



Handle with Care: Protecting Sensitive Data in Microsoft SharePoint, Collaboration Tools and File Share Applications in US, UK and German Organizations

Sponsored by **Quest** | **Metalogix**
Now part of Quest

Independently conducted by Ponemon Institute LLC

Publication Date: May 2017

Handle with Care: Protecting Sensitive Data in Microsoft SharePoint, Collaboration Tools and File Share Applications in US, UK and German Organizations

Ponemon Institute, May 2017

Part 1. Introduction

With the plethora of collaboration and file sharing tools in the workplace, the risk of data leakage due to insecure sharing of information among employees and third parties is growing. As discussed in this report, *Handle with Care: Protecting Sensitive Data in Microsoft SharePoint, Collaboration Tools and File Share Applications in US, UK and German Organizations*, sponsored by Metalogix, although security concerns about the use of collaboration and file sharing tools is high, companies are not taking sufficient steps to protect their sensitive data.¹

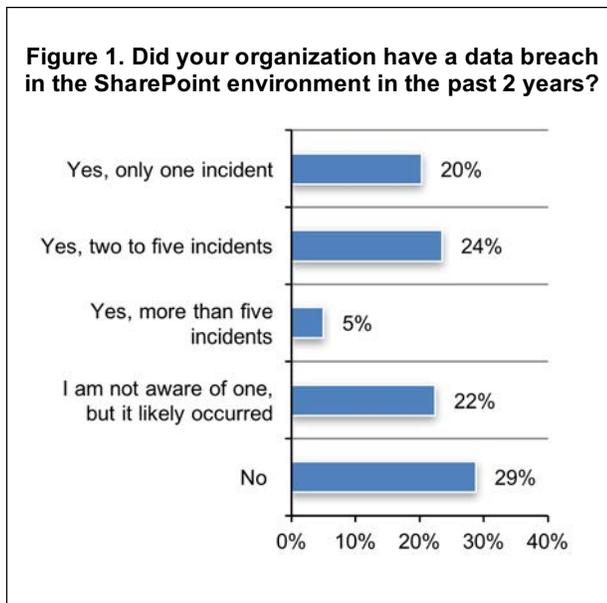
Without appropriate technologies, data breaches in the SharePoint environment can go undetected. As shown in Figure 1, almost half of respondents (49 percent) say their organizations have had at least one data breach in the SharePoint environment in the past two years. However, 22 percent of respondents believe it was likely their organization had a data breach but are not able to know this with certainty.

This research reveals that employees on a frequent basis are accidentally sharing files or documents with other employees or third parties not authorized to receive them. Employees are also receiving content they should not have access to or they are not deleting confidential materials as required by policies.

Although respondents express concern about the risk of a data breach stemming from use of collaboration and file sharing technologies, they are struggling to meet the challenge using their existing security processes and tools. Seventy percent of organizations believe that if their organization had a data breach involving the loss or theft of confidential information in the SharePoint environment they would only be able to detect it some of the time or not at all.

Most companies are not taking steps to reduce the risk through training programs, routine security audits or deployment of specific technologies that discover where sensitive or confidential information resides and how it is used. The survey found that important data governance practices that are not in place for collaboration applications in general, and that when it comes to SharePoint specifically, security tools and practices are even more lacking.

We surveyed 1,403 individuals in the US, UK and Germany who are involved in



¹ All references, citations and quotations from this survey must attribute Ponemon/Metalogix, *Handle with Care: Protecting Sensitive Data in Microsoft SharePoint, Collaboration Tools and File Share Applications*.

ensuring the protection of confidential information. Respondents work in IT and IT security as well as lines of business in a variety of industries. On average, respondents say they spend approximately 28 percent of their time in the protection of documents and other content assets in SharePoint.

All companies represented in this research use SharePoint solutions for sharing confidential documents and files. Other solutions include Office 365 and cloud-based services such as Dropbox and/or Box. Other means of collaboration include shared network drives and other file sync and share solutions.

Part 2. Key findings

In this section, we provide a deeper analysis of the findings. The complete audited findings are presented in the Appendix of this report. The report is organized according to the following seven topics:

1. Sensitive content within the organization
2. Risky user behavior
3. Lack of collaboration in security and governance practices and tools
4. Challenges in controlling risks in the SharePoint environment
5. Country differences: United States, United Kingdom and Germany
6. Industry differences
7. Conclusions and recommendations

1. Sensitive content within the organization

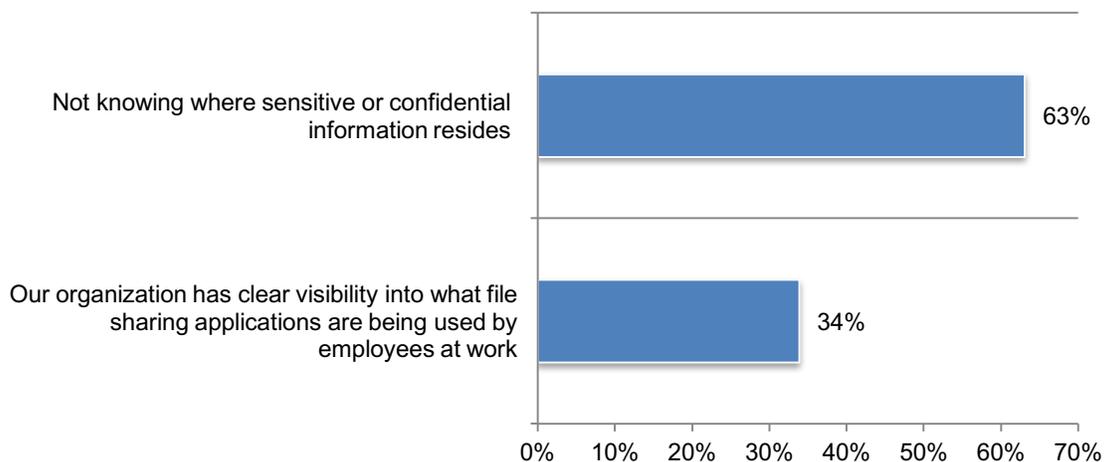
Not knowing who is sharing sensitive data or where such data is stored increases the likelihood of a breach.

As shown in Figure 2, 63 percent say the inability to know where sensitive data resides represents a serious security risk. Further, only 34 percent of respondents say their organizations have clear visibility into what file sharing applications are being used by employees at work.

These findings demonstrate the need for automated technologies that enable organizations to discover and classify sensitive or confidential information and monitor how it is used.

Figure 2. Why is sensitive data at risk in file sharing applications?

Strongly agree and Agree responses combined



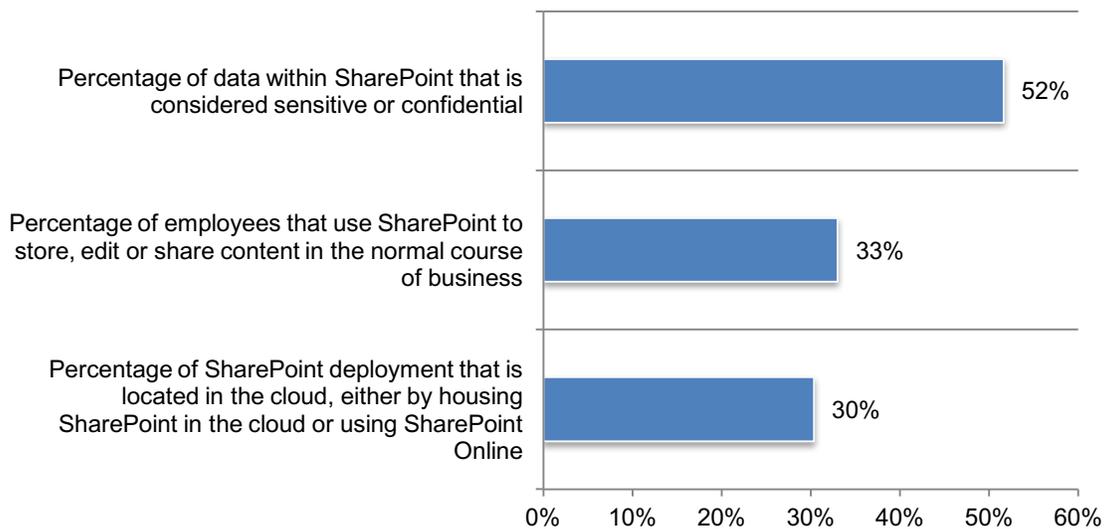
Data breaches are likely because organizations are storing a vast amount of sensitive or confidential data in SharePoint.

As presented in Figure 3, on average, 52 percent of an organization’s sensitive or confidential data is stored in SharePoint and an average of 33 percent of employees in the organizations represented use SharePoint to store, edit or share content in the normal course of business.

An average of 30 percent of organizations’ SharePoint deployment is located in the cloud, either by housing SharePoint in the cloud or using SharePoint online.

Figure 3. The state of SharePoint in organizations

Extrapolated value



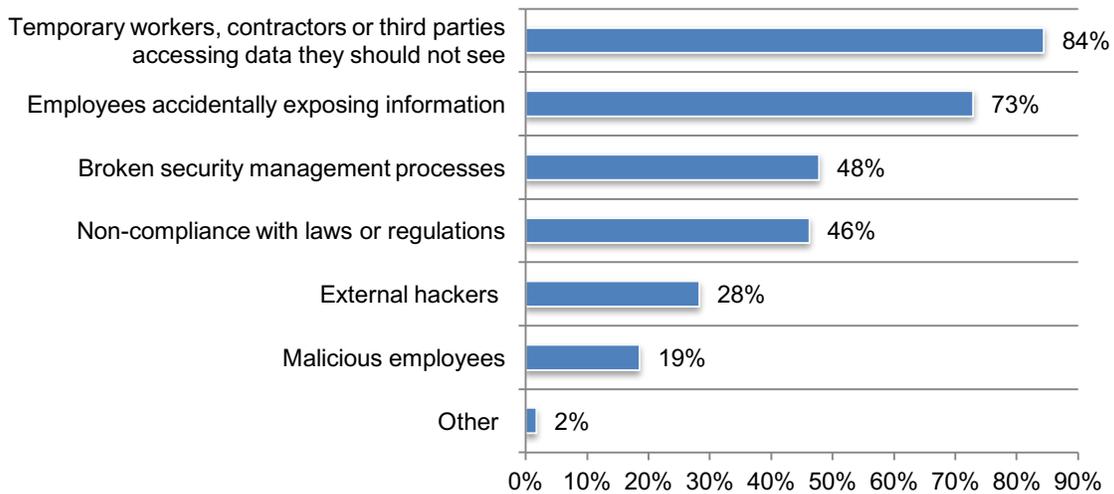
2. Risky user behavior

Employee and third party use of SharePoint are greater security concerns than external threat agents.

The pressure to be productive sometimes causes individuals to put sensitive data at risk. As shown in Figure 4, negligent employees are inviting data loss or theft by accidentally exposing information (73 percent of respondents). Eighty-four percent of respondents are worried about third parties having access to data they should not see. Based on the findings, third parties and negligent insiders are more worrisome than external hackers (28 percent of respondents) or malicious employees (19 percent of respondents).

Figure 4. What worries you most about security in the SharePoint environment?

Three choices permitted

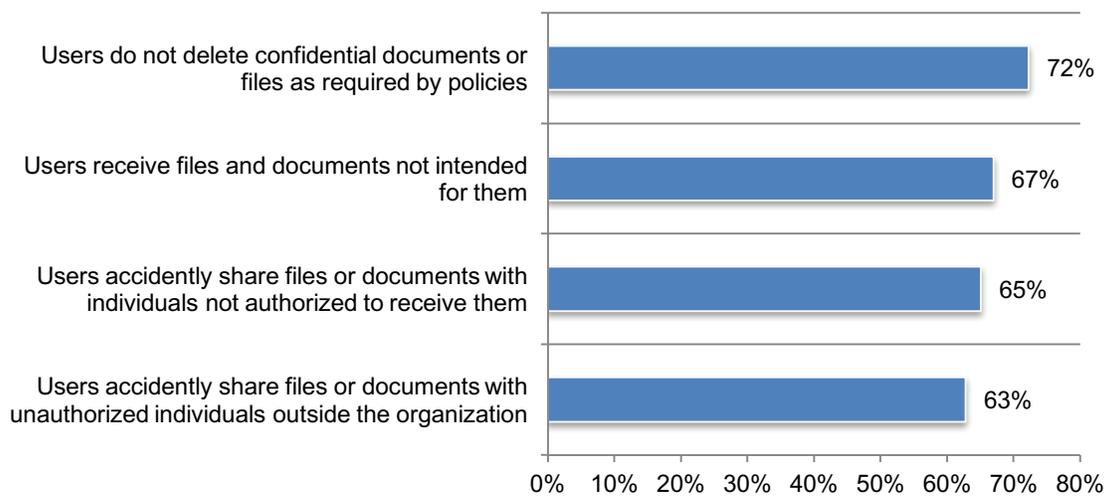


Employees are careless and often circumvent policies in their use of SharePoint.

The research reveals an epidemic of negligence in organizations. Consistent with the finding above, 72 percent of respondents, say users of SharePoint are not deleting confidential documents or files as required by policies and 67 percent of respondents say users received files and documents not intended for them, as shown in Figure 5. By accident, users are sharing files or documents with individuals not authorized to receive them (65 percent of respondents) or sharing files or documents with unauthorized individuals outside the organization (63 percent of respondents).

Figure 5. How frequently are users engaging in negligent behavior in the workplace?

