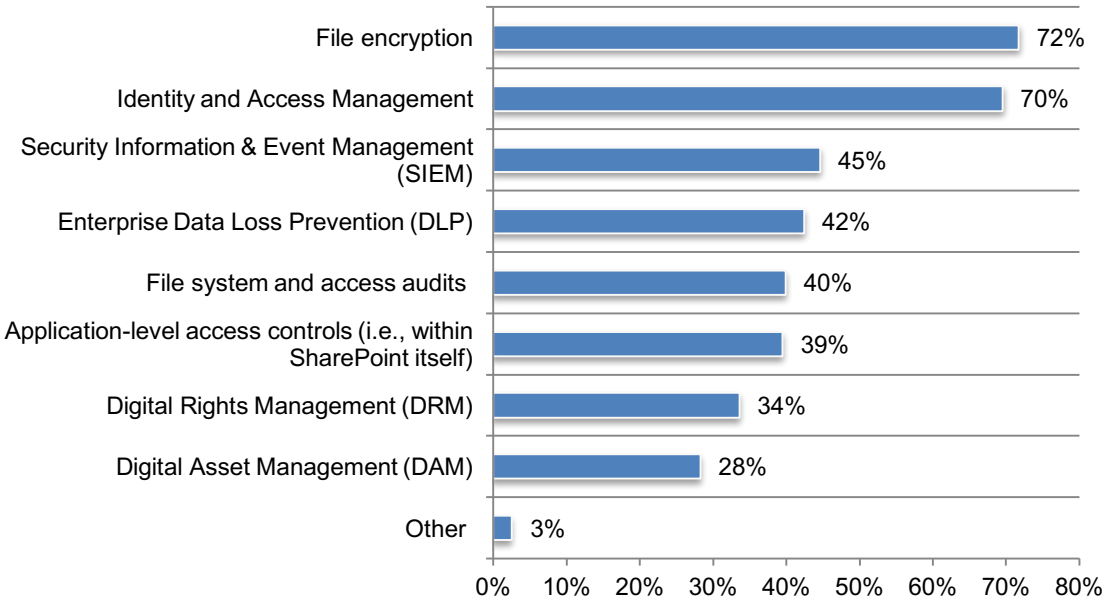

**Responsibility for file sharing and content collaboration security is dispersed throughout the organization.** As shown in Figure 10, there is not one function that has ultimate responsibility for the file sharing and content collaboration security. Those most accountable in the organizations represented in this study are the chief information officer, chief information security officer and lines of business.

**Figure 10. Who has ultimate responsibility for file sharing and content collaboration security?**
Two responses permitted



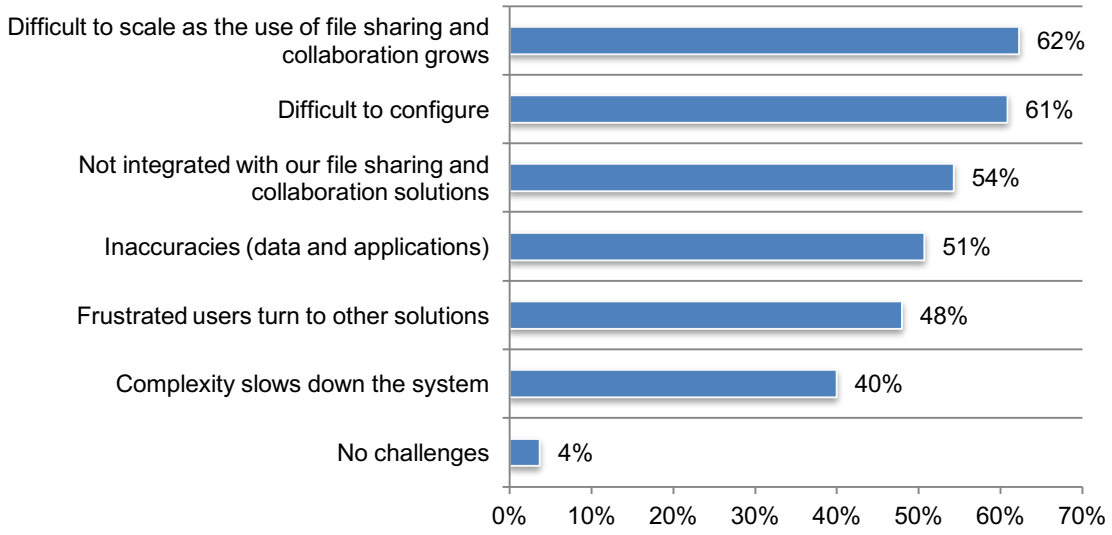
**File encryption and identity and access management are most often used to safeguard sensitive information.** Figure 11 presents the technologies most often used to safeguard sensitive information are file encryption (72 percent of respondents), identity and access management (70 percent of respondents), SIEM (45 percent of respondents) and enterprise data loss prevention (42 percent of respondents).

**Figure 11. What technologies or tools does your organization use to support the safe use of file sharing and content collaboration?**
More than one response permitted



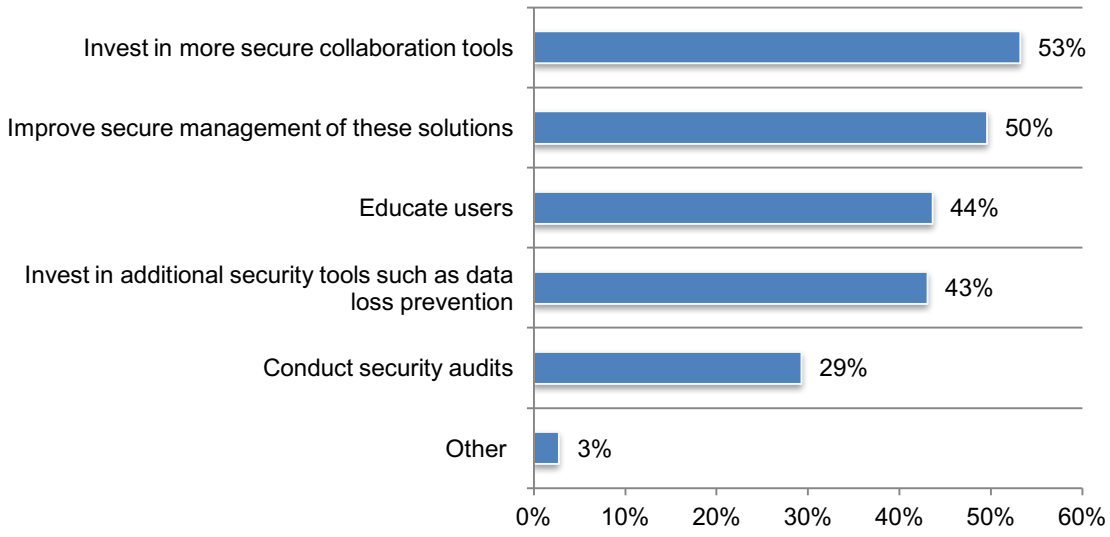
**Tools to safeguard sensitive information are often difficult to scale and configure.** As discussed only 34 percent of respondents say the tools used to support the safe use of sensitive information assets in the file sharing and collaboration environment are highly effective. According to Figure 12, 62 percent of respondents say the tools are difficult to scale as the use of file sharing and collaboration grows and 61 percent of respondents say they are difficult to configure. Integration with file sharing and collaboration solutions is a challenge when relying on tools to safeguard sensitive information assets.

