Ponemon INSTITUTE

Corporate Data: A Protected Asset or a Ticking Time Bomb?

Sponsored by Varonis

Independently conducted by Ponemon Institute LLC

Publication Date: December 2014

Corporate Data: A Protected Asset or a Ticking Time Bomb?

Ponemon Institute, December 2014

Part 1. Introduction

Companies face the challenge of keeping critical business information secure without compromising the productivity of their employees. And this is only getting more difficult as the proliferation of business data – and our dependence on it – speed along, complicating and even overwhelming organizations' attempts to protect it.

Too often, as revealed in this study, there is a lack of oversight and control over how and who among employees has access to confidential, sensitive information. This information can include customer lists and contact information, intellectual property, and private information about customers, employees and business partners.

Employees, both IT practitioners and end users, are caught in the middle of being charged with safeguarding the company's information assets but also supporting the business goals of an efficient and productive workforce. After years of concentrating on and investing in perimeter security, cyber attacks and data breaches are a greater problem than ever. How much emphasis are companies truly placing on protecting the data itself, and how is the failure to do so making them more vulnerable to a data breach?

Corporate Data: A Protected Asset or a Ticking Time Bomb? is a study sponsored by Varonis, surveying a total of 2,276 employees in US and European organizations (United Kingdom, Germany and France), including 1,110 individuals (hereafter referred to as end users) who work in such areas as sales, finance and accounting, corporate IT, and business operations, and 1,166 individuals who work in IT and IT security (hereafter referred to as IT practitioners).

In the context of this research, both IT practitioners and end users are witnessing a lack of control over their organizations' data and access to it, and the two groups generally concur that their organizations would overlook security risks before they would sacrifice productivity. Employees are often left with needlessly excessive data access privileges and loose data-sharing policies. Compounding the risk, organizations are unable to determine what happened to data when it goes missing, indicating a lack of monitoring and further absence of controls.

This presents a growing risk for organizations due to both accidental and conscious exposure of sensitive or critical data. Efforts to address these risks will need to overcome employee perceptions, as they believe data protection is not considered a high priority by senior leadership.

Following are research findings that illustrate the growing risks and challenges to productivity that data growth and a lack of internal controls currently present for organizations of all sizes:

End users believe they have access to sensitive data they should not be able to see, and more than half say that access is frequent or very frequent. Seventy-one percent of end users say that they have access to company data they should not be able to see. Fifty-four percent characterize that access as frequent or very frequent.

End users believe data protection oversight and controls are weak. Forty-seven percent of end users say the organization does not strictly enforce its policies against the misuse or unauthorized access to company data and 45 percent say they are more careful with company data than their supervisors or managers. Furthermore, only twenty-two percent of employees say their organization is able to tell them what happened to lost data, files or emails.

IT agrees. Most IT practitioners surveyed state that their companies do not enforce a strict least-privilege (or need-to-know) data policy. Four in five IT practitioners (80 percent) say their

organizations don't enforce a strict least-privilege data model. Thirty-four percent say they don't enforce any least-privilege data model.

End users and IT agree that data growth is hindering productivity more every day. Seventy-three percent of end users believe the growth of emails, presentations, multimedia files and other types of company data has very significantly or significantly affected their ability to find and access data.

Uncertainty about whether senior executives view data protection as a priority affects compliance with security policies. Only twenty-two of end users believe their organizations overall place a very high priority on data protection. About half (51 percent) of IT practitioners believe their CEO and other C-level executives consider data protection a high priority.

IT practitioners say end users are likely to put critical data at risk. Seventy-three percent of IT practitioners say their department takes data protection very seriously. However, only 47 percent believe employees in their company take the necessary steps to make sure confidential data is secure. Thus, IT departments know end user security risks exist but think they are limited in what they can do about it.

End users think it is OK to transfer confidential documents to potentially unsecure devices. Seventy-six percent of end users say there are times when it is acceptable to transfer work documents to their personal computer, table, smart phone and even the public cloud. Only 13 percent of IT practitioners agree.

End users and IT practitioners do not think their organization would accept diminished productivity to prevent the risk to critical data. Fifty-five percent of end users say their company's efforts to tighten security have a major impact on their productivity. Only 27 percent of IT practitioners say their organization would accept diminished productivity to prevent the loss or theft of critical data.

End users and IT agree that employees are unknowingly the most likely to be responsible for the leakage of company data. Sixty-four percent of end users and fifty-nine percent of IT practitioners believe that insiders are unknowingly the most likely to be the cause of leakage of company data. And only forty-six percent of IT practitioners say employees in their organizations take appropriate steps to protect the company data they access.