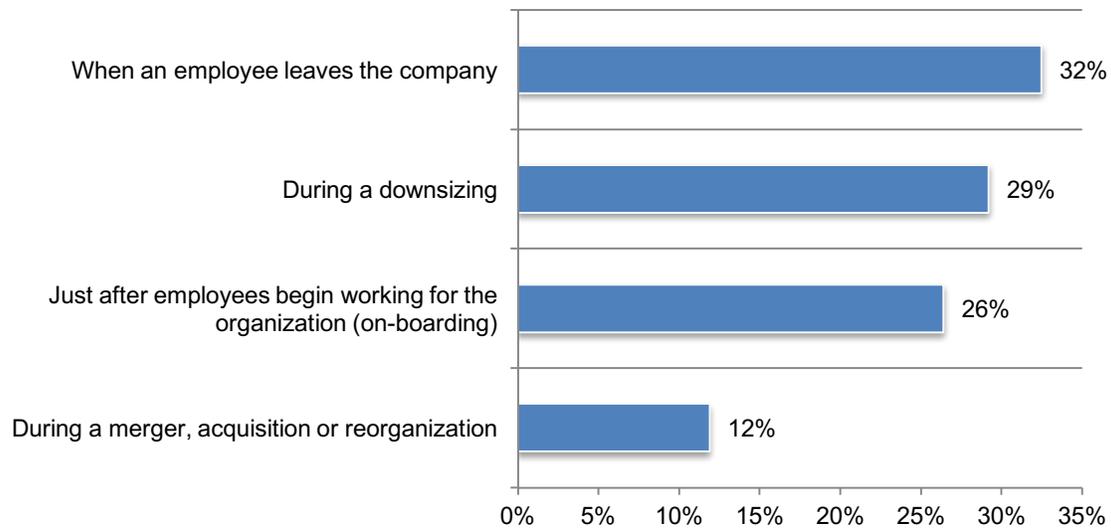
Very frequently and Frequently responses combined



Certain personnel and organizational changes can trigger a security risk.

When should companies be more vigilant to reduce the loss or theft of sensitive data due to employee negligence? According to Figure 6, the most risky situations are when employees leave the company or are affected by downsizing (32 percent and 29 percent of respondents, respectively). Negligence also can occur when employees are newly hired, need access to content, and have yet to be trained on the proper use of collaboration and file sharing tools.

Figure 6. When do you think sensitive or confidential data is at risk from negligent employee behavior?



3. Lack of collaboration in security and governance practices and tools

Despite the volume of sensitive content stored in collaboration and file sharing tools and the acknowledgement of risky employee behavior, respondents do not have sufficient policies or security tools in place to prevent either accidental exposure or intentional misuse of information.

Only 28 percent of respondents rate their organizations as being highly effective in keeping confidential documents secure in the SharePoint environment. Consequently, as reported previously (Figure 1), almost half of respondents (49 percent) report their companies had at least one data breach resulting from the loss or theft of confidential information in the SharePoint environment in the past two years and 22 percent of respondents say they are not aware of a data breach, but one is likely to have occurred.

Many companies do not have policies and processes in place to safeguard sensitive and confidential data.

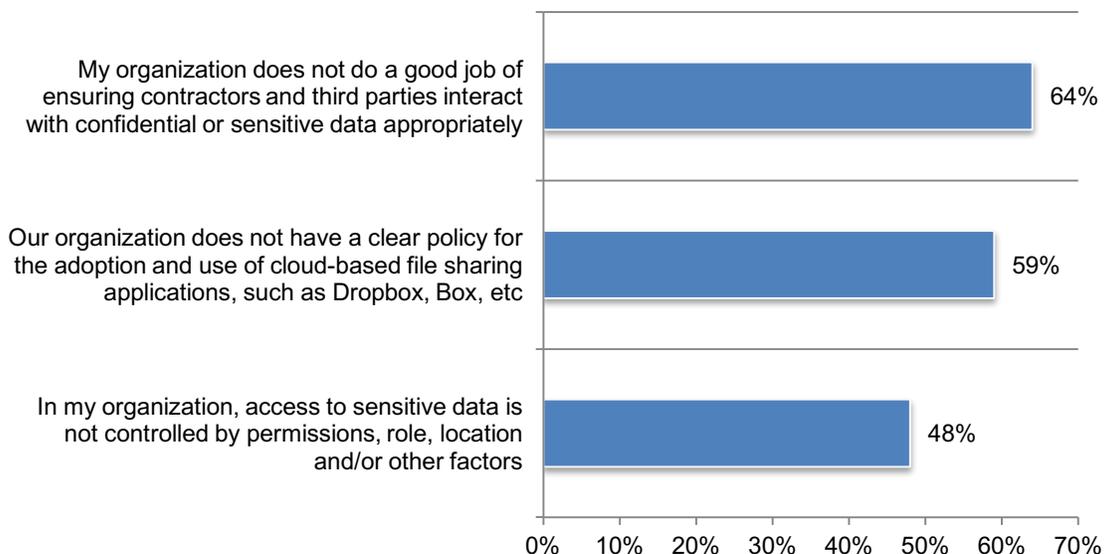
Fifty-nine percent of respondents say their organizations do not have a clear policy for the adoption and use of cloud-based file sharing applications, such as Dropbox or Box. Moreover, almost half of respondents (48 percent) say their organizations are not controlling access to sensitive data is controlled by permissions, role, location and/or other factors.

Companies are not addressing the third party risk.

As shown in Figure 7, 64 percent of respondents believe their organization does not do a good job of ensuring contractors and third parties interact with confidential or sensitive data appropriately. This puts a significant amount of sensitive data at risk because, according to respondents, an average of 36 percent of their organizations' content containing sensitive or confidential information is shared with third parties.

Figure 7. Many companies do not have policies and processes in place to safeguard sensitive and confidential data

Strongly agree and Agree responses combined

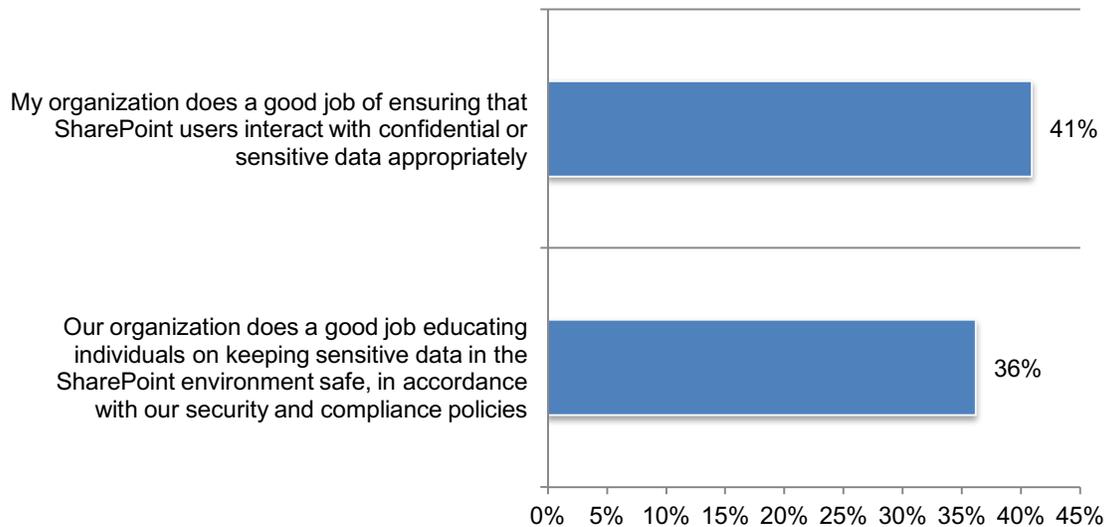


To reduce the risk of employee negligence, more companies should train on the appropriate use of SharePoint.

As shown in Figure 8, only 41 percent of respondents say their organization does a good job of ensuring that SharePoint users interact with confidential or sensitive data appropriately and only 36 percent of respondents believes their organization does a good job educating individuals on keeping sensitive data in the SharePoint environment safe, in accordance with their security and compliance policies.

Figure 8. Perceptions about training SharePoint users

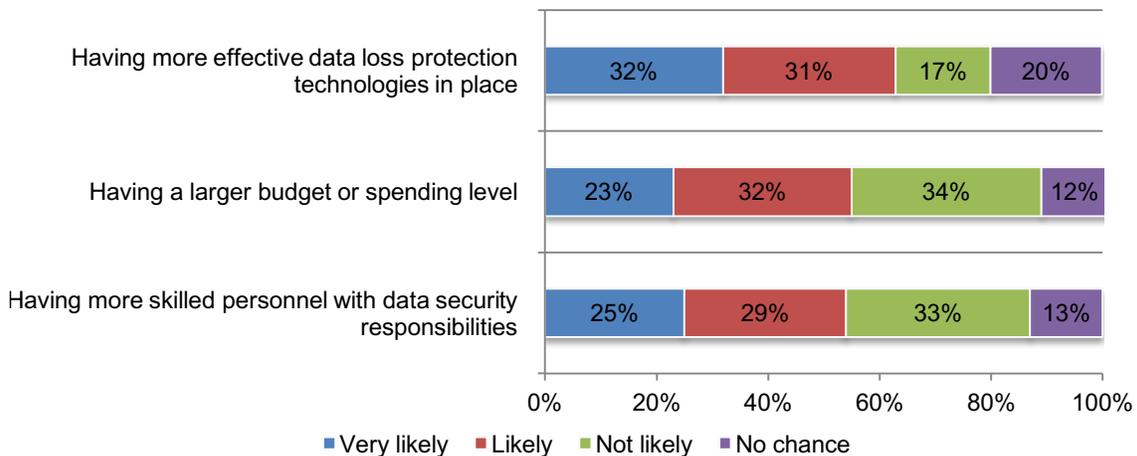
Strongly agree and Agree responses combined



More effective data loss prevention (DLP) technologies are needed to reduce the risk of a data breach.

According to Figure 9, data breaches likely could have been avoided if effective DLP technologies were in place (63 percent of respondents), a larger budget was available (55 percent of respondents) or more skilled personnel with data security responsibilities were employed (54 percent of respondents).

Figure 9. What steps would likely reduce the risk of a data breach in the SharePoint environment?

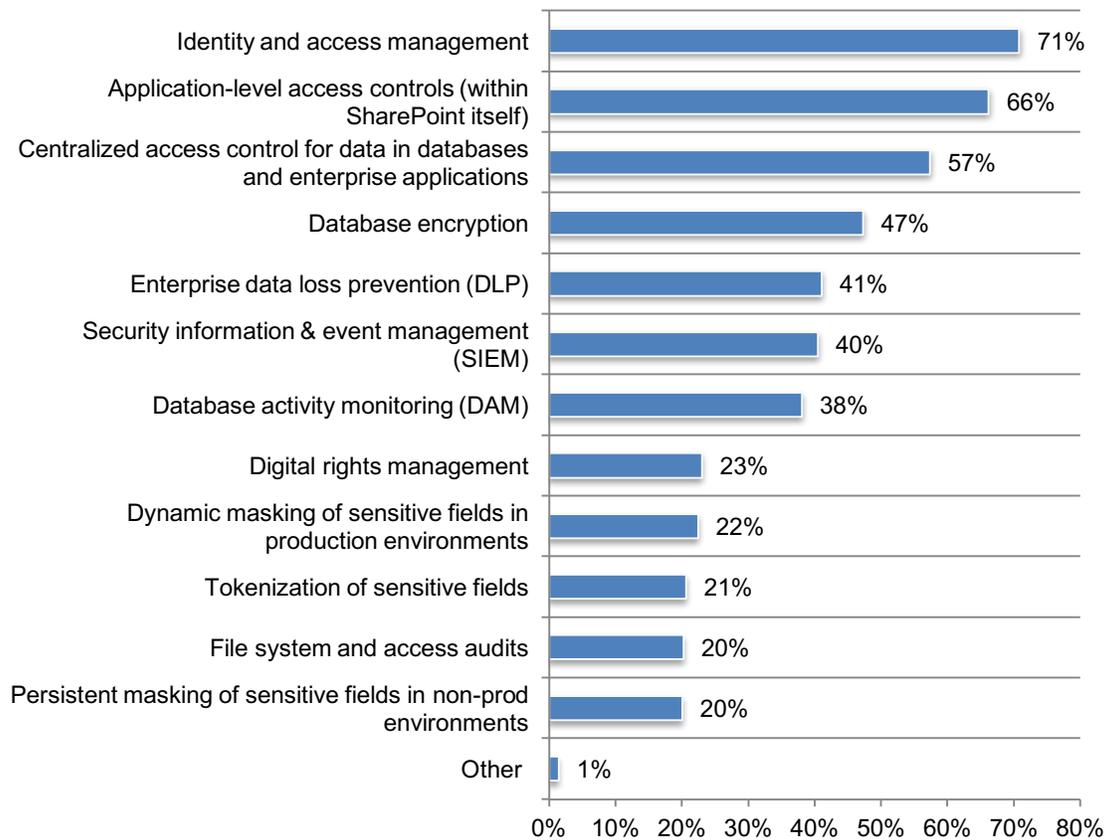


To protect data in the SharePoint environment, IAM and application-level access controls are solutions most often used.

The top three technologies or tools organizations in this study currently have in place to support the safe use of sensitive or confidential information assets in the SharePoint environment are: identity and access management (71 percent of respondents), application-level access controls within SharePoint itself (66 percent of respondents) and centralized access control for data in databases and enterprise applications (57 percent of respondents).

However, only 41 percent of respondents say they use enterprise data loss prevention (DLP). Digital rights management (23 percent of respondents), dynamic masking of sensitive fields in production environments (22 percent of respondents), tokenization of sensitive fields (21 percent of respondents) and file system and access audits (20 percent of respondents) are least used.