**Figure 12. The challenges when relying on tools to safeguard sensitive information assets in the file sharing and collaboration environment?**
More than one response permitted



**Organizations are expected to invest in more secure collaboration tools.** According to Figure 13, 53 percent of respondents say their organizations will purchase more secure collaboration tools and half (50 percent of respondents) say their organization will improve secure management of these solutions. However, despite users' careless and risky behavior only 44 percent of respondents say their organizations will provide employee training and education programs.

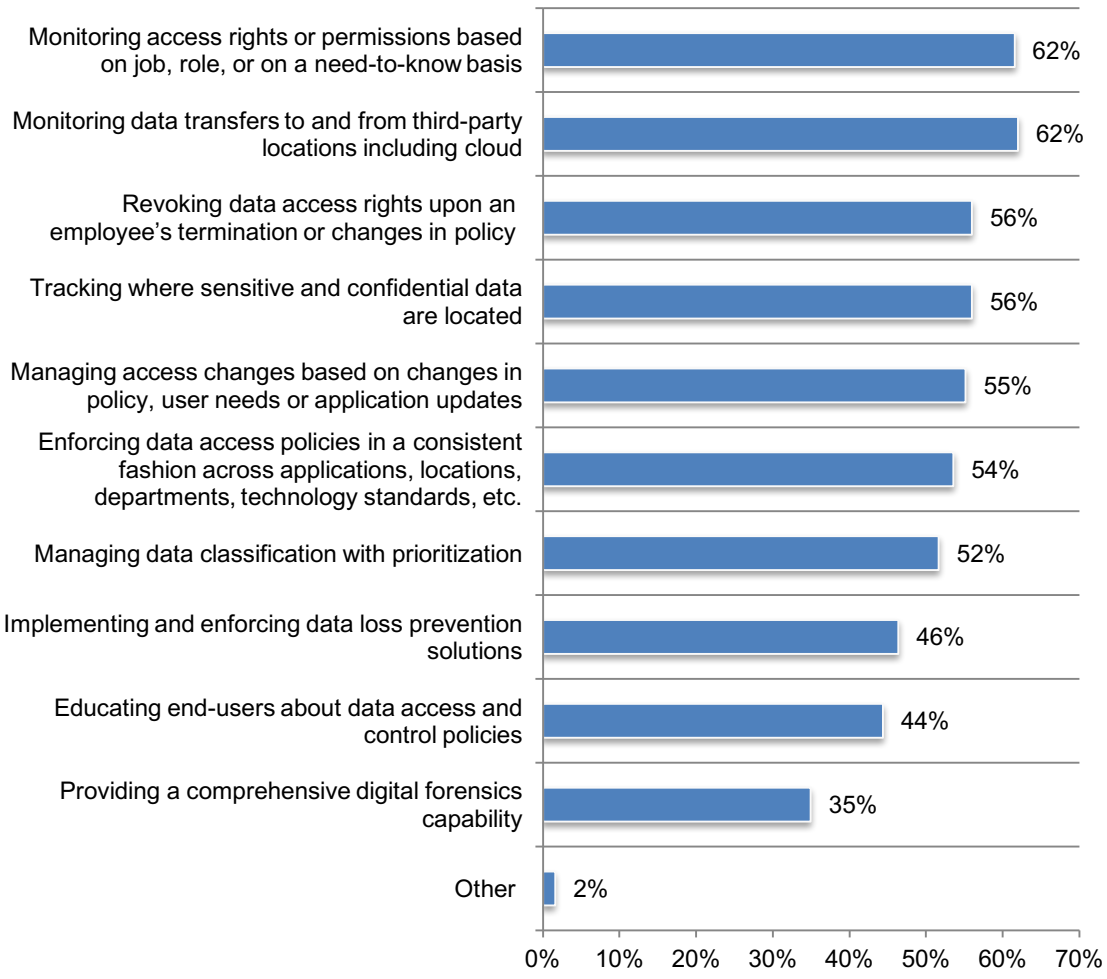
**Figure 13. Actions to be taken to protect sensitive information in the file sharing and collaboration environment**
More than one response permitted



**Governance practices are not effective in supporting a secure file sharing and content collaboration environment.** As shown in Figure 14, the majority of companies are using governance practices that should support a secure file sharing and content collaboration environment. However, as discussed previously, only 39 percent of respondents say their organizations have a high ability to keep sensitive contents secure when users are sharing files and content. This indicates that while practices may be in place, they are not accomplishing the objective of safeguarding sensitive information assets.

The top five governance practices used by organizations to protect information assets include: monitoring access rights or permissions based on job, role or on a need-to-know basis (62 percent of respondents), monitoring data transfers to and from third-party locations including the cloud (62 percent of respondents), revoking data access rights upon an employee's termination or changes in policy (56 percent of respondents), tracking where sensitive and confidential data are located (56 percent of respondents) and managing access changes based on changes in policy, user needs or application updates (55 percent of respondents). Once again, educating users about data access and control policies is at the bottom of the list with only 44 percent of respondents saying that their organizations have such a program.

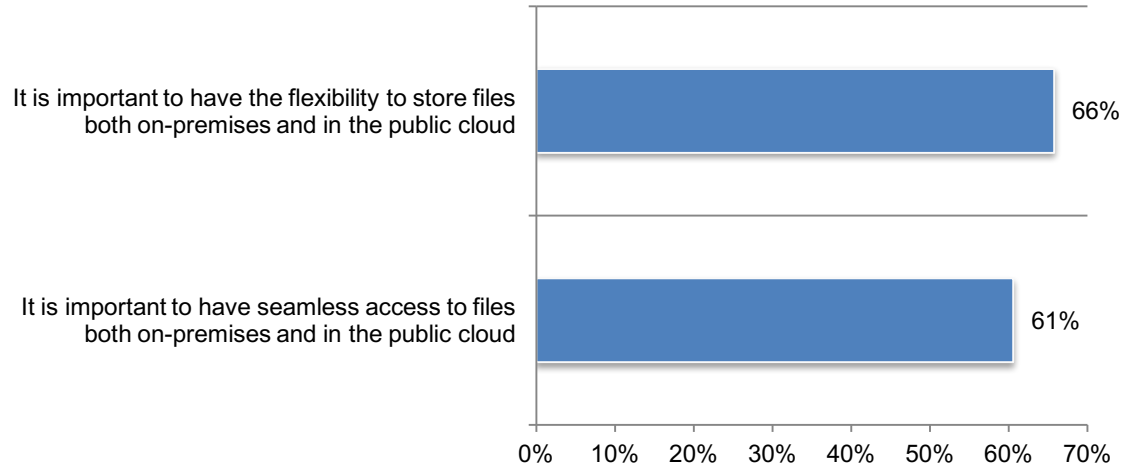
**Figure 14. Data governance tasks used to protect information assets**
More than one response permitted