Part 2. Key findings

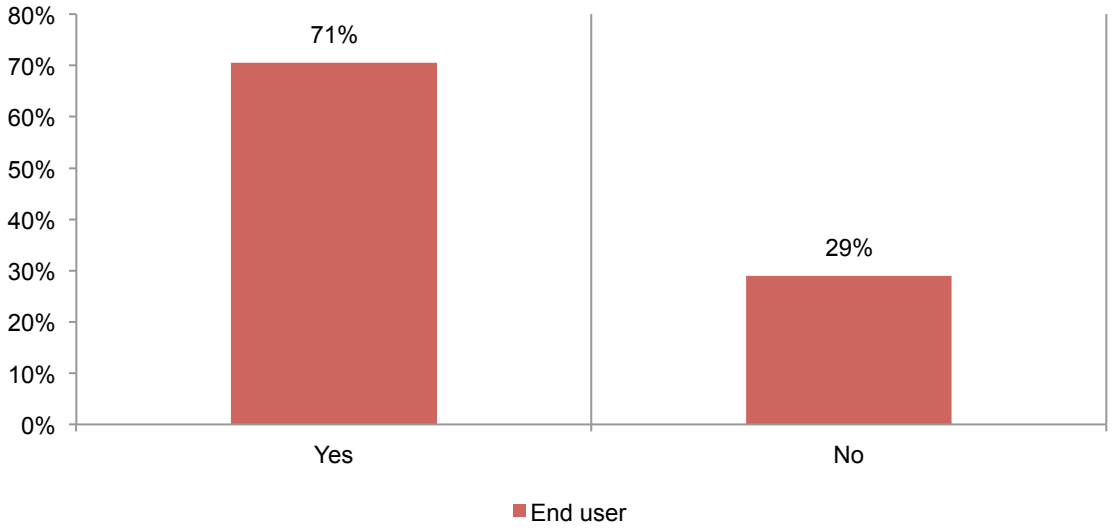
In this section, we present an analysis of the research findings. The complete audited findings are presented in the appendix of this report. We have organized the paper according to the following themes:

- Lack of controls
- Data growth hampering productivity
- Uncovering internal vulnerability

Lack of controls

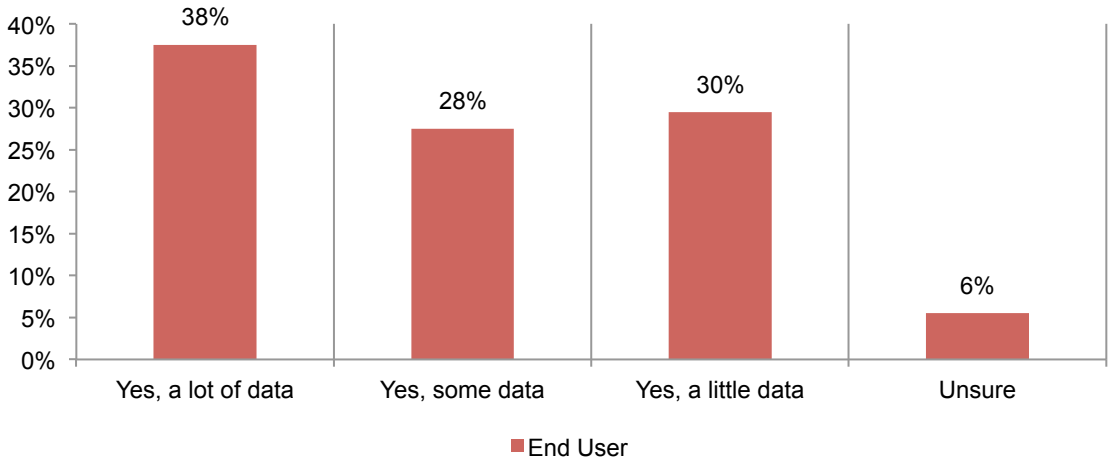
Employees are witnessing a lack of control over file access and use of company data. Despite the plethora of data breaches affecting all companies, IT and end users generally concur that employees have frequent access to a lot of sensitive data they do not need. Organizations are at risk because employees do not have appropriate access privileges. As shown in Figure 1, 71 percent of end users say they have too much access to confidential corporate data. Fifty-four percent say such access happens very frequently or frequently.

Figure 1. Is there company data you have access to that you probably should not see?