Figure 10. What technologies or tools are in place to protect sensitive data in SharePoint?
More than one choice permitted

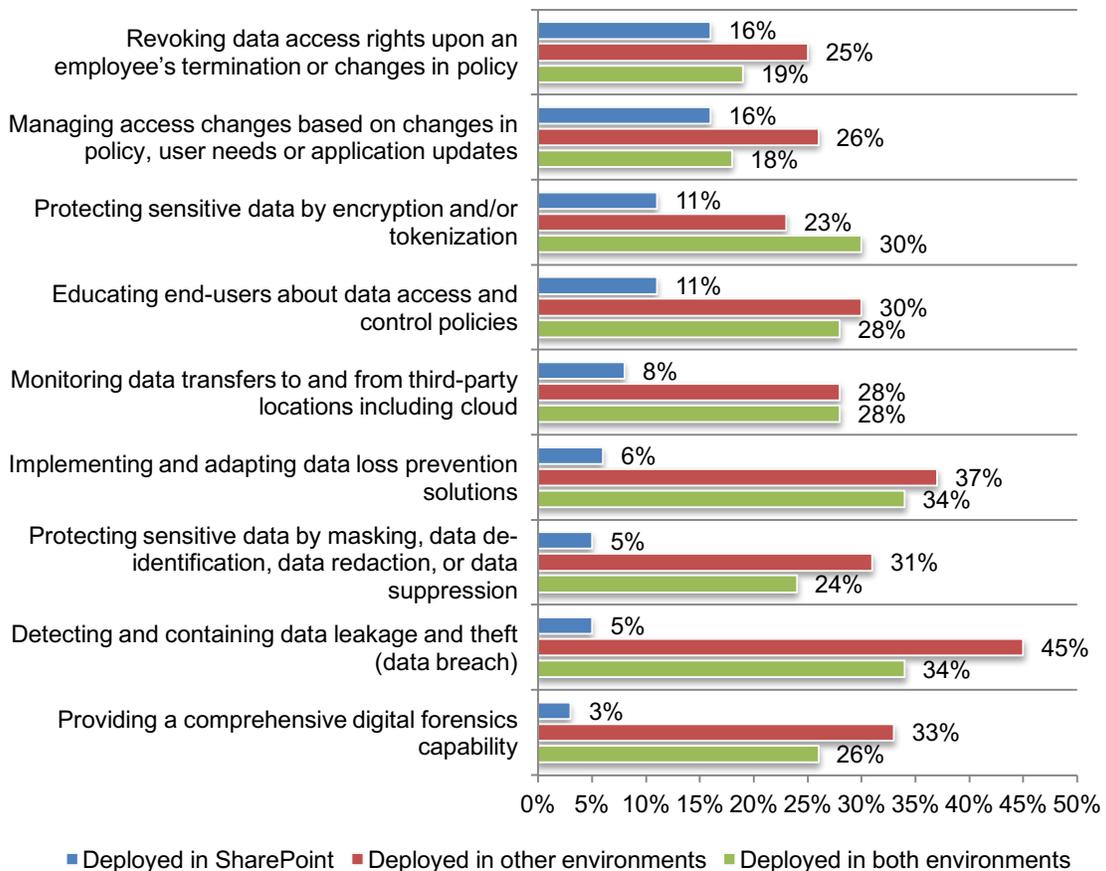


SharePoint lags other collaboration/file sharing applications in the deployment of critical data governance tasks.

We asked respondents to indicate if various security and data governance tasks are deployed in SharePoint, deployed in other environments, deployed in both SharePoint and other environments, or not deployed at all. Figure 11 shows the percentages of respondents who say the tasks are deployed in SharePoint, deployed in other collaboration environments or deployed in both SharePoint and other environments. For example, 16 percent of respondents say revoking data access rights to SharePoint users occurs upon an employee’s termination or changes in policy, while 25 percent of respondents say this task is deployed in other collaboration applications only and 19 percent of respondents say the task is deployed in both. Figure 12 shows the tasks most often not deployed.

A key takeaway from the findings in Figure 11 is that certain critical data governance tasks are rarely deployed in the SharePoint environment. These include detecting and containing data leakage (5 percent SharePoint vs. 45 percent in other applications), implementing and adapting DLP solutions (6 percent in SharePoint vs. 37 percent of respondents in other applications) and providing a comprehensive digital forensics capability (3 percent in SharePoint vs. 33 percent of respondents in other applications).

Figure 11. Data governance tasks deployed in SharePoint vs. other collaboration/file sharing applications



Important governance tasks are not deployed in ANY collaboration/file sharing environment.

According to Figure 12, tasks most often not deployed in ANY collaboration environments are: monitoring data access of privileged users across structured and unstructured data (54 percent of respondents), constructing data architecture, including maps, lineage, flows and inventories (45 percent of respondents) and tracking where sensitive and confidential data are located (44 percent of respondents). Thirty-seven percent of respondents never conduct audits or assessments to determine if content activities in the SharePoint environment are in compliance with policies, laws and regulations.

Thirty-six percent of respondents say they do not revoke data access rights upon an employee’s termination for any collaboration or file sharing application. It is possible respondents believe access rights are controlled via other means (such as via Active Directory) or by others in the organization. It is important to note that relying upon other tools, such as Active Directory, is not a foolproof way to control access and could result in former employees having access to sensitive or confidential documents months or even years after they leave the organization.

Figure 12. Top 10 governance tasks not deployed in ANY collaboration/file sharing environment

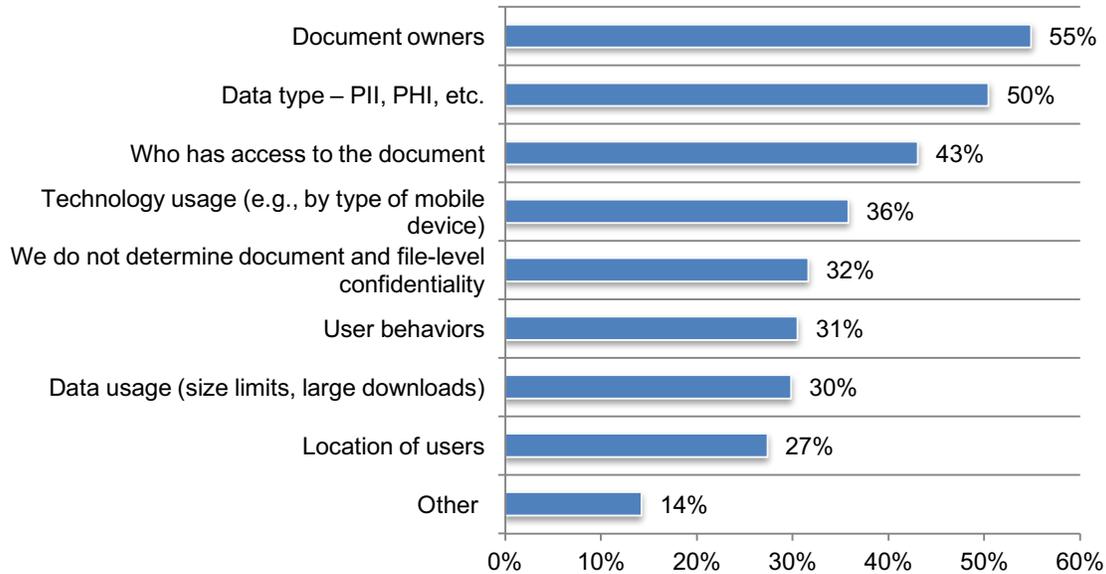


Document owners are determining the confidentiality of information in the SharePoint environment.

As shown in Figure 13, 55 percent of respondents say document owners are determining the file-level confidentiality of the documents they own and 50 percent of respondents say the sensitivity of data determines the file-level confidentiality. Thirty-two percent are not determining document and file-level confidentiality.

Figure 13. How is file-level confidentiality determined in the SharePoint environment?

More than one choice permitted



4. Challenges in controlling risks in the SharePoint environment

If companies are aware of the risk of data breaches due to insecure collaboration and they don't believe their current approaches are sufficient to keeping content safe, what is preventing them from deploying more effective security solutions?

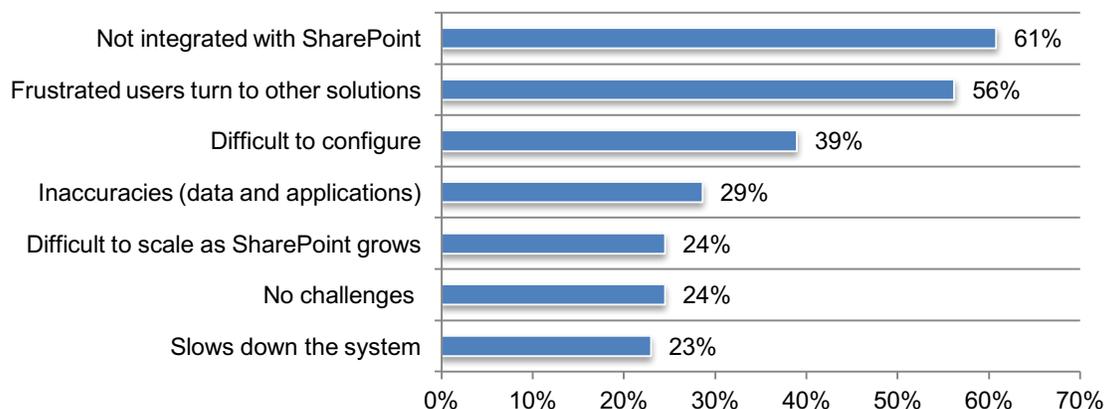
A lack of integration is the biggest challenge to reducing SharePoint security risks.

Seventy-nine percent of respondents say they do not have the right tools in place to support the safe use of sensitive or confidential information assets in SharePoint. Either they believe their tools are only somewhat effective (41 percent of respondents), not effective (49 percent of respondents) or they do not have enough information to know (10 percent of respondents).

As shown in Figure 14, 61 percent of respondents say their current toolset is not effective to secure content collaboration and file sharing in SharePoint due to the lack of integration. Other challenges include having to deal with frustrated users who turn to other solutions to accomplish their tasks (56 percent of respondents) or having to work with tools too difficult to configure (39 percent of respondents).

Figure 14. What challenges do you face when relying on tools to safeguard sensitive data in SharePoint?

More than one choice permitted



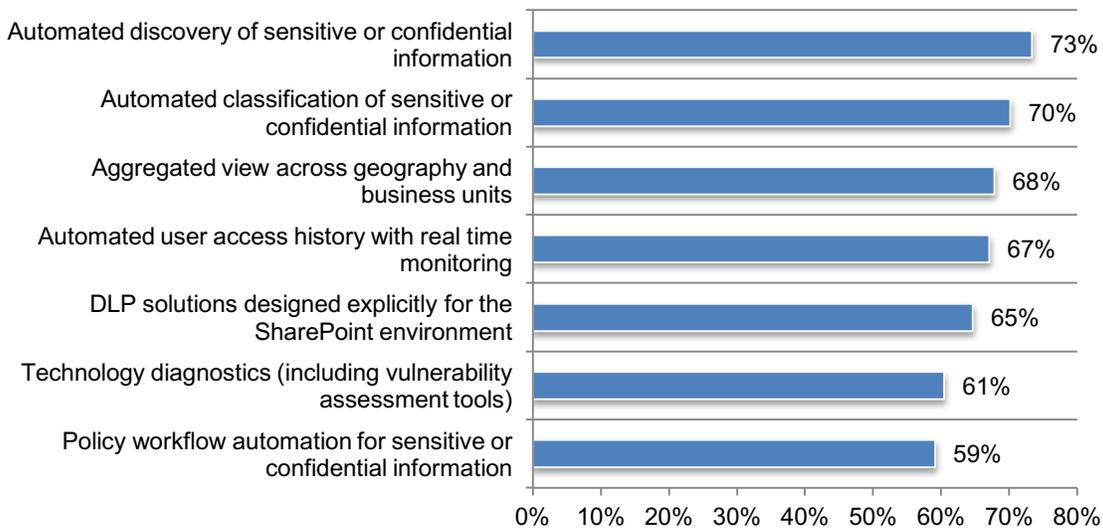
Automated tools would improve organizations' information security posture in the SharePoint environment.

Currently only 28 percent of respondents say their organization uses automated tools to discover where sensitive or confidential information is located within the SharePoint environment and/or how that content is accessed and shared.

However, as shown in Figure 15, 73 percent of respondents say the automated *discovery* of sensitive or confidential information and 70 percent say the automated *classification* of sensitive or confidential information would improve their ability to secure data in the SharePoint environment. Other solutions that would be effective are an aggregated view across geography and business units (68 percent of respondents) and automated user access history with real time monitoring (67 percent of respondents).

Figure 15. Would certain capabilities improve information security posture in the SharePoint environment?

Significant Improvement and Improvement responses combined

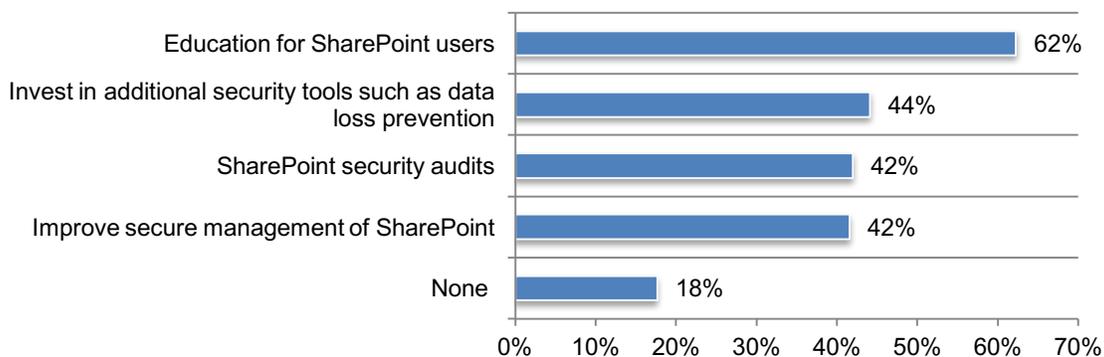


Education of SharePoint users is a priority for most companies.

Respondents do recognize the risks to sensitive content in SharePoint and 82 percent of respondents say their companies plan to take steps to address those risks in the next year. These steps are shown in Figure 16. Sixty-two percent of respondents say in the next 12 months they will provide training for SharePoint users. Forty-four percent of respondents say they will invest in additional security tools such as data loss prevention. Forty-two percent of respondents say they will invest in additional security tools such as data loss prevention. Forty-two percent of respondents say they will improve secure management of SharePoint. Eighteen percent of respondents say they will take none of these steps.