**Features that improve the file sharing and collaboration environment**

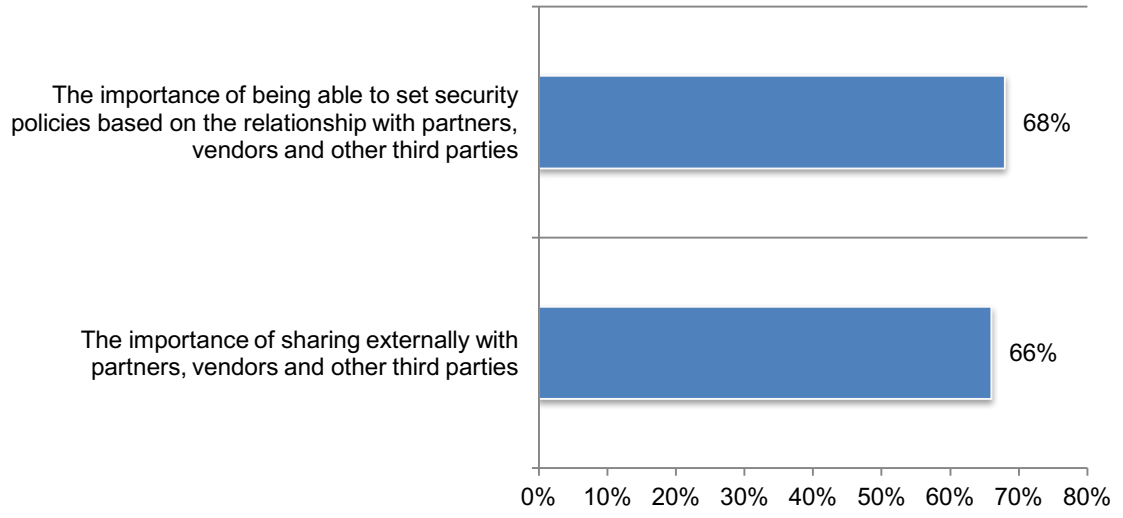
**Flexibility and seamless access are important when sharing files in the cloud**. More than half of respondents (49 percent) say their organizations are concerned about storing all of its unstructured data in the public cloud. According to Figure 15, 66 percent of respondents believe it is important to have the flexibility to store files both on-premises and in the public cloud and 61 percent say it is important to have seamless access to files both on-premises and in the public cloud.

**Figure 15. File sharing and collaboration in the cloud**
Strongly agree and Agree responses combined




**The ability to share files with third parties securely is critical**. On average, 42 percent of an organization's sensitive information is shared with third parties. Sixty-six percent of respondents say sharing information with partners, vendors and other third parties is very important, but it must be secure. To prevent a possible third-party data breach, 68 percent of respondents say their organizations should be able to set security policies based on their relationship with partners, vendors and other third parties, as shown in Figure 16.

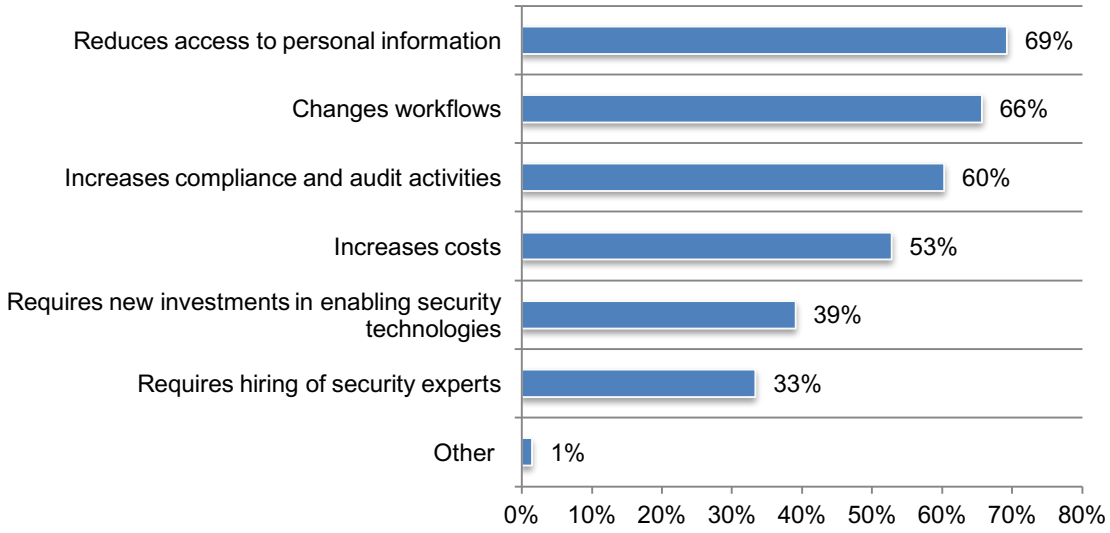
**Figure 16. File sharing and collaboration with third parties**
7+ responses on a scale of 1 = not important to 10 = very important



**A flexible security framework for different file sharing and collaboration scenarios is important for GDPR compliance.** Fifty-nine percent of respondents say their organizations are concerned about complying with The EU's General Data Privacy Regulation (GDPR) requirements for personal data in the file sharing and collaboration environment.

Only 29 percent of organizations represented in this study have achieved full compliance with GDPR, which went into effect May 25, 2018. The two biggest impacts of GDPR on file sharing and content collaboration are it reduces access to personal information (69 percent of respondents) and changes workflows (66 percent of respondents).