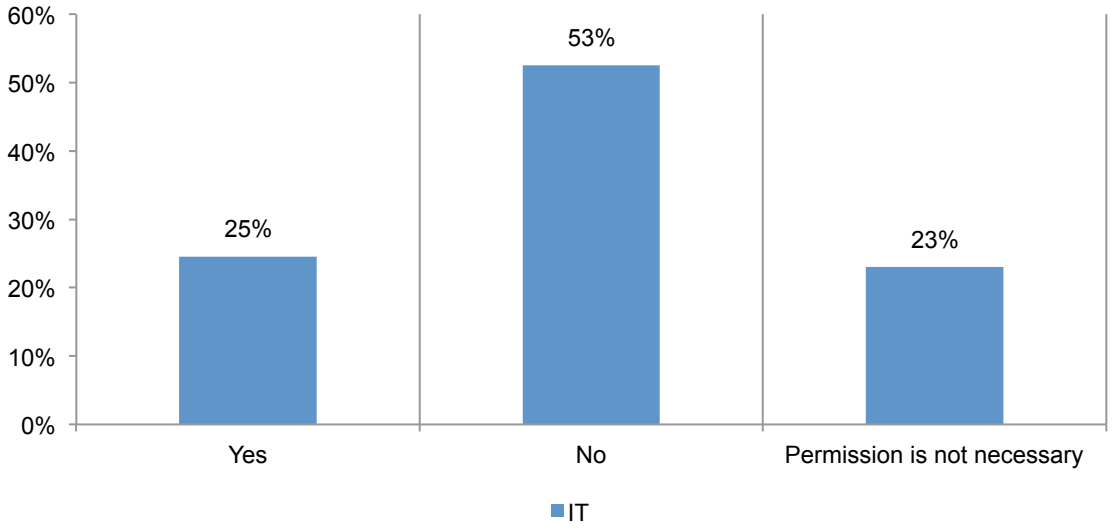
As shown above, 71 percent of end users report they have too much access to confidential company data. Of those respondents, 38 percent say they have seen "a lot of data". Fifty-eight percent say they have seen some or a little confidential data, and 6 percent are unsure.

Figure 2. How much confidential data would you or your co-workers likely see?



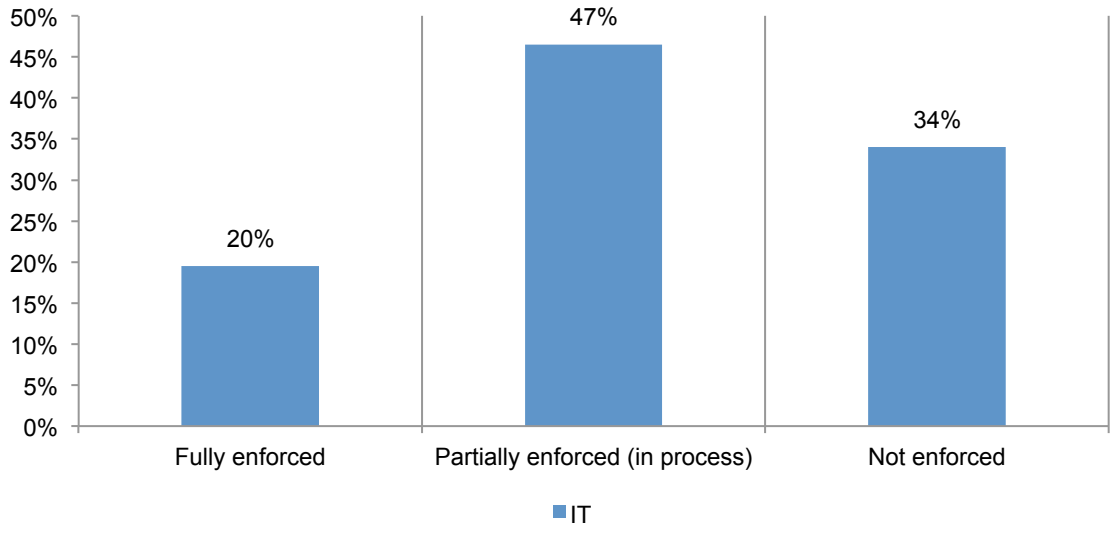
Many organizations allow public cloud file sync services. As shown in Figure 3**,** 48 percent of IT practitioners say their organization either permits employees to use public cloud file sync services (25 percent) or permission is not necessary (23 percent). Fifty-three percent of those organizations that do not permit public cloud file sync services do offer alternative solutions.

Figure 3. Does your organization permit end users to use public cloud file sync services?



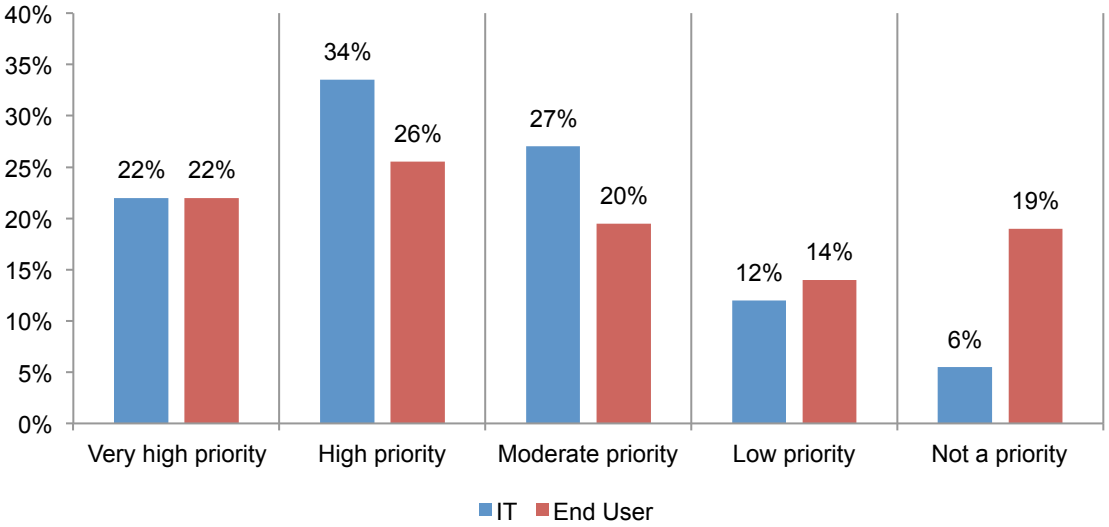
IT practitioners recognize that end users have too much access to company data. As shown in Figure 4, only 20 percent of IT practitioners say their organization enforces a strict least privilege model (i.e. access to company data only on a need to know basis). Thirty-four percent say it is not enforced at all.