Figure 16. Steps to be taken to better protect sensitive data in SharePoint

More than one choice permitted

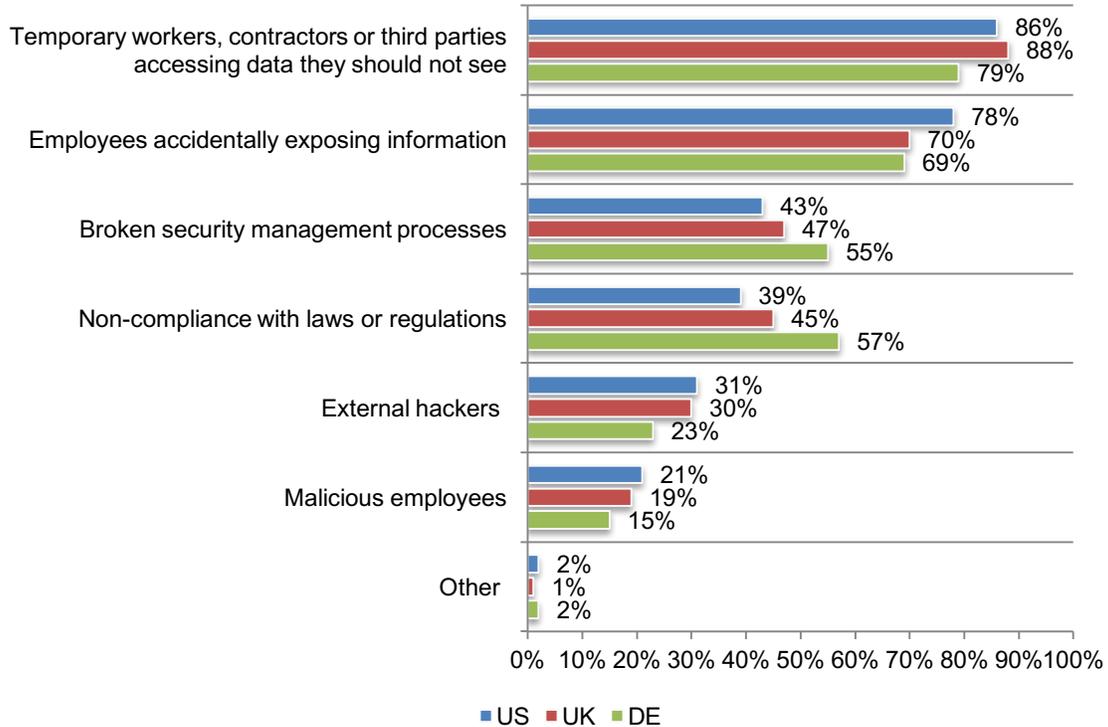


5. Country differences: United States, United Kingdom and Germany

The study identifies clear differences in attitudes and behaviors related to file sharing and collaboration tools among respondents in the United States (US), United Kingdom (UK) and Germany. As shown in Figure 17, German respondents are less concerned than US or UK respondents about the potential for security breaches in their SharePoint environment, regardless of whether the source of the breach is internal or external to their organization.

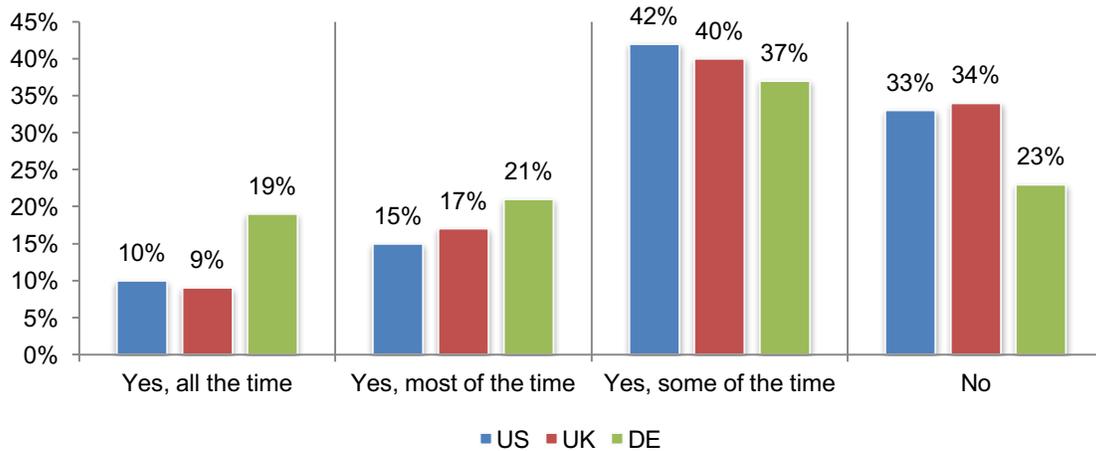
Figure 17. With respect to security in the SharePoint environment, what worries you the most?

Three choices permitted



As shown in Figure 18, German respondents are most likely to believe they have the capabilities to detect SharePoint-related data breach. These results are similar to other studies conducted by Ponemon Institute in Germany. Based on research, German organizations tend to be more aware of security risks and compliance issues than their counterparts in the US. In addition, IT security practitioners in Germany have more confidence in their ability to reduce security threats.

Figure 18. If your organization had a data breach involving the loss or theft of confidential information in the SharePoint environment, would you be able to detect it?



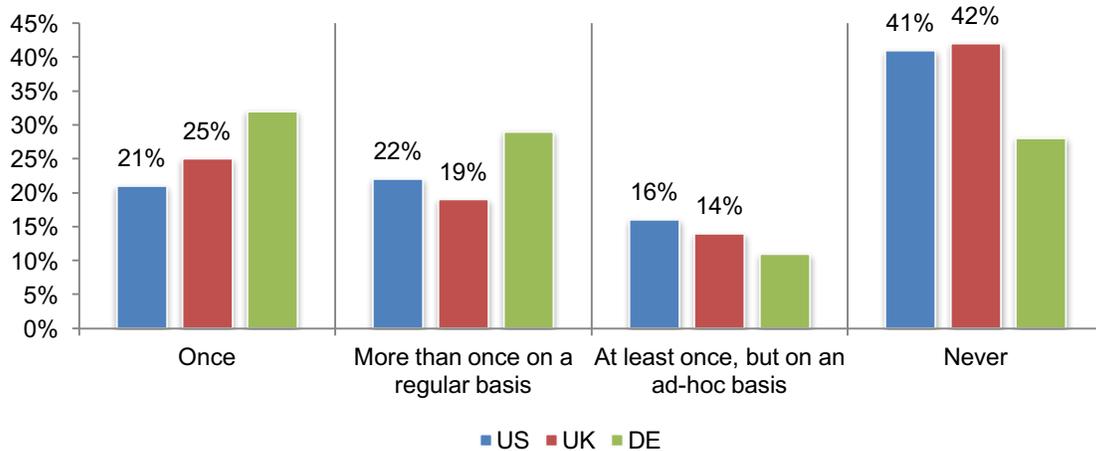
What makes German organizations more confident?

Based on the research, German organizations are leaders in three areas when it comes to the protection of sensitive or confidential information: audits and training to support good governance, centralized ownership and effective technology.

Audits and training to support good governance

As shown in Figure 19, 72 percent of German respondents say their organization conducts audits to see if content-related activities in SharePoint are in compliance with policies, laws and regulations, compared with 59 percent of respondents in the US and 58 percent in the UK.

Figure 19. How often does your organization conduct audits to ensure content activities are in compliance with policies, laws and regulations?

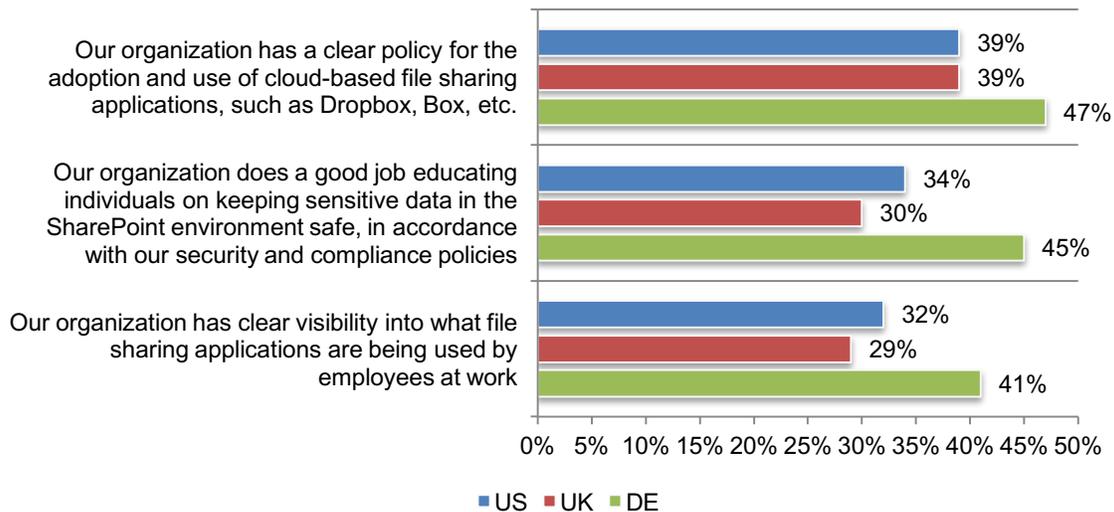


According to Figure 20, 47 percent of German respondents say their organizations have clear policies for the adoption and use of cloud-based file-sharing applications, compared with 39 percent of respondents in the US and UK. As a result, German respondents say they have much more visibility into the file sharing applications employees use (41 percent of respondents) compared to US and UK respondents (32 percent and 29 percent of respondents, respectively).

German respondents also report they are more likely to have effective training programs on secure content practices. Forty-five percent of German respondents say their organizations are effective at training SharePoint users to interact with content appropriately, compared to 34 percent of US respondents and only 30 percent of UK respondents.

Figure 20. Perceptions about training SharePoint users

Strongly agree and Agree responses combined

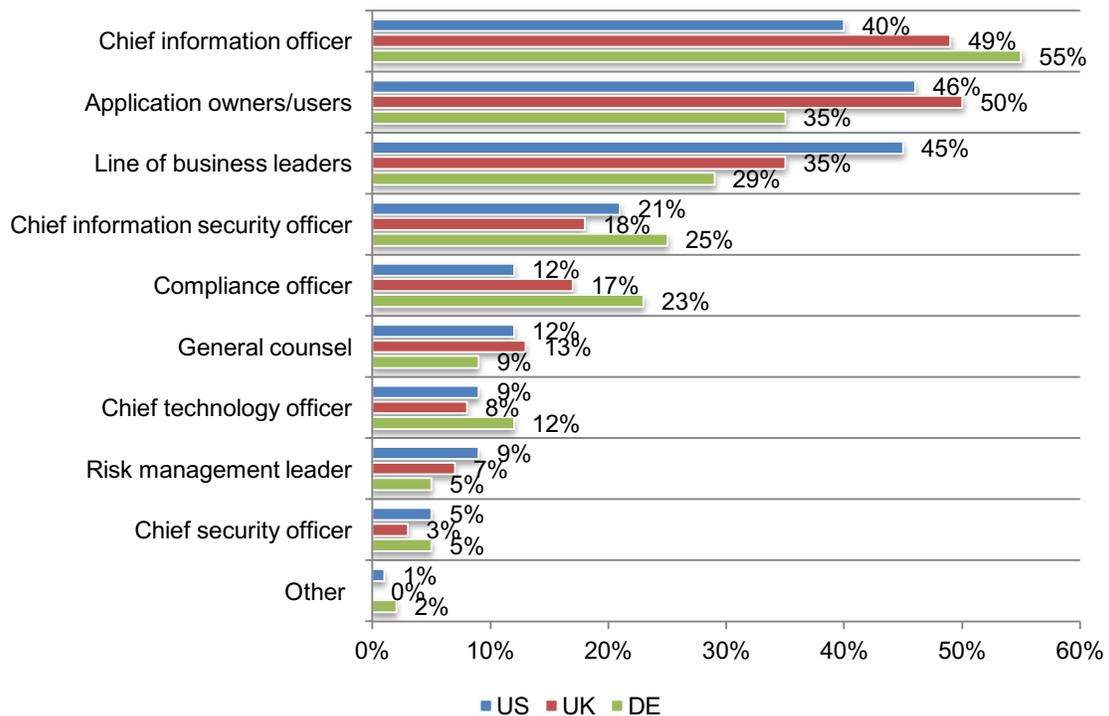


Centralized ownership

It is important to note that among German respondents the ultimate responsibility for the safe use of sensitive or confidential information assets in SharePoint is likely to fall under the chief information security officer, chief technology officer or chief information officer, as shown in Figure 21.

In contrast, based on US and UK responses, organizations in these countries appear to have a more decentralized responsibility for SharePoint security, giving line of business owners and application owners a large portion of control and ownership.

Figure 21. Who has ultimate responsibility for the safe use of sensitive or confidential information assets in the SharePoint environment?