**Figure 17. How does GDPR affect file sharing and content collaboration**
More than one response permitted

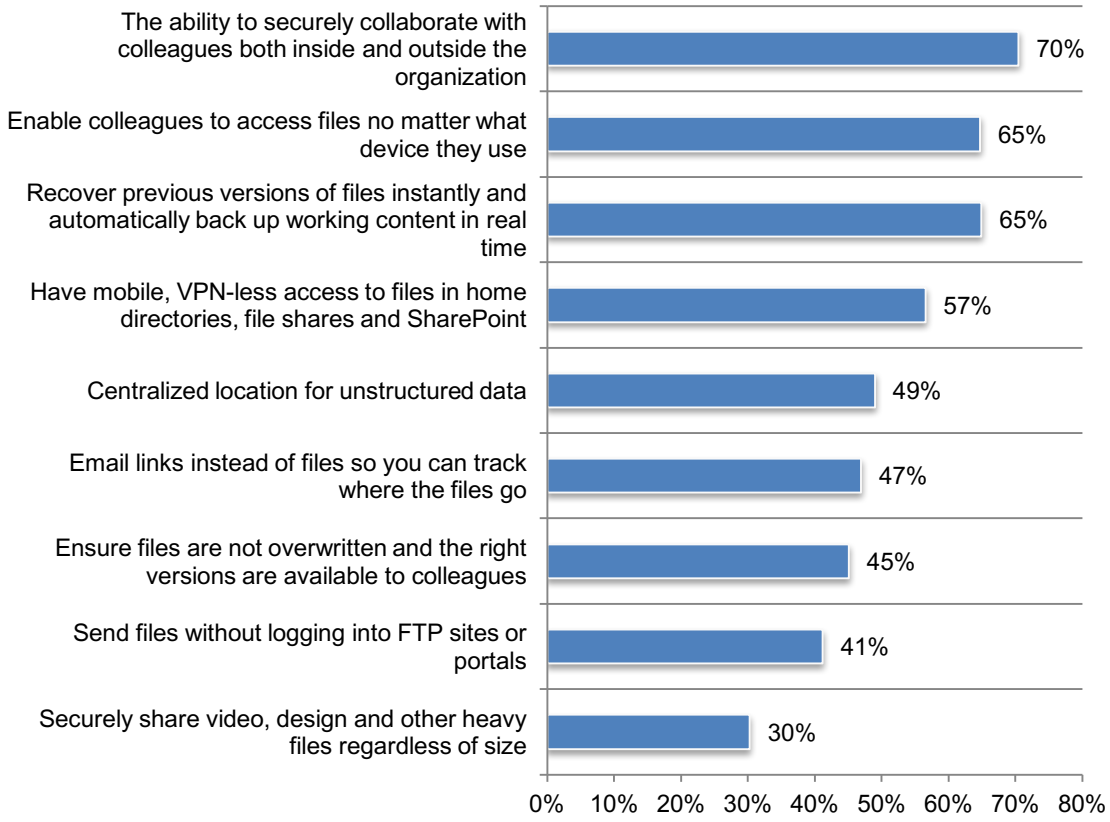


**Security of file sharing and collaboration both inside and outside the organization is the most important capability for a solution**. Figure 18 presents nine features of a solution and their importance to respondents. The most important feature that would improve the security and productivity of end users is the ability to securely collaborate with colleagues both inside and outside the organization (70 percent of respondents).

Other important features are those that enable colleagues to access files no matter what device they use (65 percent of respondents), recover previous versions of files instantly and automatically back up contents in real time (65 percent of respondents), have mobile, VPN-less access to files in home directories, file shares and SharePoint (57 percent of respondents) and have a centralized location for unstructured data (49 percent of respondents).

Features that are not considered as important are ensuring files are not overwritten and the right versions are available to colleagues (45 percent of respondents), sending files without logging into FTP sites or portals (41 percent of respondents) and ability to securely share video, design and other files regardless of size (30 percent of respondents).

**Figure 18. Features that improve the file sharing and collaboration environment**
Significant improvement and Improvement responses combined

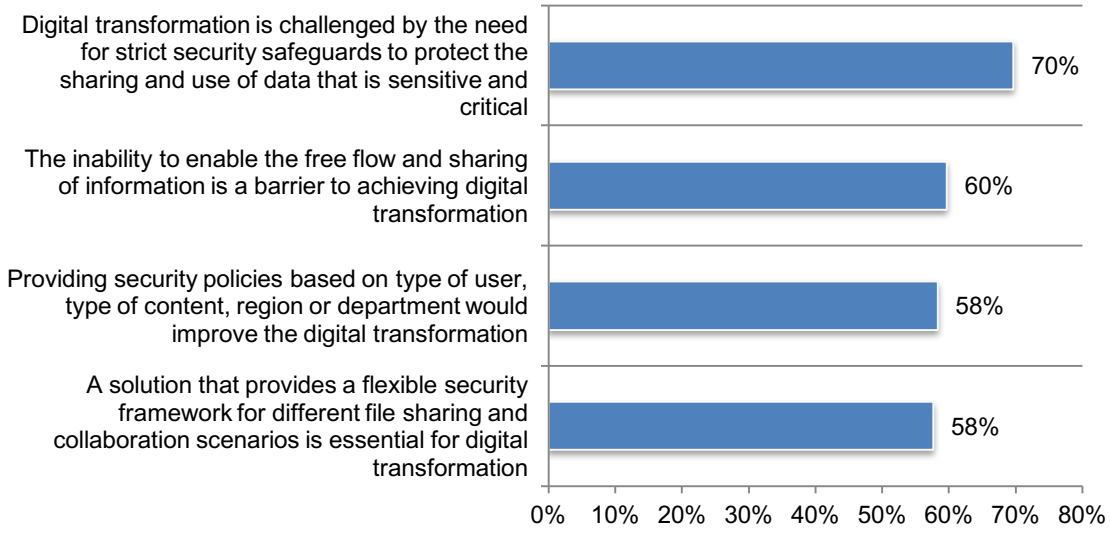


**A secure file sharing and content collaboration environment is important for organizations to achieve a successful digital transformation.** In the context of this research, digital transformation means making decisions based on market demand and business opportunity, empowering consumers and fostering collaboration through innovation (mobile, cloud, IoT) and quickly and effectively releasing new applications to drive growth. From an IT security perspective, it means assessing digital exposure and overall risk to the business, protecting critical assets across the organization (network, endpoints, servers, cloud) and conforming and complying with regulations, industry standards and security best practices.

Figure 19, presents the features considered important for organizations' digital transformation. Seventy percent of respondents say digital transformation is challenged by the need for strict security safeguards to protect the sharing and use of data that is sensitive and critical and 60 percent of respondents say the inability to enable the free flow and sharing of information is a barrier to achieving digital transformation

Fifty-eight percent of respondents say a solution that provides a flexible security framework for different file sharing and collaboration scenarios is essential for digital transformation. In addition, providing security policies based on type of user, type of content, region or department would improve the digital transformation.

**Figure 19. The impact of digital transformation on file sharing and content collaboration**
Strongly agree and Agree responses combined




**Conclusion: Achieving secure file sharing & content collaboration**

An effective file sharing and content collaboration environment is a balance between security and user convenience. Following are recommendations to achieve this objective based on the research findings.

- Establish policies and procedures for all users who are sharing files and collaborating on content. Such policies should be based on the type of user, type of content, region or department and should be strictly enforced.

- Assign one function to be accountable for mitigating the threats to sensitive information in the file sharing and content collaboration environment. Almost half of respondents (49 percent) say the likelihood of a data breach can be avoided if there were fewer silos and/or turf issues among IT, IT security and lines of business.

- Educate users about the importance of being careful when sharing sensitive information with colleagues inside and outside the organization. As revealed in the research, most users are putting sensitive information at risk because of carelessness and mistakes made when sharing files.

- Allocate more resources, both personnel and budget, to managing the risk of insecure file sharing and content collaboration. Sixty-three percent of respondents already believe their organizations had a data breach because current governance practices and technologies are ineffective.

- Compliance with GDPR and a successful digital transformation process is dependent upon the security of the file sharing and content collaboration environment. This is another reason to invest in technologies and in-house expertise.

- Assess the effectiveness of technologies to improve scalability and integration with file sharing and content collaboration tools. The two biggest challenges with current technologies in use is the difficulty in keeping up with more users using file sharing and content collaboration tools and the inability to integrate with these tools.

- Assess the effectiveness of the organization's governance practices. While many organizations represented have governance practices in place, most respondents say their organizations are not doing a good job in safeguarding sensitive information, which indicates that their practices are not effective.

- Invest in technologies that provide visibility into users' practices when accessing sensitive information and where all sensitive information is located on-premises and in the cloud.