Figure 4. Does your organization enforce a strict least privilege model?



Data protection is not perceived as a priority. As shown in Figure 5, only 22 percent of both IT practitioners and employees believe their organization places a very high priority on the protection of company data. However a higher percentage of IT practitioners (34 percent vs. 26 percent) say it is a high priority in their organization. Nineteen percent of end users say data protection is not a priority.

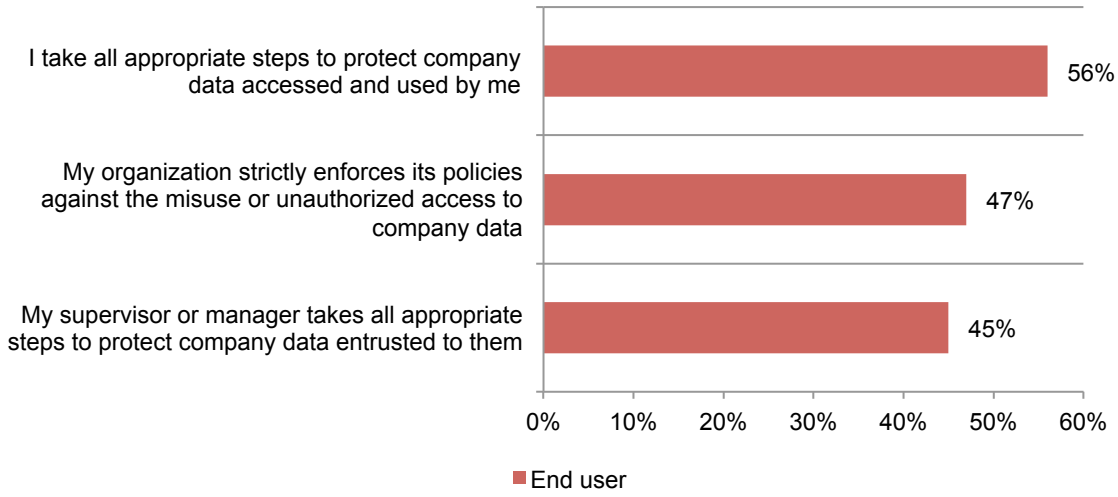
Figure 5. Is the protection of company critical information a priority?



Why is data protection not believed to be a priority? Perhaps it is because leadership is not demonstrating how important it is to protect confidential information. Specifically, as shown in Figure 6, only 47 percent of end users believe their organization strictly enforces its policies against the misuse or unauthorized access to company data.

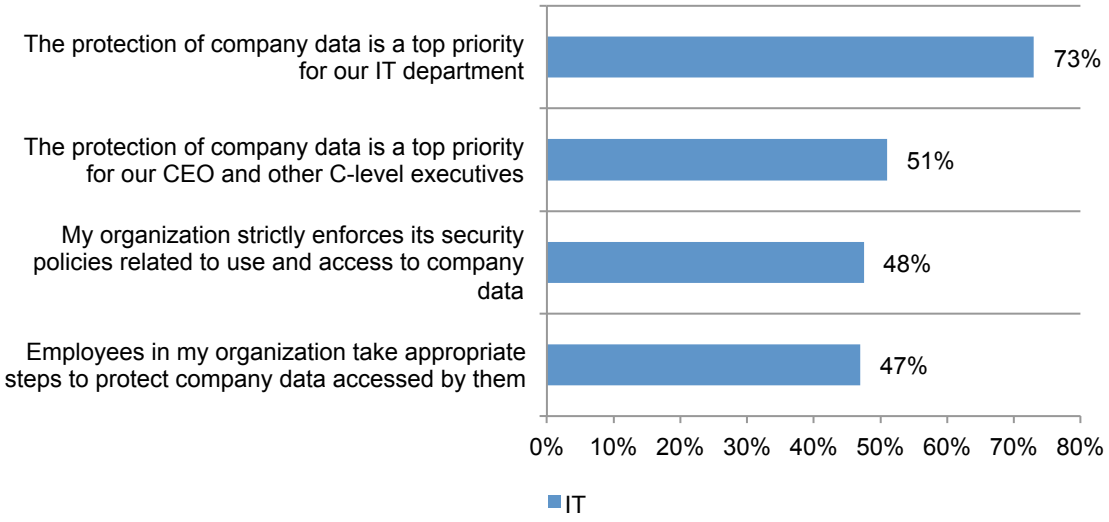
More concerning is that only 45 percent of end users believe their direct supervisor or manager takes all appropriate steps to protect the confidential data entrusted to them. However, end users do think they are doing a good job of protecting data.