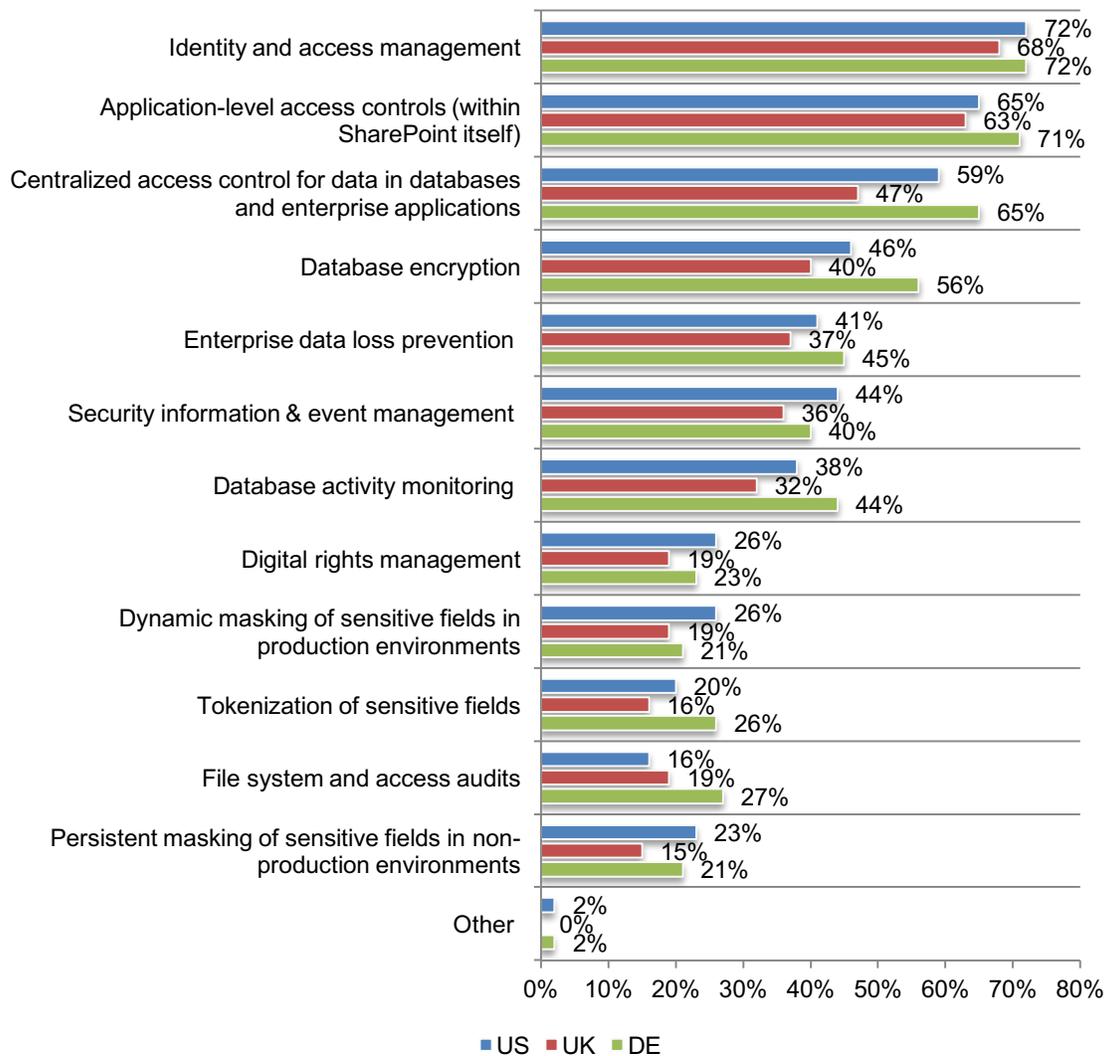


Effective technology

When it comes to solutions that keep sensitive information in SharePoint secure, German respondents say their organizations are much more likely to believe that the tools they use are at least somewhat effective (58 percent of respondents) compared with the US (49 percent of respondents) or the UK (44 percent of respondents).

As shown in Figure 22, 71 percent of German respondents say their organizations use application-level access controls, compared with 65 percent of respondents in the US and 63 percent of respondents in the UK. In addition, 27 percent of German respondents say they employ file system and access audits, compared with only 16 percent of respondents and 19 percent of respondents in the US and UK, respectively.

Figure 22. What technologies or tools does your organization have in place to support the safe use of sensitive or confidential information assets in the SharePoint environment?
More than one permitted



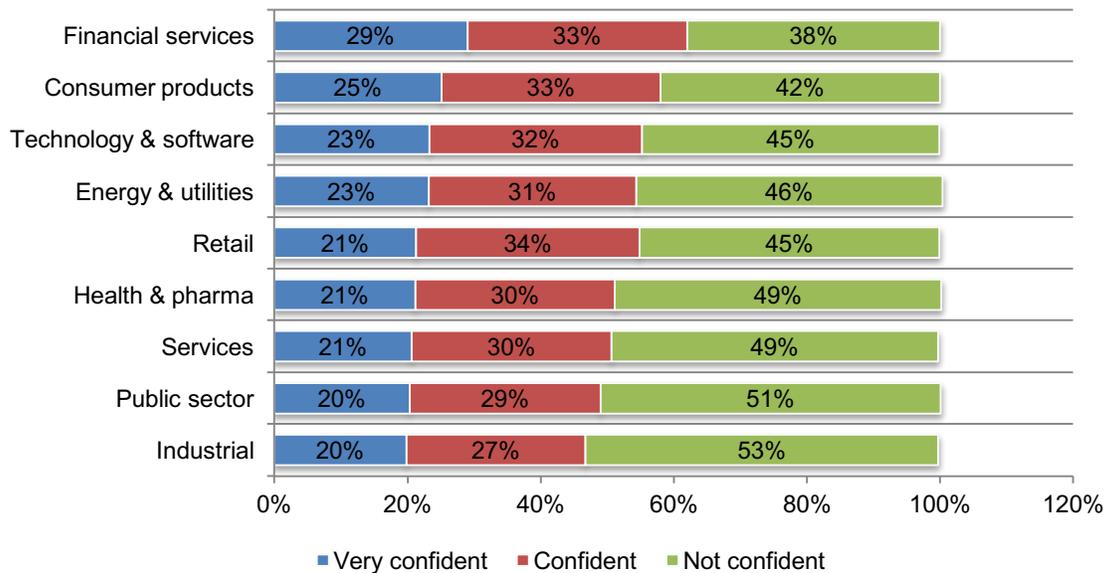
6. Industry differences

In addition to differences among respondents in the different countries represented in this research, we provide an analysis of respondents in nine different industries in the study. Two industries of particular interest are financial services and health and pharma.

Consistent with previous studies conducted by Ponemon Institute, financial services seems to be most effective in dealing with security vulnerabilities. Awareness of information security concerns is consistently high in the financial services industry. A possible reason is the myriad of compliance requirements also requires financial services companies to invest in security tools and develop governance processes at a higher rate than other industries. Typically, financial services companies employ a larger security team with a more diverse set of skills.

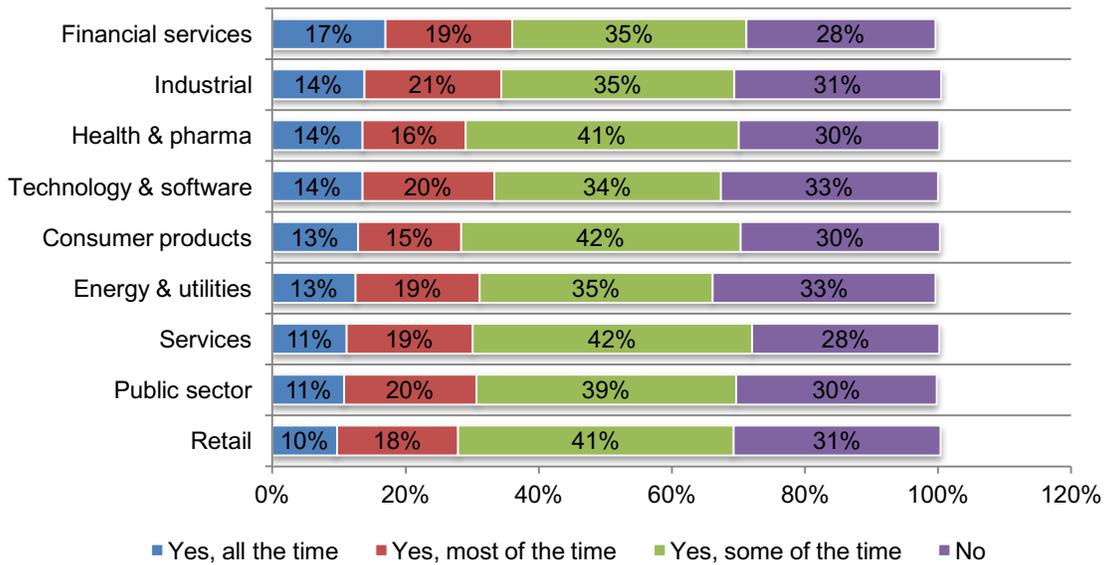
According to Figure 23, 29 percent of respondents in financial services companies are very confident that they have visibility into users' access to sensitive or confidential information assets in the SharePoint environment. This is in contrast to 21 percent of respondents in healthcare who are very confident.

Figure 23. How confident are you that your organization has visibility into users' access to sensitive or confidential information assets in the SharePoint environment?



While respondents in all industries do not believe they are able all or most of the time to detect a data breach involving the loss or theft of confidential information in the SharePoint environment, respondents in financial services are slightly more confident, as shown in Figure 24.

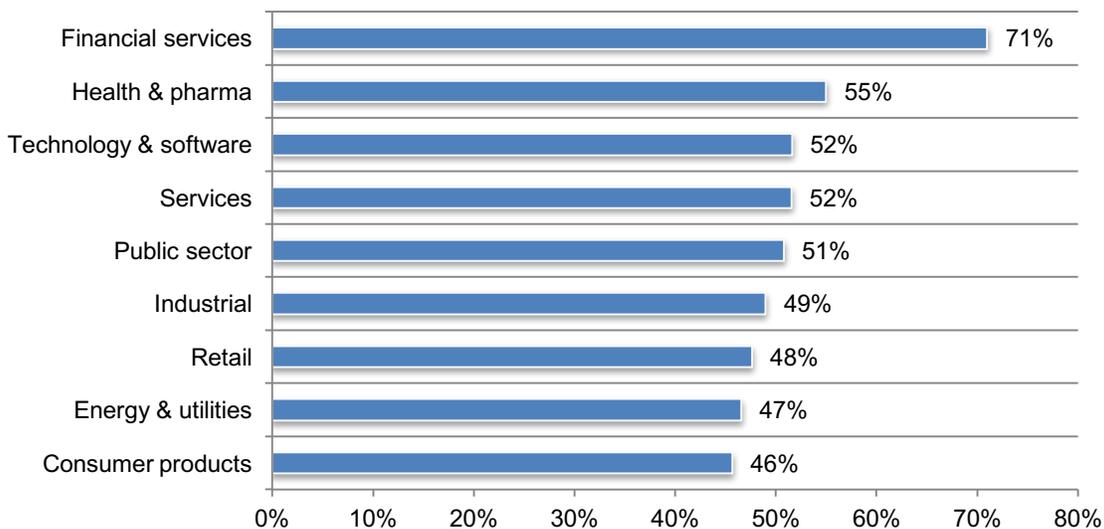
Figure 24. If your organization had a data breach involving the loss or theft of confidential information in the SharePoint environment, would you be able to detect it?



As shown in Figure 25, financial services are far more confident they have effective tools in place to support the safe use of sensitive or confidential information assets in SharePoint. Respondents in energy & utilities and consumer products are far less likely to believe their tools are effective.

Figure 25. How effective are the tools you have in place to support the safe use of sensitive or confidential information assets in SharePoint?

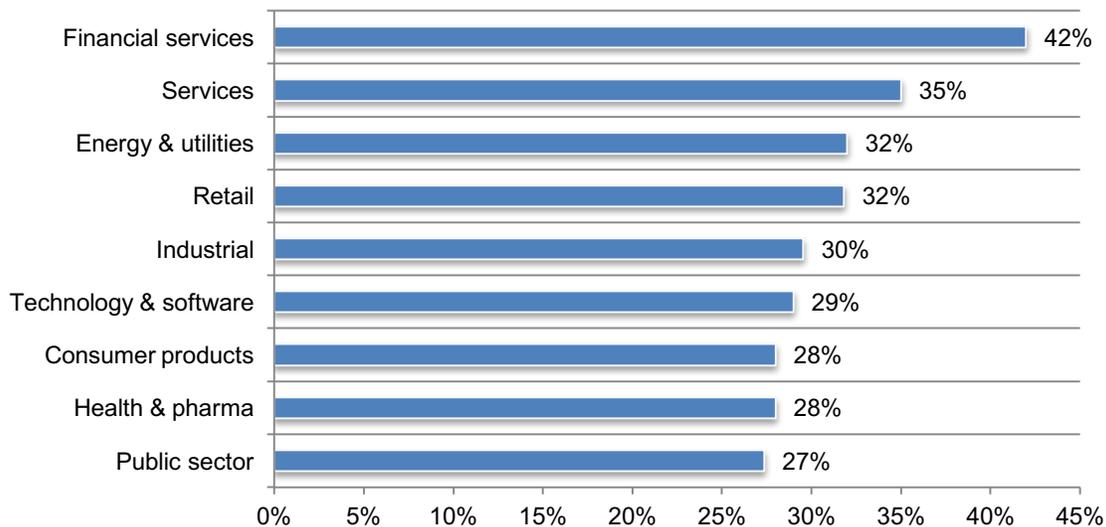
Very effective and Somewhat effective responses combined



Once again, as shown in Figure 26, financial services are most likely to believe they are highly effective in keeping confidential documents secure in the SharePoint environment. Respondents in Health and pharma and public sector are less likely to believe their organizations are highly effective in the security of SharePoint.