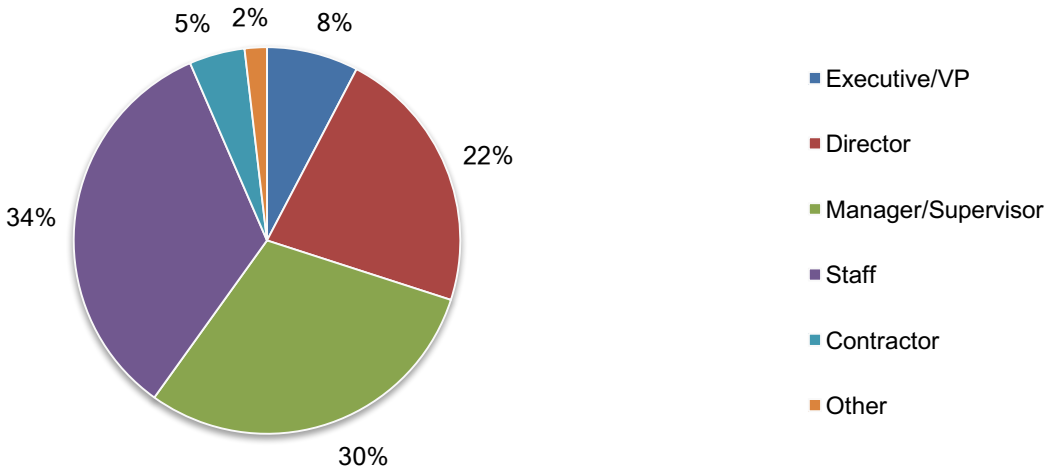
## Part 3. Methods

The sampling frame is composed of 40,111 IT and IT security practitioners in North America, the United Kingdom, Germany and France. As shown in Table 1, 1,592 respondents completed the survey. Screening removed 221 surveys. The final sample was 1,371 surveys (or a 3.4 percent response rate).

| Table 1. Sample response | Freq | Pct% |
|---|---|---|
| Total sampling frame | 40,111 | 100.0% |
| Total returns | 1,592 | 4.0% |
| Rejected or screened surveys | 221 | 0.6% |
| Final sample | 1,371 | 3.4% |

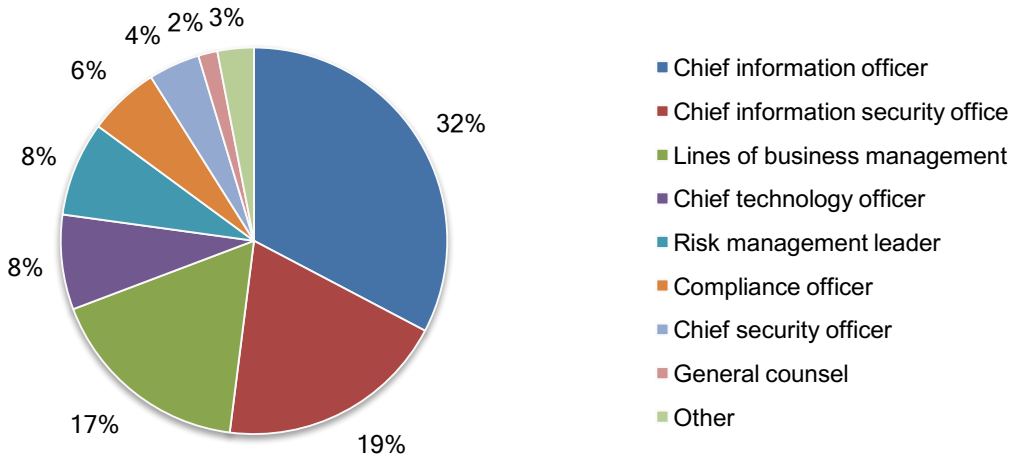
Pie Chart 1 reports the current position or organizational level of the respondents. Sixty percent of respondents reported their current position as supervisory or above.

**Pie Chart 1. Distribution of respondents according to position level**



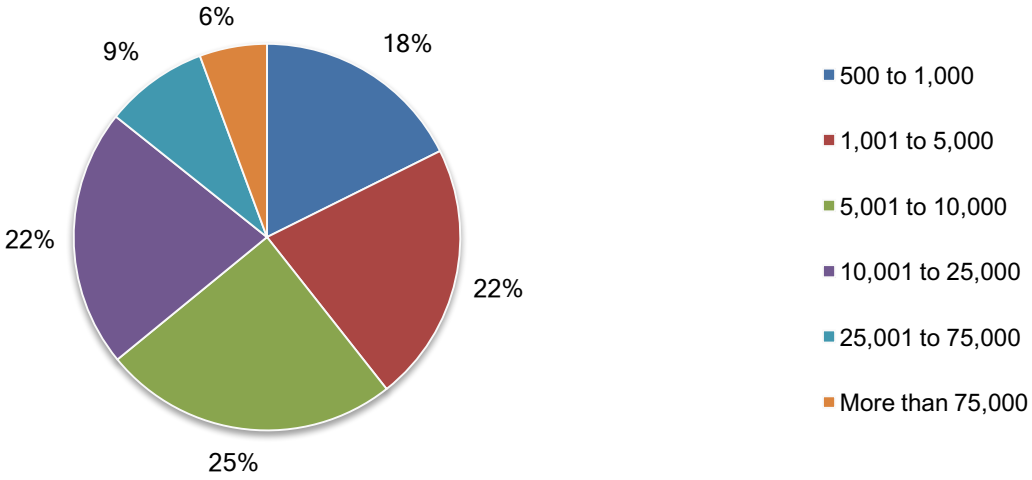
Pie Chart 2 identifies the primary person to whom the respondent or their IT security leader reports. Thirty-two percent of respondents identified the chief information officer as the person to whom they report. Another 19 percent indicated they report directly to the chief information security officer and 17 percent of respondents report to a line of business leader.

**Pie Chart 2. Distribution of respondents according to reporting channel**



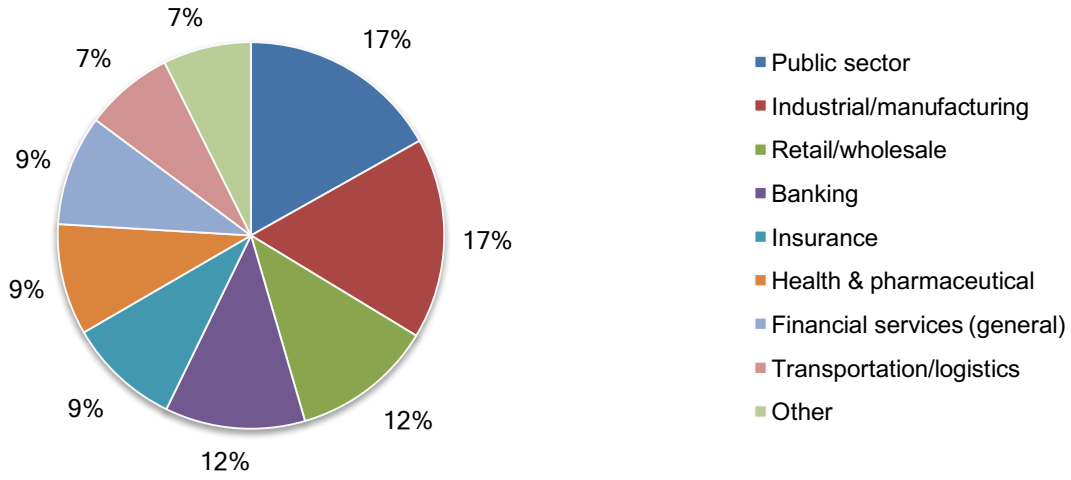

According to Pie Chart 3, 62 percent of respondents are from organizations with a global full-time headcount of more than 5,000 employees.