Figure 6. What do end users think about their organizations' data protection practices?
Strongly agree and agree response combined



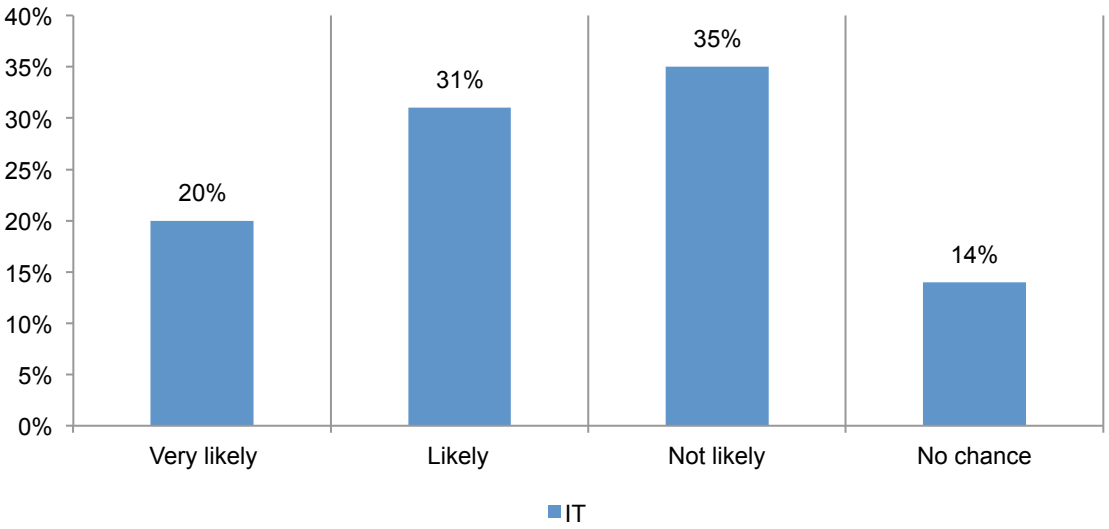
IT does not think their management places a high priority on protecting data. As demonstrated in Figure 7, only 47 percent say employees in their organization take appropriate steps to protect company data accessed by them. As evidence that IT practitioners do not think data protection is a priority, about half (51 percent) say the CEO and other C-level executives make data protection a priority and less than half say there is strict enforcement of security policies related to use and access to company data.

Figure 7. What do IT practitioners think about their organizations' data protection practices? Strongly agree and agree response combined



Organizations lose track of employees' documents, emails or files. Figure 8 reveals that 49 percent of IT practitioners say it is not likely (35 percent) or no chance (14 percent) that when documents, files or emails are lost or change unexpectedly the organization will be able to assess what happened to them. Only 20 percent say it is very likely they would be able to know what happened and if data in these documents is at risk.

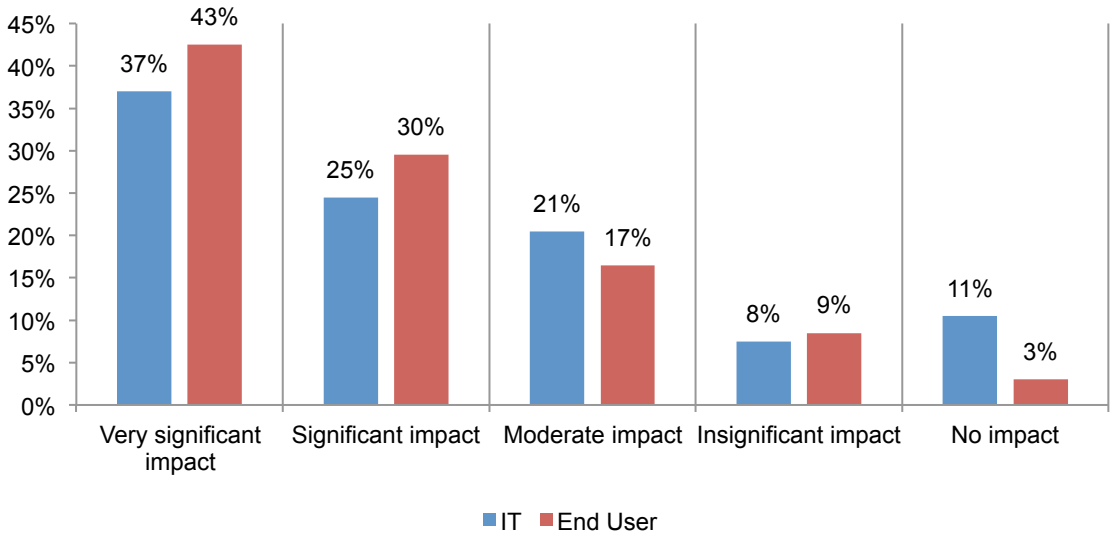
Figure 8. When documents, files or emails get lost or change unexpectedly, will you know what happened to them?