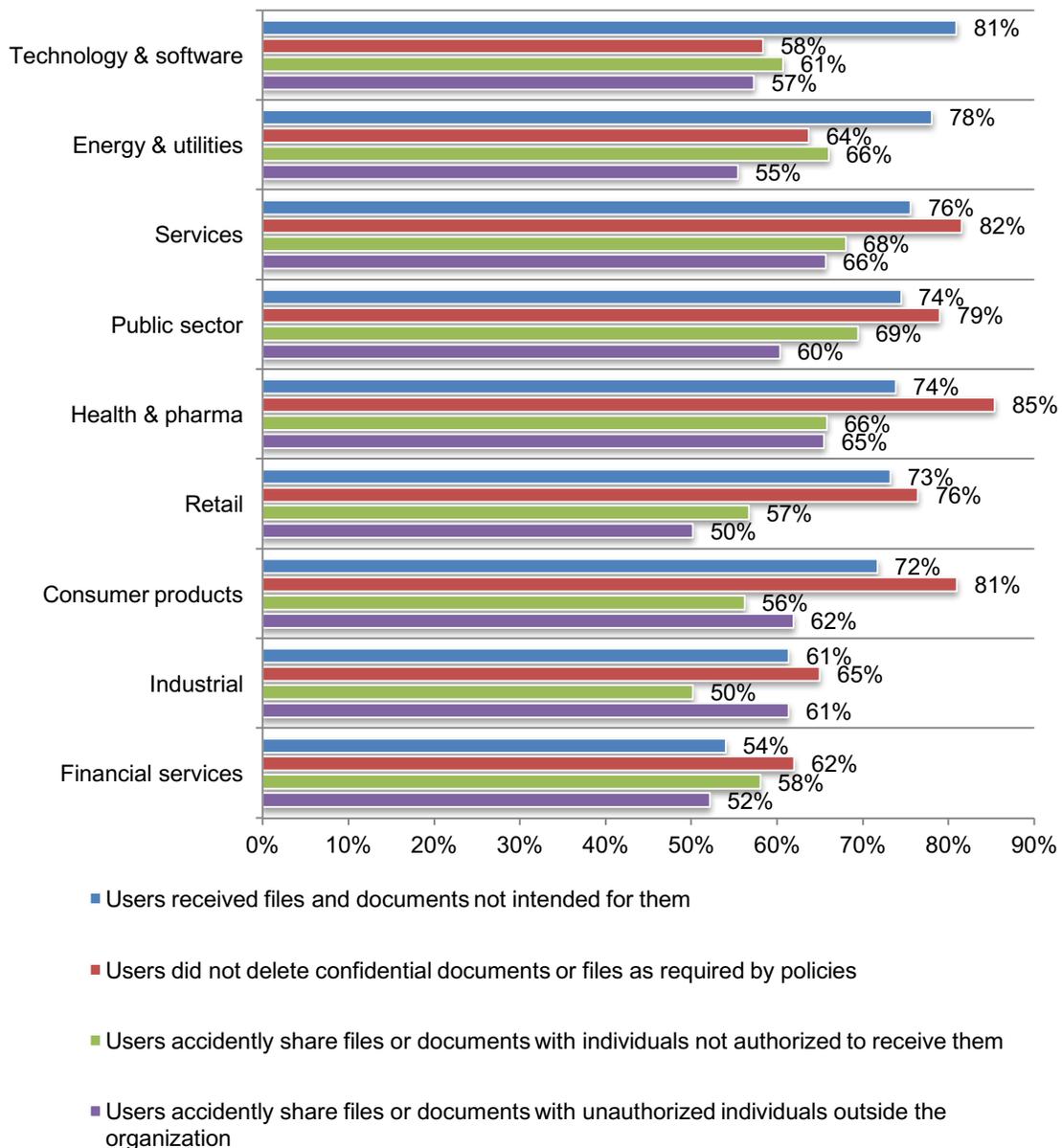
Figure 26. How would you rate your organization’s effectiveness in keeping confidential documents secure in the SharePoint environment?

1 = not effective to 10 = very effective, 7 + responses combined.



As shown in Figure 27, all industries struggle with employees who are careless and often circumvent policies in their use of SharePoint. However, the industries where employee negligence is most evident are: technology & software (81 percent of respondents say users received documents and files not intended for them); health & pharma (85 percent of respondents say users did not delete confidential documents as required by policies); public sector (69 percent of respondents say users shared confidential documents with individuals not authorized to receive them) and services (66 percent of respondents say users accidentally shared files or document with unauthorized individual outside the organization). Consistent with other findings, financial services is much better at mitigating the risk of employee negligence.

Figure 27. How frequently are users engaging in negligent behavior in the workplace?
Very Frequently and Frequently responses combined



8. Conclusions and recommendations

Despite evidence of data breaches and the increasing pressure from regulators, customers and shareholders to protect confidential data from accidental exposure, companies in this study do not seem to be taking security in file sharing and collaboration environments as seriously as they should.

Following are recommendations for creating a more secure environment for sensitive content.

- Use automated tools to improve the organization's ability to discover where sensitive or confidential information resides within SharePoint, file sharing and collaboration tools.
- Instead of relying upon document owners to classify sensitive or confidential information, use automated tools to improve the ability to secure data in the SharePoint environment. Assign centralized accountability and responsibility for securing documents and files containing confidential information to the department with the necessary expertise, such as IT security.
- Be aware that personnel and organizational changes can trigger security vulnerabilities. According to respondents, negligent or malicious behaviors can occur when employees leave the organization or there is downsizing. Consider the use of automated user access history with real time monitoring.
- Conduct meaningful training programs that specifically address the consequences of negligent or careless file sharing practices. These types of behaviors include keeping documents or files no longer needed, receiving and not deleting files and documents not intended for the recipient, forwarding confidential files or documents to individuals not authorized to receive them, using personal or unauthorized file sharing apps to exchange confidential documents and files in the workplace and sending confidential files or documents to unauthorized individuals outside the organization.
- Address the risks created by third parties, contractors and temporary workers by monitoring and restricting their access to sensitive or confidential information.
- Have policies that restrict or limit the sharing of confidential documents and enforce those policies, especially to reduce the risks associated with allowing workers to have confidential information on their home computers and devices.
- Conduct audits to determine the security vulnerabilities and non-compliance of the sharing and accessing practices of employees and third parties. The research proves the ability of such audits to reveal security vulnerabilities in the protection of confidential documents and files.

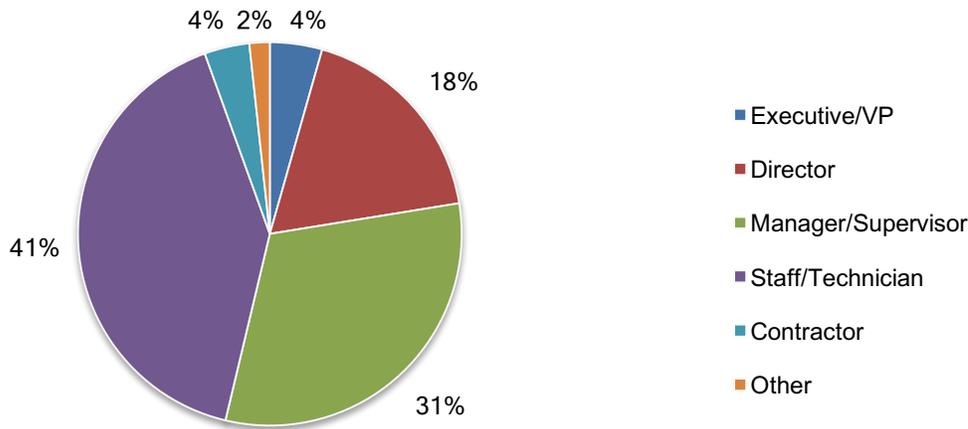
Part 3. Methods

A sampling frame of 44,841 individuals in the United States, United Kingdom and Germany who are involved in the protection of confidential information were selected as participants in the research. Table 1 shows 1,551 total returns. Screening and reliability checks required the removal of 148 surveys. Our final sample consisted of 1,403 surveys, or a 3.1 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	44,841	100%
Total returns	1,551	3.5%
Rejected or screened surveys	148	0.3%
Final sample	1,403	3.1%

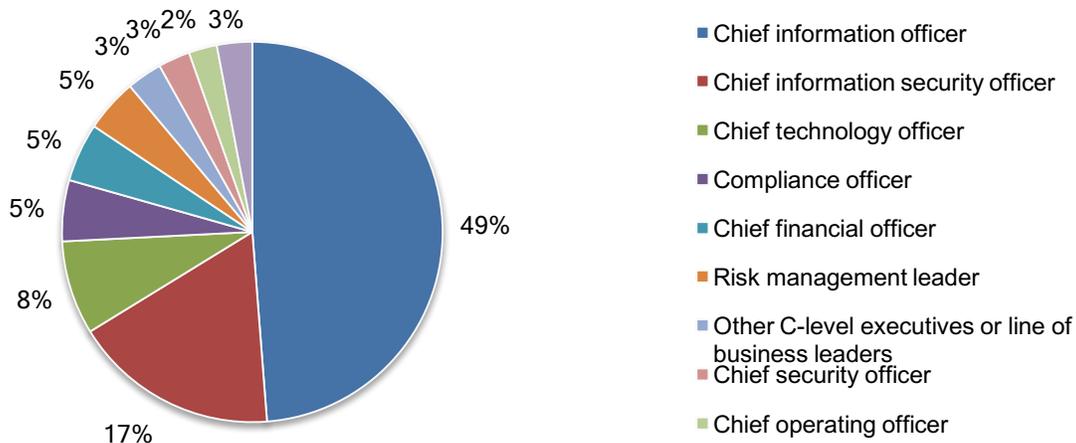
Pie Chart 1 reports the respondent’s organizational level within participating organizations. By design, more than half of the respondents (53 percent) are at or above the supervisory levels.

Pie Chart 1. Position level within the organization



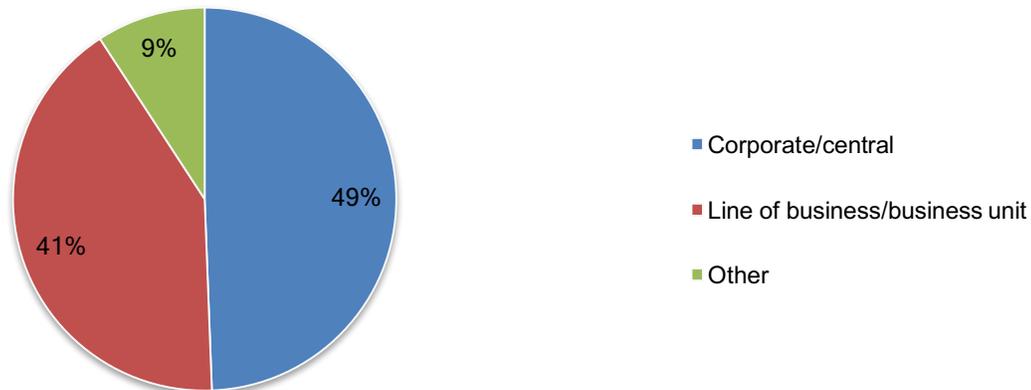
As shown in Pie Chart 2, 49 percent of respondents report directly to the chief information officer and 17 percent report to the chief information security officer.

Pie Chart 2. The primary person reported to within the organization



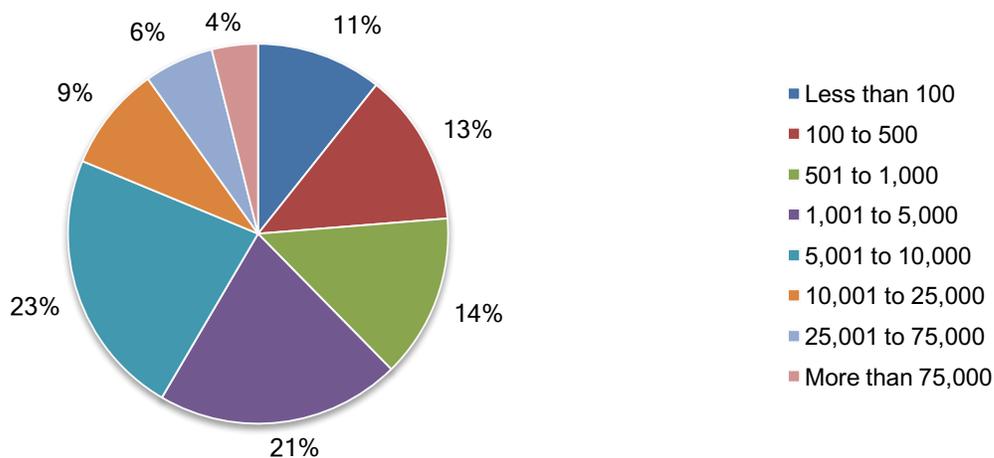
Almost half of respondents (49 percent) described the scope of their job or role as corporate or central within the organization and 41 percent indicated line of business, as shown in Pie Chart 3.

Pie Chart 3. The scope of job or role within the organization



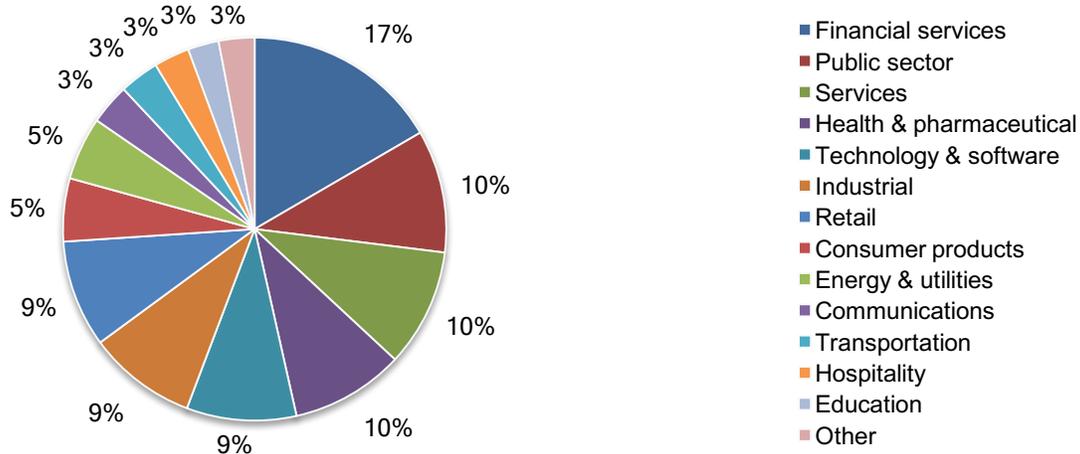
Sixty-two percent of the respondents are from organizations with a global headcount of more than 1,000 employees, as shown in Pie Chart 4.