**Pie Chart 3. Distribution of respondents according to the full-time headcount of the global organization**



Pie Chart 6 reports the primary industry classification of respondents' organizations. This chart identifies public sector (17 percent of respondents) and industrial/manufacturing (17 percent of respondents) as the largest segments, followed by retail/wholesale (12 percent of respondents), and banking (12 percent of respondents).

**Pie chart 6. Distribution of respondents according to 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 in various organizations in North America, the United Kingdom. Germany and France. 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 August 17 to August 31, 2018.

| **Survey response** | Total |
|---|---|
| Total sampling frame | 40,111 |
| Total returns | 1,592 |
| Rejected surveys | 221 |
| Final sample | 1,371 |
| Response rate | 3.4% |

**Part 1. Screening**

| S1. How familiar are you with content collaboration solutions? | Total |
|---|---|
| Very familiar | 38% |
| Familiar | 38% |
| Somewhat familiar | 23% |
| Not familiar (stop) | 0% |
| Total | 100% |

| S2. What percentage of your job function relates to the management, production and protection of information stored in files, such as content and other information assets? | Total |
|---|---|
| Zero (stop) | 0% |
| Less than 10% | 16% |
| 10 to 25% | 31% |
| 26 to 50% | 30% |
| 51 to 75% | 18% |
| 76 to 100% | 5% |
| Total | 100% |
| Extrapolated value | 33.5% |

**Part 2. Background**

| Q1. Which of the following solutions does your organization use for sharing confidential content and files among employees and, possibly, third parties? Please select all that apply. | Total |
|---|---|
| Microsoft SharePoint | 38% |
| Office 365 (OneDrive) | 49% |
| E-mail file sharing | 61% |
| Cloud-based services such as Dropbox and/or Box | 50% |
| Shared network drives | 47% |
| Other file sync and share solutions | 43% |
| Other content collaboration platforms (CCP) | 19% |
| We don't use any content collaboration solutions | 24% |
| Total | 331% |

| Q2. How would you rate your organization's ability to keep sensitive content secure in the file sharing and collaboration environment? Please use the following 10-point scale from 1 = no ability to 10 = high ability. | Total |
|---|---|
| 1 or 2 | 7% |
| 3 or 4 | 18% |
| 5 or 6 | 36% |
| 7 or 8 | 24% |
| 9 or 10 | 15% |
| Total | 100% |
| Extrapolated value | 595% |

| Q3. How would you rate the importance of protecting sensitive content stored in files? Please use the following 10-point scale from 1 = not important to 10 = very important. | Total |
|---|---|
| 1 or 2 | 1% |
| 3 or 4 | 5% |
| 5 or 6 | 21% |
| 7 or 8 | 24% |
| 9 or 10 | 48% |
| Total | 100% |
| Extrapolated value | 7.75 |

| Q4a. What percentage of your organization's sensitive information is unstructured? | Total |
|---|---|
| Less than 10% | 5% |
| 10 to 25% | 12% |
| 26 to 50% | 32% |
| 51 to 75% | 23% |
| 76 to 100% | 28% |
| Total | 100% |
| Extrapolated value | 53.0% |

| Q4b. How many petabytes of unstructured data does your organization have? | Total |
|---|---|
| Less than 1 | 10% |
| 1 to 2 | 44% |
| 3 to 5 | 32% |
| More than 5 | 14% |
| Total | 100% |
| Extrapolated value | 2.67 |

| Q5a. Do you know how much of your total unstructured data is stored in **Office 365 (OneDrive)**? | Total |
|---|---|
| Less than 10% | 11% |
| 10 to 25% | 13% |
| 26 to 50% | 14% |
| 51 to 75% | 10% |
| 76 to 100% | 3% |
| We don't use Office 365 (OneDrive) | 50% |
| Total | 100% |
| Extrapolated value | 16.8% |

| Q5b. Do you know how much of your total unstructured data is stored in **email file sharing solutions**? | Total |
|---|---|
| Less than 10% | 10% |
| 10 to 25% | 16% |
| 26 to 50% | 16% |
| 51 to 75% | 11% |
| 76 to 100% | 8% |
| We don't use an email file sharing solution | 39% |
| Total | 100% |
| Extrapolated value | 23.4% |

| Q5c. Do you know how much of your total unstructured data is stored in **cloud-based services such as Dropbox and/or Box**? | Total |
|---|---|
| Less than 10% | 5% |
| 10 to 25% | 12% |
| 26 to 50% | 17% |
| 51 to 75% | 8% |
| 76 to 100% | 7% |
| We don't use Dropbox and/or Box | 50% |
| Total | 100% |
| Extrapolated value | 19.9% |

| Q5d. Do you know how much of your total unstructured data is stored in **shared network drives**? | Total |
|---|---|
| Less than 10% | 5% |
| 10 to 25% | 13% |
| 26 to 50% | 18% |
| 51 to 75% | 11% |
| 76 to 100% | 5% |
| We don't use shared network drives | 53% |
| Total | 104% |
| Extrapolated value | 20.5% |

| Q5e. Do you know how much of your total unstructured data is stored in **other file sync and share solutions**? | Total |
|---|---|
| Less than 10% | 11% |
| 10 to 25% | 12% |
| 26 to 50% | 17% |
| 51 to 75% | 10% |
| 76 to 100% | 6% |
| We don't use file sync and share solutions | 44% |
| Total | 100% |
| Extrapolated value | 20.1% |

| Q6. What percentage of your organization's data within file sharing and collaboration environment is considered sensitive? | Total |
|---|---|
| Less than 10% | 17% |
| 10 to 25% | 33% |
| 26 to 50% | 30% |
| 51 to 75% | 12% |
| 76 to 100% | 9% |
| Total | 100% |
| Extrapolated value | 32.8% |

| Q7. What percentage of your organization's sensitive information is located (stored) in the public cloud? | Total |
|---|---|
| Less than 10% | 23% |
| 10 to 25% | 26% |
| 26 to 50% | 35% |
| 51 to 75% | 12% |
| 76 to 100% | 4% |
| Total | 100% |
| Extrapolated value | 29.6% |

| Q8. What percentage of your organization's sensitive information is located (stored) on-premises? | Total |
|---|---|
| Less than 10% | 5% |
| 10 to 25% | 18% |
| 26 to 50% | 26% |
| 51 to 75% | 34% |
| 76 to 100% | 17% |
| Total | 100% |
| Extrapolated value | 49.0% |

| Q9. What percentage of your organization's sensitive information is located (stored) in the hybrid cloud? | Total |
|---|---|
| Less than 10% | 31% |
| 10 to 25% | 43% |
| 26 to 50% | 15% |
| 51 to 75% | 8% |
| 76 to 100% | 3% |
| Total | 100% |
| Extrapolated value | 22.3% |