Data growth hampering productivity

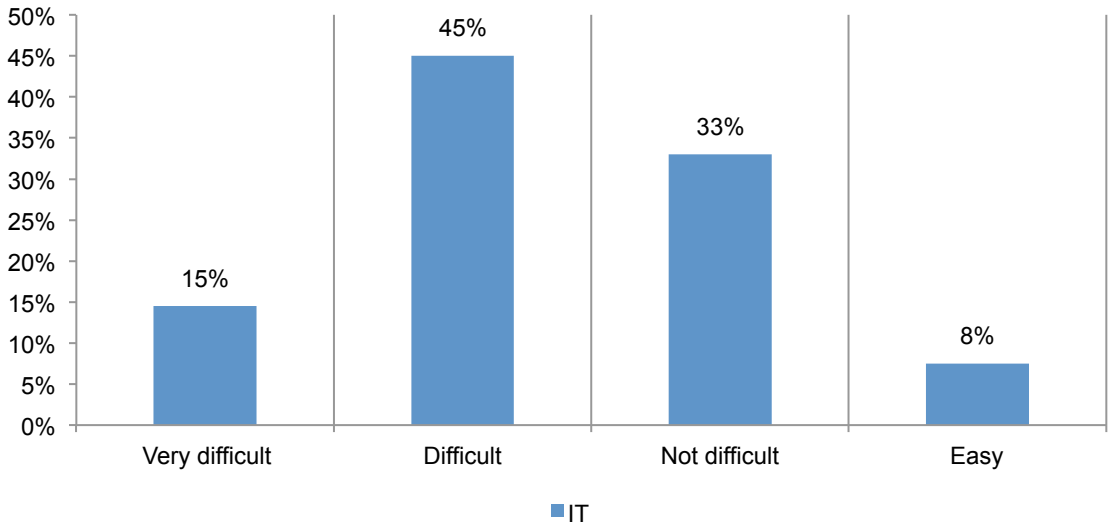
Employees have difficulty finding data they need. Seventy-three percent of employees believe the growth of emails, presentations, multimedia and other types of company data has very significantly (43 percent) or significantly (30 percent) affected their ability to find and access data. Sixty-two percent of IT practitioners (37 percent + 25 percent) believe this is the case, as shown in Figure 9.

Figure 9. Does the growth of emails, presentations, multimedia and other types of company data impact the ability to find and access data?



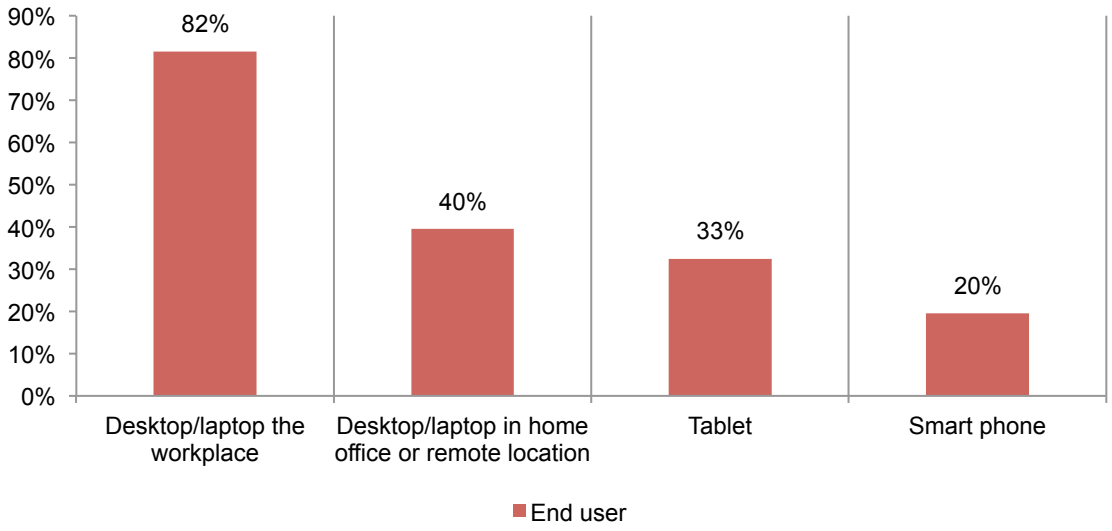
Many IT practitioners agree, as shown in Figure 10. Sixty percent of IT practitioners say it is very difficult (15 percent) or difficult (45 percent) for employees to find company data or files they or their co-workers have created that isn't stored on their computers. Further, only 34 percent of IT practitioners say their organization has a fully deployed internal enterprise search capability so employees can find and retrieve company files. This can explain why employees are reluctant to delete data created in the course of their work because they may never find it again.