Pie Chart 4. Worldwide headcount of the organization



Pie Chart 5 reports the industry classification of respondents' organizations. This chart identifies financial services (17 percent of respondents) as the largest segment, followed by public sector (10 percent of respondents), services and health and pharmaceutical (both at 10 percent of respondents).

Pie Chart 5. Primary industry classification



Part 4. Caveats to this study

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 involved in the protection of confidential information. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide 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 between February 1, 2017 and February 10, 2017.

Survey response	US	UK	DE	Combined
Total sampling frame	17,673	13,118	14,050	44,841
Total returns	628	453	470	1,551
Rejected surveys	60	45	43	148
Final sample	568	408	427	1,403
Response rate	3.2%	3.1%	3.0%	3.1%
Sample weights	0.40	0.29	0.30	1.00

Part 1. Screening

S1. Which of the following solutions does your organization use for sharing confidential documents and files among employees and, possibly, third parties? Please select all that apply.	US	UK	DE	Combined
Microsoft SharePoint (proceed)	100%	100%	100%	100%
Office 365	67%	59%	56%	61%
Cloud-based services such as Dropbox and/or Box	54%	43%	39%	46%
Shared network drives	45%	50%	54%	49%
Other file sync and share solutions	38%	34%	35%	36%
We don't use any content management solution (Stop)	0%	0%	0%	0%

S2. What best defines your role in protecting confidential information in the SharePoint environment?	US	UK	DE	Combined
I am fully responsible for ensuring the protection of confidential information	31%	28%	25%	28%
I am partially responsible for ensuring the protection of confidential information	69%	72%	75%	72%
I am not responsible for ensuring the protection of confidential information (Stop)	0%	0%	0%	0%
Total	100%	100%	100%	100%

S3. What percentage of your job function relates to the protection of information, such as documents and other content assets in SharePoint?	US	UK	DE	Combined
Zero (stop)	0%	0%	0%	0%
Less than 5%	6%	11%	4%	7%
5 to 10%	18%	16%	20%	18%
11 to 25%	33%	40%	29%	34%
26 to 50%	24%	21%	34%	26%
51 to 75%	14%	12%	11%	13%
76 to 100%	5%	0%	2%	3%
Total	100%	100%	100%	100%
Extrapolated value	30%	24%	28%	28%

Part 2. Background

Q1. What percentage of your organization's SharePoint deployment is located in the cloud, either by housing SharePoint in the cloud or using SharePoint Online?	US	UK	DE	Combined
Zero	30%	38%	40%	35%
Less than 5%	3%	8%	6%	5%
5 to 10%	6%	9%	4%	6%
11 to 25%	11%	10%	7%	9%
26 to 50%	13%	12%	18%	14%
51 to 75%	14%	12%	11%	13%
76 to 100%	23%	11%	14%	17%
Total	100%	100%	100%	100%
Extrapolated value	37%	24%	28%	30%

Q2. With respect to security in the SharePoint environment, what worries you the most? Please select your top three choices.	US	UK	DE	Combined
External hackers	31%	30%	23%	28%
Malicious employees	21%	19%	15%	19%
Broken security management processes	43%	47%	55%	48%
Employees accidentally exposing information	78%	70%	69%	73%
Temporary workers, contractors or third parties accessing data they should not see	86%	88%	79%	84%
Non-compliance with laws or regulations	39%	45%	57%	46%
Other (please specify)	2%	1%	2%	2%
Total	300%	300%	300%	300%

Q3. Do you know where your organization's sensitive or confidential content is located within SharePoint?	US	UK	DE	Combined
Yes, all content	11%	9%	15%	12%
Yes, most content	19%	21%	23%	21%
Yes, some content	39%	41%	40%	40%
No	31%	29%	22%	28%
Total	100%	100%	100%	100%

Q4. If your organization had a data breach involving the loss or theft of confidential information in the SharePoint environment, would you be able to detect it?	US	UK	DE	Combined
Yes, all the time	10%	9%	19%	12%
Yes, most of the time	15%	17%	21%	17%
Yes, some of the time	42%	40%	37%	40%
No	33%	34%	23%	30%
Total	100%	100%	100%	100%

Part 3. Attributions – Strongly Agree and Agree responses combined	US	UK	DE	Combined
Q5a. Not knowing where my organization's sensitive or confidential information resides represents a significant security risk.	67%	63%	58%	63%
Q5b. In my organization, securing and/or protecting confidential information is a high priority.	50%	51%	59%	53%
Q5c. My organization does a good job of ensuring that SharePoint users interact with confidential or sensitive data appropriately.	37%	39%	48%	41%
Q5d. My organization does a good job of ensuring contractors and third parties interact with confidential or sensitive data appropriately.	34%	33%	40%	36%
Q5e. In my organization, access to sensitive data is controlled by permissions, role, location and/or other factors.	48%	52%	56%	52%
Q5f. Our organization has a clear policy for the adoption and use of cloud-based file sharing applications, such as Dropbox, Box, etc.	39%	39%	47%	41%
Q5g. Our organization has clear visibility into what file sharing applications are being used by employees at work.	32%	29%	41%	34%
Q5h. Our organization does a good job educating individuals on keeping sensitive data in the SharePoint environment safe, in accordance with our security and compliance policies.	34%	30%	45%	36%

Part 4. Issues

Q6. In the context of data loss or theft, what types of confidential information do you consider to be most at risk in your organization? Top two choices.	US	UK	DE	Combined
Customer PII	61%	56%	51%	57%
Employee PII	34%	43%	48%	41%
Analytics (algorithms and models)	11%	9%	11%	10%
Finance and accounting	18%	16%	15%	17%
Payment data (i.e. credit card number)	20%	18%	16%	18%
Intellectual property	53%	56%	59%	56%
Other (please specify)	3%	2%	0%	2%
Total	200%	200%	200%	200%

Q7. What percentage of your organization's data within SharePoint is considered sensitive or confidential?	US	UK	DE	Combined
Less than 10%	5%	3%	0%	3%
10 to 25%	8%	11%	10%	9%
26 to 50%	38%	43%	33%	38%
51 to 75%	32%	29%	39%	33%
76 to 100%	17%	14%	18%	16%
Total	100%	100%	100%	100%
Extrapolated value	51%	49%	55%	52%

Q8. What percentage of your organization's employees use SharePoint to store, edit or share content in the normal course of business?	US	UK	DE	Combined
Less than 10%	15%	20%	13%	16%
10 to 25%	34%	40%	30%	35%
26 to 50%	26%	25%	30%	27%
51 to 75%	18%	11%	18%	16%
76 to 100%	7%	4%	9%	7%
Total	100%	100%	100%	100%
Extrapolated value	34%	28%	37%	33%

Q9. What percentage of your organization's content containing sensitive or confidential information is shared with third parties?	US	UK	DE	Combined
Less than 10%	12%	14%	26%	17%
10 to 25%	16%	26%	35%	25%
26 to 50%	35%	27%	24%	29%
51 to 75%	27%	25%	12%	22%
76 to 100%	10%	8%	3%	7%
Total	100%	100%	100%	100%
Extrapolated value	43%	38%	27%	36%

Q10. Who within your organization has ultimate responsibility for the safe use of sensitive or confidential information assets in the SharePoint environment? Note that we are asking about responsibility for <u>both</u> the tool and the behavior of users. Please check only two responses.	US	UK	DE	Combined
Chief information security officer	21%	18%	25%	21%
Chief security officer	5%	3%	5%	4%
Chief information officer	40%	49%	55%	47%
Chief technology officer	9%	8%	12%	10%
General counsel	12%	13%	9%	11%
Compliance officer	12%	17%	23%	17%
Risk management leader	9%	7%	5%	7%
Line of business leaders	45%	35%	29%	37%
Application owners/users	46%	50%	35%	44%
Other (please specify)	1%	0%	2%	1%
Total	200%	200%	200%	200%

Q11. What technologies or tools does your organization have in place to support the safe use of sensitive or confidential information assets in the SharePoint environment? Please check all that apply.	US	UK	DE	Combined
Application-level access controls (within SharePoint itself)	65%	63%	71%	66%
Centralized access control for data in databases and enterprise applications	59%	47%	65%	57%
Enterprise data loss prevention (DLP)	41%	37%	45%	41%
Database activity monitoring (DAM)	38%	32%	44%	38%
Database encryption	46%	40%	56%	47%
Digital rights management	26%	19%	23%	23%
Dynamic masking of sensitive fields in production environments	26%	19%	21%	22%
File system and access audits	16%	19%	27%	20%
Identity and access management	72%	68%	72%	71%
Persistent masking of sensitive fields in non-prod environments	23%	15%	21%	20%
Security information & event management (SIEM)	44%	36%	40%	40%
Tokenization of sensitive fields	20%	16%	26%	21%
Other (please specify)	2%	0%	2%	1%
Total	478%	411%	513%	469%

Q12. How effective are the tools you have in place to support the safe use of sensitive or confidential information assets in SharePoint?	US	UK	DE	Combined
Very effective	21%	19%	25%	22%
Somewhat effective	28%	25%	33%	29%
Not effective	41%	44%	36%	40%
Not sure	10%	12%	6%	9%
Total	100%	100%	100%	100%

Q13. What challenges do you face when relying on tools to support the safe use of sensitive or confidential information assets in SharePoint? Please select all that apply.	US	UK	DE	Combined
Inaccuracies (data and applications)	34%	29%	21%	29%
Not integrated with SharePoint	65%	62%	54%	61%
Difficult to configure	39%	43%	35%	39%
Slows down the system	23%	27%	19%	23%
Difficult to scale as SharePoint grows	23%	25%	26%	24%
Frustrated users turn to other solutions	56%	63%	50%	56%
No challenges (none of the above)	23%	26%	25%	24%
Total	263%	275%	230%	256%

Q14. How confident are you that your organization has visibility into users' access to sensitive or confidential information assets in the SharePoint environment?	US	UK	DE	Combined
Very confident	20%	21%	25%	22%
Confident	30%	28%	31%	30%
Not confident	50%	51%	44%	48%
Total	100%	100%	100%	100%

Q15. How confident are you that your organization has visibility into users' access to sensitive or confidential information assets in the file share / network drive environment?	US	UK	DE	Combined
Very confident	20%	18%	27%	22%
Confident	28%	30%	33%	30%
Not confident	52%	52%	40%	48%
Total	100%	100%	100%	100%

Q17a. Does your organization currently use any automated tools to discover how sensitive or confidential information in the SharePoint environment is being used?	US	UK	DE	Combined
Yes	31%	25%	27%	28%
No	69%	75%	73%	72%
Total	100%	100%	100%	100%

Q17b. If no, do you believe using any automated tools for discovering the location of sensitive or confidential information would increase the effectiveness of security activities in the SharePoint environment?	US	UK	DE	Combined
Yes	71%	65%	63%	67%
No	29%	35%	37%	33%
Total	100%	100%	100%	100%

Q18a. Did your organization experience a data breach resulting from the loss or theft of confidential information in the SharePoint environment in the past 24-month period?	US	UK	DE	Combined
Yes, only one incident	23%	18%	19%	20%
Yes, two to five incidents	25%	23%	22%	24%
Yes, more than five incidents	8%	4%	2%	5%
I am not aware of one, but it likely occurred	23%	23%	21%	22%
No (skip to Q19)	21%	32%	36%	29%
Total	100%	100%	100%	100%

Q18b. If yes, do you believe this breach incident would have been avoided if your organization had more effective data loss protection technologies in place?	US	UK	DE	Combined
Very likely	34%	33%	28%	32%
Likely	30%	29%	33%	31%
Not likely	15%	18%	20%	17%
No chance	21%	20%	19%	20%
Total	100%	100%	100%	100%

Q18c. If yes, do you believe this breach incident would have been avoided if your organization had a larger budget or spending level?	US	UK	DE	Combined
Very likely	26%	22%	19%	23%
Likely	34%	32%	29%	32%
Not likely	29%	33%	40%	34%
No chance	11%	13%	12%	12%
Total	100%	100%	100%	100%

Q18d. If yes, do you believe this breach incident would have been avoided if your organization had more skilled personnel with data security responsibilities?	US	UK	DE	Combined
Very likely	31%	25%	16%	25%
Likely	30%	30%	26%	29%
Not likely	27%	30%	45%	33%
No chance	12%	15%	13%	13%
Total	100%	100%	100%	100%

Q19. What actions do you plan to take in the next 12 months to better protect sensitive data in SharePoint? Please select all that apply.	US	UK	DE	Combined
Invest in additional security tools such as data loss prevention	53%	35%	41%	44%
Improve secure management of SharePoint	44%	43%	37%	42%
Education for SharePoint users	67%	55%	63%	62%
SharePoint security audits	33%	45%	51%	42%
None (no action taken)	21%	19%	12%	18%
Total	218%	197%	204%	208%

Q20. When do you think sensitive or confidential data is at risk from negligent employee behavior?	US	UK	DE	Combined
Just after employees begin working for the organization (on-boarding)	21%	26%	34%	26%
During a merger, acquisition or reorganization	11%	12%	13%	12%
During a downsizing	31%	28%	28%	29%
When an employee leaves the company	37%	34%	25%	32%
Total	100%	100%	100%	100%

Q21. If you had the following capabilities, do you believe you would improve your organization's information security posture in the SharePoint environment? Please respond to each capability using the scale provided below the item. Significant Improvement and Improvement responses combined.	US	UK	DE	Combined
Q21a. Automated discovery of sensitive or confidential information	77%	74%	68%	73%
Q21b. Automated classification of sensitive or confidential information	75%	71%	63%	70%
Q21c. Automated user access history with real time monitoring	68%	68%	65%	67%
Q21d. Aggregated view across geography and business units	70%	71%	62%	68%
Q21e. DLP solutions designed explicitly for the SharePoint environment	68%	66%	59%	65%
Q21f. Technology diagnostics (including vulnerability assessment tools)	65%	60%	55%	61%
Q21g. Policy workflow automation for sensitive or confidential information	60%	56%	61%	59%