| Q10. What percentage of your organization's employees use file sharing and collaboration solutions to store, edit or share content in the normal course of business? | Total |
|---|---|
| Less than 10% | 10% |
| 10 to 25% | 23% |
| 26 to 50% | 26% |
| 51 to 75% | 24% |
| 76 to 100% | 17% |
| Total | 100% |
| Extrapolated value | 44.0% |

| Q11. What percentage of your organization's content containing sensitive information is shared with third parties? | Total |
|---|---|
| Less than 10% | 13% |
| 10 to 25% | 24% |
| 26 to 50% | 22% |
| 51 to 75% | 27% |
| 76 to 100% | 13% |
| Total | 100% |
| Extrapolated value | 41.9% |

| Q12. How would you rate the importance of sharing externally with partners, vendors and other third parties? Please use the following 10-point scale from 1 = not important to 10 = very important. | Total |
|---|---|
| 1 or 2 | 6% |
| 3 or 4 | 12% |
| 5 or 6 | 17% |
| 7 or 8 | 21% |
| 9 or 10 | 45% |
| Total | 100% |
| Extrapolated value | 7.22 |

| Q13. How would you rate the importance of being able to set security policies based on the relationship with partners, vendors and other third parties? Please use the following 10-point scale from 1 = not important to 10 = very important. | Total |
|---|---|
| 1 or 2 | 6% |
| 3 or 4 | 9% |
| 5 or 6 | 16% |
| 7 or 8 | 31% |
| 9 or 10 | 37% |
| Total | 100% |
| Extrapolated value | 7.19 |

| **Part 3. Attributions:** Please rate your opinion to each item using the scale provided below each statement. **Strongly Agree and Agree response combined.** | Total |
|---|---|
| Q14a. Not knowing where my organization's sensitive information resides represents a significant security risk. | 65% |
| Q14b. Our organization is concerned about storing all of its unstructured data in the public cloud. | 49% |
| Q14c. It is important to have the flexibility to store files both on-premises and in the public cloud. | 66% |
| Q14d. It is important to have seamless access to files both on-premises and in the public cloud. | 61% |
| Q14e. In my organization, securing and/or protecting sensitive information is a high priority. | 49% |
| Q14f. Our organization's employees understand the importance of secure file sharing and collaboration. | 43% |
| Q14g. Our organization's third parties, vendors and other third parties understand the importance of secure file sharing and collaboration. | 39% |
| Q14h. In my organization, access to sensitive data is controlled by permissions, role, location and/or other factors. | 42% |
| Q14i. Our organization is concerned about Shadow IT in the file sharing and collaboration environment. | 38% |
| Q14j. Our organization has clear visibility into what file sharing applications are being used by employees at work. | 27% |
| Q14k. Our organization does a good job educating individuals on keeping sensitive data in the collaboration and file-sharing environment safe, in accordance with our security and compliance policies. | 33% |
| Q14l. Our organization is concerned about meeting GDPR requirements for personal data in the file-sharing and collaboration environment. | 59% |
| Q14m. In my organization, digital transformation is challenged by the need for strict security safeguards to protect the sharing and use of data that is sensitive and critical. | 70% |
| Q14n. A solution that provides a flexible security framework for different file sharing and collaboration scenarios is essential for our organization's digital transformation. | 58% |
| Q14o. The inability to enable the free flow and sharing of information is a barrier to achieving digital transformation. | 60% |
| Q14p. Providing security policies based on type of user, type of content, region or department would improve the digital transformation. | 58% |

**Part 4. Managing risk in the file sharing and collaboration environment**

| Q15. In the context of data loss or theft, what types of sensitive information do you consider to be most at risk in your organization? Please select your top two choices. | Total |
|---|---|
| Customer PII | 54% |
| Employee PII | 24% |
| Analytics (algorithms and models) | 13% |
| Finance and accounting | 14% |
| Payment data (i.e. credit card number) | 19% |
| Confidential content and files | 49% |
| Intellectual property | 32% |
| Other (please specify) | 2% |
| Total | 208% |

| Q16. With respect to security in the content collaboration and file-sharing environment, what worries you the most? Please select your top two choices. | Total |
|---|---|
| External hackers | 33% |
| Malicious employees | 15% |
| Broken security management processes | 29% |
| Employees accidentally exposing information | 60% |
| Temporary workers, contractors or third parties accessing data they should not see | 50% |
| Costly fines and penalties from non-compliance with such regulations as GDPR | 11% |
| Other (please specify) | 2% |
| Total | 200% |

| Q17. Who within your organization has ultimate responsibility for the safe use of sensitive information assets in the file sharing and collaboration environment? Note that we are asking about responsibility for both the tool and the behavior of users. Please check only two responses. | Total |
|---|---|
| Chief information security officer | 40% |
| Chief security officer | 4% |
| Chief information officer | 46% |
| Chief technology officer | 17% |
| General counsel | 1% |
| Compliance officer | 26% |
| Risk management leader | 8% |
| Line of business leaders | 38% |
| Application owners/users | 17% |
| Other (please specify) | 2% |
| Total | 200% |

| Q18. What technologies or tools does your organization have in place to support the safe use of sensitive information assets in the file sharing collaboration environment? Please check all that apply. | Total |
|---|---|
| Application-level access controls (i.e. within SharePoint itself) | 39% |
| Enterprise Data Loss Prevention (DLP) | 42% |
| Digital Asset Management (DAM) | 28% |
| File encryption | 72% |
| Digital Rights Management (DRM) | 34% |
| File system and access audits | 40% |
| Identity and Access Management | 70% |
| Security Information & Event Management (SIEM) | 45% |
| Other (please specify) | 3% |
| Total | 372% |

| Q19. How would you rate the tools you have in place to support the safe use of sensitive information assets in the file sharing and collaboration environment? Please use the following 10-point scale from 1 = not effective to 10 = very effective. | Total |
|---|---|
| 1 or 2 | 10% |
| 3 or 4 | 14% |
| 5 or 6 | 41% |
| 7 or 8 | 21% |
| 9 or 10 | 13% |
| Total | 100% |
| Extrapolated value | 577% |

| Q20. What challenges do you face when relying on tools to support the safe use of sensitive information assets in the file sharing and collaboration environment? Please select all that apply. | Total |
|---|---|
| Inaccuracies (data and applications) | 51% |
| Not integrated with our file sharing and collaboration solutions | 54% |
| Difficult to configure | 61% |
| Complexity slows down the system | 40% |
| Difficult to scale as the use of file sharing and collaboration grows | 62% |
| Frustrated users turn to other solutions | 48% |
| No challenges | 4% |
| Total | 320% |

| Q21. How confident are you that your organization has visibility into users' access to sensitive information assets in the file-sharing and collaboration environment? Please use the following 10-point scale from 1 = no confidence to 10 = very confident. | Total |
|---|---|
| 1 or 2 | 19% |
| 3 or 4 | 20% |
| 5 or 6 | 31% |
| 7 or 8 | 21% |
| 9 or 10 | 10% |
| Total | 100% |
| Extrapolated value | 516% |