Figure 10. How difficult is it for end users to find company data that isn't stored on their individual PC/workstations?



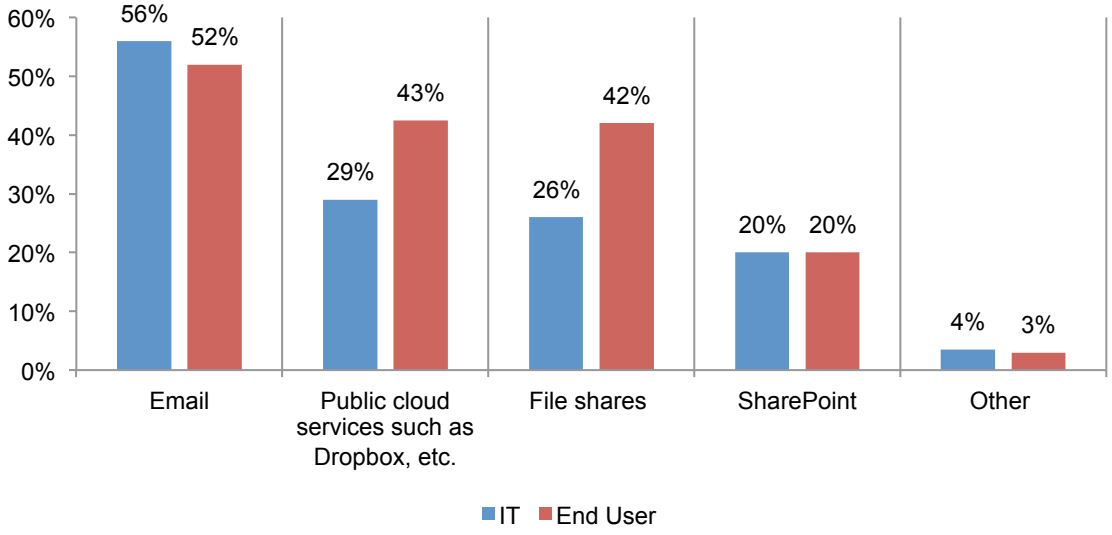
To be productive, end users need to access confidential data routinely. Seventy-six percent of employees say as part of their work they need to access and use proprietary information. As shown in Figure 11, 53 percent of employees say they use tablets (33 percent) or smartphones (20 percent) to access corporate data. Most (82 percent of employees) use desktops or laptops.

Change Figure 11. What devices do you use to access company data?
More than one response permitted



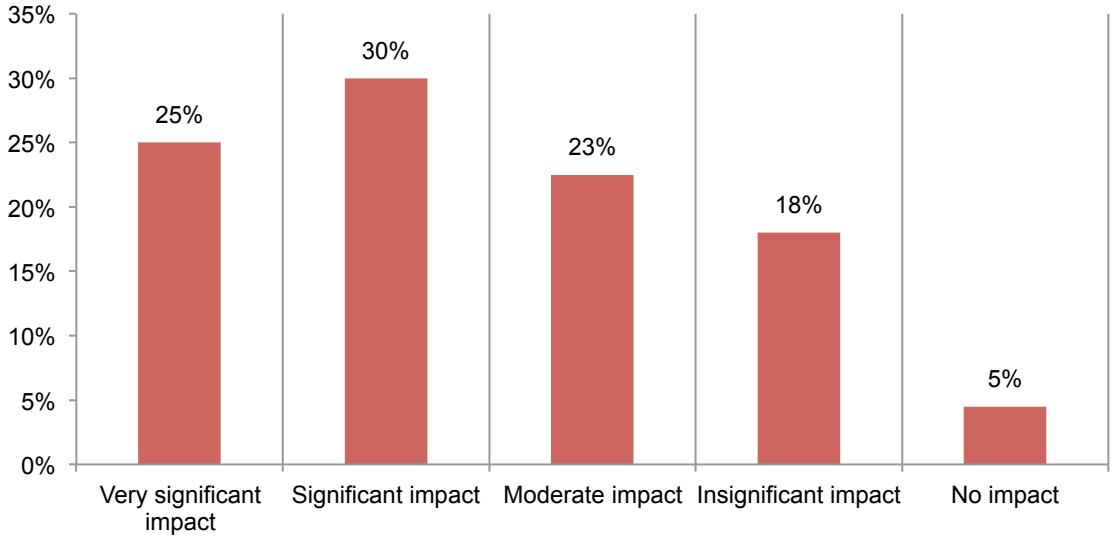
End users choose convenience. The most popular way of sharing company data or files with co-workers is by email. Fifty-six percent of IT practitioners and 52 percent of employees say they prefer email, as shown in Figure 12. Both groups also say it is very difficult or difficult to share company data or files with business partners.