Q22. How frequently do the following incidents happen among users (knowledge workers) in the SharePoint environment? Very Frequently and Frequently responses combined.	US	UK	DE	Combined
Q22a. Users received files and documents not intended for them.	70%	67%	63%	67%
Q22b. Users did not delete confidential documents or files as required by policies.	75%	72%	69%	72%
Q22c. Users accidentally share files or documents with individuals not authorized to receive them.	69%	63%	62%	65%
Q22d. Users accidentally share files or documents with unauthorized individuals outside the organization.	65%	68%	55%	63%

Q23. With respect to classifying documents by level of security, how is file-level confidentiality determined in the SharePoint environment? Please select all that apply.	US	UK	DE	Combined
Data type – PII, PHI, etc.	51%	45%	55%	50%
Data usage (size limits, large downloads)	29%	33%	28%	30%
Technology usage (e.g., by type of mobile device)	37%	35%	35%	36%
Location of users	28%	31%	23%	27%
Document owners	56%	49%	59%	55%
Who has access to the document	44%	45%	40%	43%
User behaviors	38%	28%	23%	31%
We do not determine document and file-level confidentiality	34%	31%	29%	32%
Other (please specify)	14%	18%	11%	14%
Total	331%	315%	303%	318%

Q24. How would you rate your organization's effectiveness in keeping confidential documents secure in the SharePoint environment? Please use the following 10-point scale from 1 = not effective to 10 = very effective.	US	UK	DE	Combined
1 or 2	13%	17%	8%	13%
3 or 4	26%	19%	11%	19%
5 or 6	39%	45%	38%	40%
7 or 8	10%	13%	26%	16%
9 or 10	12%	6%	17%	12%
Total	100%	100%	100%	100%
Extrapolated value	5.14	4.94	6.16	5.39

Q25. In the past 12 months, how often did your organization conduct audits or assessments to determine if content activities in the SharePoint environment are in compliance with policies, laws and regulations?	US	UK	DE	Combined
Once	21%	25%	32%	26%
More than once on a regular basis	22%	19%	29%	23%
At least once, but on an ad-hoc basis	16%	14%	11%	14%
Never	41%	42%	28%	37%
Total	100%	100%	100%	100%

Part 5. Demographics

D1. What best describes your position level within the organization?	US	UK	DE	Combined
Executive/VP	5%	4%	4%	4%
Director	21%	15%	17%	18%
Manager/Supervisor	31%	33%	30%	31%
Staff/Technician	36%	43%	45%	41%
Contractor	5%	4%	2%	4%
Other (please specify)	2%	1%	2%	2%
Total	100%	100%	100%	100%

D2. Who do you or your immediate supervisor(s) report to within the organization?	US	UK	DE	Combined
CEO/executive committee	2%	0%	1%	1%
Chief operating officer	3%	2%	2%	2%
Chief financial officer	5%	6%	4%	5%
Chief information security officer	19%	18%	15%	17%
Chief security officer	3%	2%	3%	3%
Chief information officer	45%	53%	50%	49%
Chief technology officer	8%	9%	7%	8%
General counsel	2%	0%	0%	1%
Compliance officer	4%	5%	7%	5%
Risk management leader	6%	3%	4%	5%
Other C-level executives or line of business leaders	3%	2%	4%	3%
Other (please specify)	0%	0%	3%	1%
Total	100%	100%	100%	100%

D3. What best describes the scope of your job or role?	US	UK	DE	Combined
Corporate/central	44%	50%	56%	49%
Line of business/business unit	45%	41%	37%	41%
Other (please specify)	11%	9%	7%	9%
Total	100%	100%	100%	100%

D4. What range best describes the full-time headcount of your global organization?	US	UK	DE	Combined
Less than 100	8%	12%	13%	11%
100 to 500	11%	18%	11%	13%
501 to 1,000	16%	12%	13%	14%
1,001 to 5,000	19%	21%	23%	21%
5,001 to 10,000	21%	23%	25%	23%
10,001 to 25,000	11%	7%	8%	9%
25,001 to 75,000	8%	5%	4%	6%
More than 75,000	6%	2%	3%	4%
Total	100%	100%	100%	100%

D5. What best describes your organization's primary industry classification?	US	UK	DE	Combined
Agriculture & food services	1%	0%	1%	1%
Communications	4%	3%	3%	3%
Consumer products	5%	6%	5%	5%
Defense & aerospace	1%	0%	0%	0%
Education	2%	3%	3%	3%
Energy & utilities	5%	6%	5%	5%
Entertainment & media	2%	1%	1%	1%
Financial services	18%	16%	15%	17%
Health & pharmaceutical	11%	9%	8%	10%
Hospitality	3%	4%	2%	3%
Industrial	7%	9%	12%	9%
Public sector	10%	11%	10%	10%
Retail	9%	10%	8%	9%
Services	9%	10%	11%	10%
Technology & software	8%	9%	11%	9%
Transportation	3%	2%	5%	3%
Other (please specify)	2%	1%	0%	1%
Total	100%	100%	100%	100%

Results for the United States sample						
Q16. Following is a list of data governance tasks for the protection of information assets in the file sharing and collaboration environment. Please rate each task in terms of the current state of deployment within your organization, as follows: 1=task is primarily deployed in the SharePoint environment; 2=task is primarily deployed in other collaboration environments; 3=task is deployed in both SharePoint and other collaboration environments; 4=task is not deployed; 5=Unsure.	Deployed in SharePoint (1)	Deployed in other environments (2)	Both SharePoint and other environments (3)	Task not deployed (4)	Unsure (5)	Total
Tracking where sensitive and confidential data are located	15%	14%	18%	44%	9%	100%
Constructing data architecture - including maps, lineage, flows and inventories	15%	18%	14%	45%	8%	100%
Managing data classification with prioritization	18%	12%	21%	41%	8%	100%
Monitoring access rights or permissions based on job, role, or on a need-to-know-basis	20%	25%	18%	33%	4%	100%
Managing access changes based on changes in policy, user needs or application updates	16%	26%	18%	35%	5%	100%
Revoking data access rights upon an employee's termination or changes in policy	16%	25%	19%	36%	4%	100%
Enforcing data access policies in a consistent fashion across applications, locations, departments, technology standards, etc.	19%	26%	19%	33%	3%	100%
Monitoring data access of privileged users across structured and	13%	15%	12%	54%	6%	100%

unstructured data						
Providing evidence of compliance with policies and regulations	15%	21%	21%	37%	6%	100%
Creating acceptable use policies	18%	22%	21%	32%	7%	100%
Monitoring data transfers to and from third-party locations including cloud	8%	28%	28%	30%	6%	100%
Educating end-users about data access and control policies	11%	30%	28%	26%	5%	100%
Detecting and contain data leakage and theft (data breach)	5%	45%	34%	12%	4%	100%
Implementing and adapting data loss prevention solutions	6%	37%	34%	20%	3%	100%
Protecting sensitive data by encryption and/or tokenization	11%	23%	30%	31%	5%	100%
Protecting sensitive data by masking, data de-identification, data redaction, or data suppression	5%	31%	24%	35%	5%	100%
Providing a comprehensive digital forensics capability	3%	33%	26%	34%	4%	100%

Results for the United Kingdom sample						
Q16. Following is a list of data governance tasks for the protection of information assets in the file sharing and collaboration environment. Please rate each task in terms of the current state of deployment within your organization, as follows: 1=task is primarily deployed in the SharePoint environment; 2=task is primarily deployed in other collaboration environments; 3=task is deployed in both SharePoint and other collaboration environments; 4=task is not deployed; 5=Unsure.	Deployed in SharePoint (1)	Deployed in other environments (2)	Both SharePoint and other environments (3)	Task not deployed (4)	Unsure (5)	Total
Tracking where sensitive and confidential data are located	11%	17%	17%	46%	9%	100%
Constructing data architecture - including maps, lineage, flows and inventories	17%	14%	15%	46%	8%	100%
Managing data classification with prioritization	17%	15%	19%	40%	9%	100%
Monitoring access rights or permissions based on job, role, or on a need-to-know-basis	20%	19%	16%	41%	4%	100%
Managing access changes based on changes in policy, user needs or application updates	17%	27%	17%	34%	5%	100%
Revoking data access rights upon an employee's termination or changes in policy	15%	23%	15%	42%	5%	100%
Enforcing data access policies in a consistent fashion across applications, locations, departments, technology standards, etc.	18%	26%	23%	30%	3%	100%
Monitoring data access of privileged users across structured and unstructured data	11%	19%	13%	51%	6%	100%

Providing evidence of compliance with policies and regulations	19%	17%	21%	36%	7%	100%
Creating acceptable use policies	18%	25%	16%	33%	8%	100%
Monitoring data transfers to and from third-party locations including cloud	8%	33%	25%	29%	5%	100%
Educating end-users about data access and control policies	11%	28%	29%	27%	5%	100%
Detecting and contain data leakage and theft (data breach)	4%	37%	35%	20%	4%	100%
Implementing and adapting data loss prevention solutions	6%	32%	32%	28%	2%	100%
Protecting sensitive data by encryption and/or tokenization	12%	23%	35%	36%	4%	110%
Protecting sensitive data by masking, data de-identification, data redaction, or data suppression	5%	30%	24%	36%	5%	100%
Providing a comprehensive digital forensics capability	3%	31%	28%	34%	4%	100%

Results for the German sample						
Q16. Following is a list of data governance tasks for the protection of information assets in the file sharing and collaboration environment. Please rate each task in terms of the current state of deployment within your organization, as follows: 1=task is primarily deployed in the SharePoint environment; 2=task is primarily deployed in other collaboration environments; 3=task is deployed in both SharePoint and other collaboration environments; 4=task is not deployed; 5=Unsure.	Deployed in SharePoint (1)	Deployed in other environments (2)	Both SharePoint and other environments (3)	Task not deployed (4)	Unsure (5)	Total
Tracking where sensitive and confidential data are located	15%	11%	19%	44%	11%	100%
Constructing data architecture - including maps, lineage, flows and inventories	14%	16%	14%	46%	10%	100%
Managing data classification with prioritization	18%	14%	19%	41%	8%	100%
Monitoring access rights or permissions based on job, role, or on a need-to-know-basis	18%	17%	25%	37%	3%	100%
Managing access changes based on changes in policy, user needs or application updates	14%	31%	17%	36%	2%	100%
Revoking data access rights upon an employee's termination or changes in policy	17%	22%	18%	38%	5%	100%
Enforcing data access policies in a consistent fashion across applications, locations, departments, technology standards, etc.	17%	27%	26%	27%	3%	100%
Monitoring data access of privileged users across structured and unstructured data	11%	15%	18%	51%	5%	100%

Providing evidence of compliance with policies and regulations	18%	21%	21%	33%	7%	100%
Creating acceptable use policies	19%	23%	14%	36%	8%	100%
Monitoring data transfers to and from third-party locations including cloud	9%	32%	19%	35%	5%	100%
Educating end-users about data access and control policies	11%	34%	27%	24%	4%	100%
Detecting and contain data leakage and theft (data breach)	4%	33%	30%	30%	3%	100%
Implementing and adapting data loss prevention solutions	7%	38%	29%	24%	2%	100%
Protecting sensitive data by encryption and/or tokenization	12%	24%	32%	27%	5%	100%
Protecting sensitive data by masking, data de-identification, data redaction, or data suppression	6%	25%	25%	39%	5%	100%
Providing a comprehensive digital forensics capability	3%	31%	27%	36%	3%	100%

Results for the Consolidated sample						
Q16. Following is a list of data governance tasks for the protection of information assets in the file sharing and collaboration environment. Please rate each task in terms of the current state of deployment within your organization, as follows: 1=task is primarily deployed in the SharePoint environment; 2=task is primarily deployed in other collaboration environments; 3=task is deployed in both SharePoint and other collaboration environments; 4=task is not deployed; 5=Unsure.	Deployed in SharePoint (1)	Deployed in other environments (2)	Both SharePoint and other environments (3)	Task not deployed (4)	Unsure (5)	Total
Tracking where sensitive and confidential data are located	14%	14%	18%	44%	9%	99%
Constructing data architecture - including maps, lineage, flows and inventories	15%	18%	14%	45%	8%	100%
Managing data classification with prioritization	18%	12%	21%	41%	8%	100%
Monitoring access rights or permissions based on job, role, or on a need-to-know-basis	20%	25%	18%	33%	4%	100%
Managing access changes based on changes in policy, user needs or application updates	16%	26%	18%	35%	5%	100%
Revoking data access rights upon an employee's termination or changes in policy	16%	25%	19%	36%	4%	100%
Enforcing data access policies in a consistent fashion across applications, locations, departments, technology standards, etc.	19%	26%	19%	33%	3%	100%
Monitoring data access of privileged users across structured and unstructured data	13%	15%	12%	54%	6%	100%

Providing evidence of compliance with policies and regulations	15%	21%	21%	37%	6%	100%
Creating acceptable use policies	18%	22%	21%	32%	7%	100%
Monitoring data transfers to and from third-party locations including cloud	8%	28%	28%	30%	6%	100%
Educating end-users about data access and control policies	11%	30%	28%	26%	5%	100%
Detecting and contain data leakage and theft (data breach)	5%	45%	34%	12%	4%	100%
Implementing and adapting data loss prevention solutions	6%	37%	34%	20%	3%	100%
Protecting sensitive data by encryption and/or tokenization	11%	23%	30%	31%	5%	100%
Protecting sensitive data by masking, data de-identification, data redaction, or data suppression	5%	31%	24%	35%	5%	100%
Providing a comprehensive digital forensics capability	3%	33%	26%	34%	4%	100%

Please contact research@ponemon.org or call us at 800.877.3118 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.

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.