| Q22. Which of the following data governance tasks has your organization deployed for the protection of information assets in the file sharing and collaboration environment? Please select all that apply. | Total |
|---|---|
| Tracking where sensitive and confidential data are located | 56% |
| Managing data classification with prioritization | 52% |
| Monitoring access rights or permissions based on job, role, or on a need-to-know-basis | 62% |
| Managing access changes based on changes in policy, user needs or application updates | 55% |
| Revoking data access rights upon an employee's termination or changes in policy | 56% |
| Enforcing data access policies in a consistent fashion across applications, locations, departments, technology standards, etc. | 54% |
| Monitoring data transfers to and from third-party locations including cloud | 62% |
| Educating end-users about data access and control policies | 44% |
| Implementing and enforcing data loss prevention solutions | 46% |
| Providing a comprehensive digital forensics capability | 35% |
| Other (please specify) | 2% |
| Total | 523% |

| Q23. Very Likely and Likely responses combined | Total |
|---|---|
| Q23a. How likely do you believe your organization had a data breach resulting from the loss or theft of sensitive information in the file sharing and collaboration environment in the past 2 years? | 63% |
| Q23b. If very likely or likely, do you believe this breach incident would have been avoided if your organization had more effective data loss protection technologies in place? | 65% |
| Q23c. If very likely or likely, do you believe this breach incident would have been avoided if your organization had a larger budget or spending level? | 56% |
| Q23d. If very likely or likely, do you believe this breach incident would have been avoided if your organization had more skilled personnel with data security responsibilities? | 73% |
| Q23e. If very likely or likely, do you believe this breach incident would have been avoided if your organization had fewer silos and/or turf issues among IT, IT security and lines of business (LoB)? | 49% |

| Q24. What actions do you plan to take in the next 12 months to better protect sensitive data in the file sharing and collaboration environment? Please select all that apply. | Total |
|---|---|
| Invest in additional security tools such as data loss prevention | 43% |
| Invest in more secure collaboration tools | 53% |
| Improve secure management of these solutions | 50% |
| Educate users | 44% |
| Conduct security audits | 29% |
| Other (please specify) | 3% |
| Total | 221% |

| Q25. If you had the following capabilities, do you believe it would improve the security and productivity of end users in the file sharing and collaboration environment? Please respond to each capability using the scale provided below the item. **Significant improvement and improvement responses combined.** | Total |
|---|---|
| Q25a. Centralized location for unstructured data | 49% |
| Q25b. The ability to securely collaborate with colleagues both inside and outside the organization | 70% |
| Q25c. Enable colleagues to access files no matter what device they use | 65% |
| Q25d. Ensure files are not overwritten and the right versions are available to colleagues | 45% |
| Q25e. Securely share video, design and other heavy files regardless of size | 30% |
| Q25f. Send files without logging into FTP sites or portals | 41% |
| Q25g. Email links instead of files so you can track where the files go | 47% |
| Q25e. Recover previous versions of files instantly and automatically back up working contents in real time | 65% |
| Q25f. Have mobile, VPN-less access to files in home directories, file shares and SharePoint | 57% |

| Q26. How frequently do the following incidents happen among users (knowledge workers) in the file sharing and collaboration environment? **Very Frequently and Frequently responses combined**. | Total |
|---|---|
| Q26a. Users received files and contents not intended for them. | 70% |
| Q26b. Users did not delete confidential contents or files as required by policies. | 62% |
| Q26c. Users accidently share files or contents with individuals not authorized to receive them. | 67% |
| Q26d. Users accidently share files or contents with unauthorized individuals outside the organization. | 59% |

| Q27. With respect to classifying contents by level of security, how is file-level confidentiality determined in the file sharing and collaboration environment? Please select all that apply. | Total |
|---|---|
| Data type – PII, PHI, etc. | 60% |
| Data usage (size limits, large downloads) | 62% |
| Technology usage (e.g., by type of mobile device) | 52% |
| Location of users | 61% |
| Content owners | 47% |
| Who has access to the content | 44% |
| User behaviors | 36% |
| We do not determine content and file-level confidentiality | 24% |
| Other (please specify) | 2% |
| Total | 389% |

| Q28. In the past 12 months, how often did your organization conduct audits or assessments to determine if content activities in the file sharing and collaboration environment are in compliance with policies, laws and regulations? | Total |
|---|---|
| Once | 22% |
| More than once on a regular basis | 24% |
| At least once, but on an ad-hoc basis | 27% |
| Never | 27% |
| Total | 100% |

| **Part 5. General Data Privacy Regulation (GDPR)** | |
|---|---|
| Q29. How familiar are you with the GDPR? | Total |
| Very familiar | 31% |
| Familiar | 43% |
| Not familiar | 17% |
| No knowledge (skip to Part 6) | 10% |
| Total | 100% |

| Q30. Are your file sharing and content collaboration activities in compliance with data protection regulations, such as GDPR? | Total |
|---|---|
| Yes, full compliance | 29% |
| Yes, partial compliance | 36% |
| Not in compliance | 17% |
| Unsure | 18% |
| Total | 100% |

| Q31. How does GDPR affect your organization's file sharing and content collaboration activities? | Total |
|---|---|
| Increases costs | 53% |
| Requires new investments in enabling security technologies | 39% |
| Requires hiring of security experts | 33% |
| Changes workflows | 66% |
| Reduces access to personal information | 69% |
| Increases compliance and audit activities | 60% |
| Other (please specify) | 1% |
| Total | 322% |

| Q32. Does GDPR require your organization to change the way sensitive information is accessed and shared? | Total |
|---|---|
| Significant change | 27% |
| Some change | 39% |
| Insignificant change | 17% |
| No change | 17% |
| Total | 100% |

| **Part 6. Demographics & organizational characteristics** | |
|---|---|
| D1. What best describes your position level within the organization? | Total |
| Executive/VP | 8% |
| Director | 22% |
| Manager/Supervisor | 30% |
| Staff | 34% |
| Contractor | 5% |
| Other (please specify) | 2% |
| Total | 100% |

| D2. To whom do you report to within the organization? | Total |
|---|---|
| CEO/executive committee | 1% |
| Chief operating officer | 1% |
| Chief financial officer | 0% |
| Chief information security office | 19% |
| Chief security officer | 4% |
| Chief information officer | 32% |
| Chief technology officer | 8% |
| General counsel | 2% |
| Compliance officer | 6% |
| Risk management leader | 8% |
| Lines of business management | 17% |
| Other (please specify) | 1% |
| Total | 99% |

| D3. What range best describes the full-time headcount of your global organization? | Total |
|---|---|
| 500 to 1,000 | 18% |
| 1,001 to 5,000 | 22% |
| 5,001 to 10,000 | 25% |
| 10,001 to 25,000 | 22% |
| 25,001 to 75,000 | 9% |
| More than 75,000 | 6% |
| Total | 100% |

| D4. What best describes your organization's primary industry classification? | Total |
|---|---|
| Financial services (general) | 9% |
| Banking | 12% |
| Insurance | 9% |
| Health & pharmaceutical | 9% |
| Industrial/manufacturing | 17% |
| Public sector | 17% |
| Retail/wholesale | 12% |
| Transportation/logistics | 7% |
| Other (please specify) | 7% |
| Total | 100% |

**Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.**

## 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.

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.