Figure 12. The preferred ways to share company data or files with co-workers
Two responses permitted



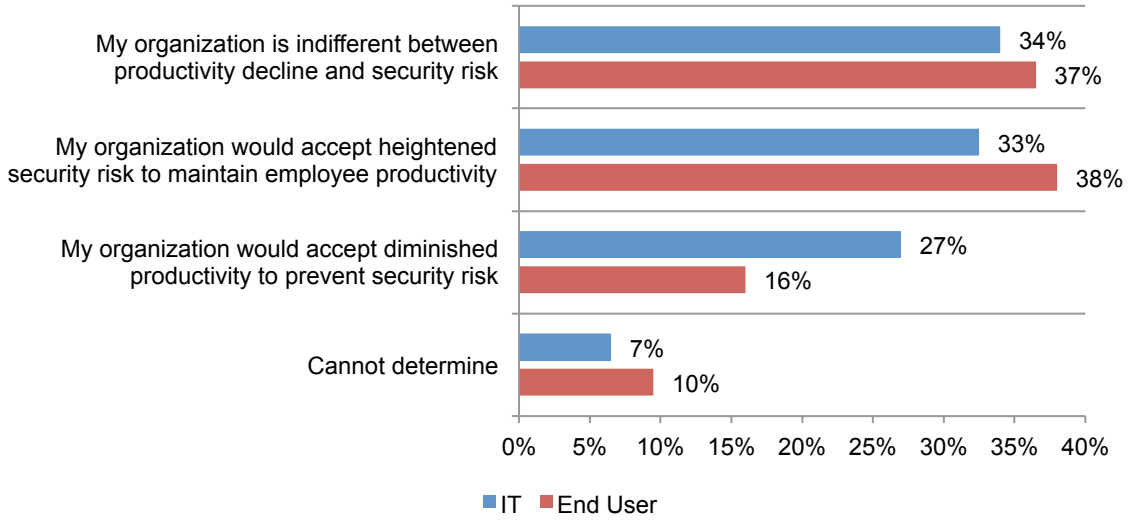
Companies are tightening access to data because of security and employees say it affects productivity. Fifty-two percent of end users say their access to company data is being restricted. As shown in Figure 13, these respondents say it has had a very significant (25 percent) or significant impact (30 percent) on their productivity.

Figure 13. What best defines how tightened security impacts end user job productivity?



Both employees and IT practitioners believe their organizations would tend to overlook security risks in order to maintain productivity. One-third of IT practitioners and 38 percent of end users say in order to maintain productivity their organizations would accept more risk to their corporate data. Only 16 percent of employees and 27 percent of IT practitioners say their management would accept a decline in their productivity to minimize security risks, according to Figure 14.

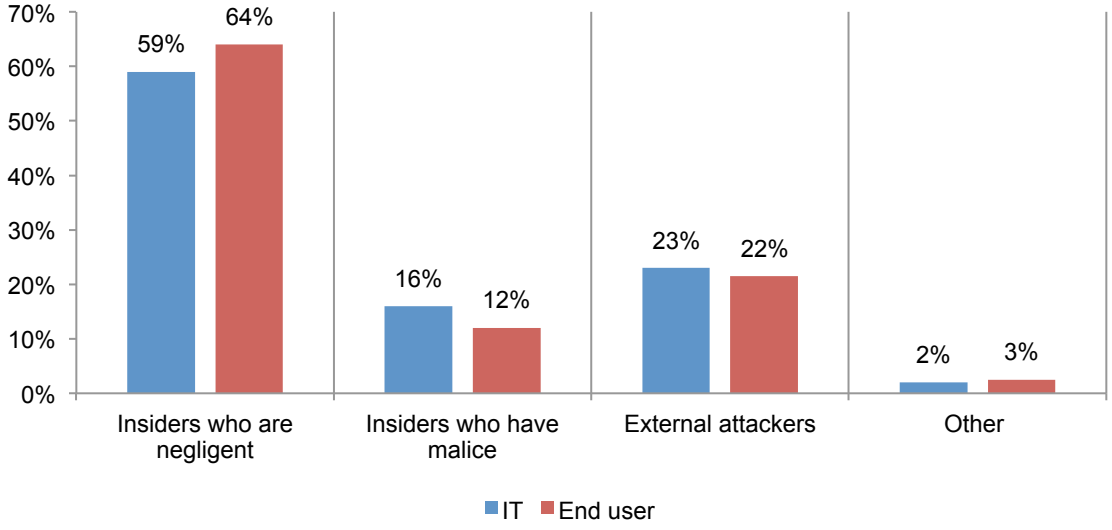
Figure 14. What IT practitioners & end users believe is their organizations' attitude about productivity and security



Uncovering internal vulnerability

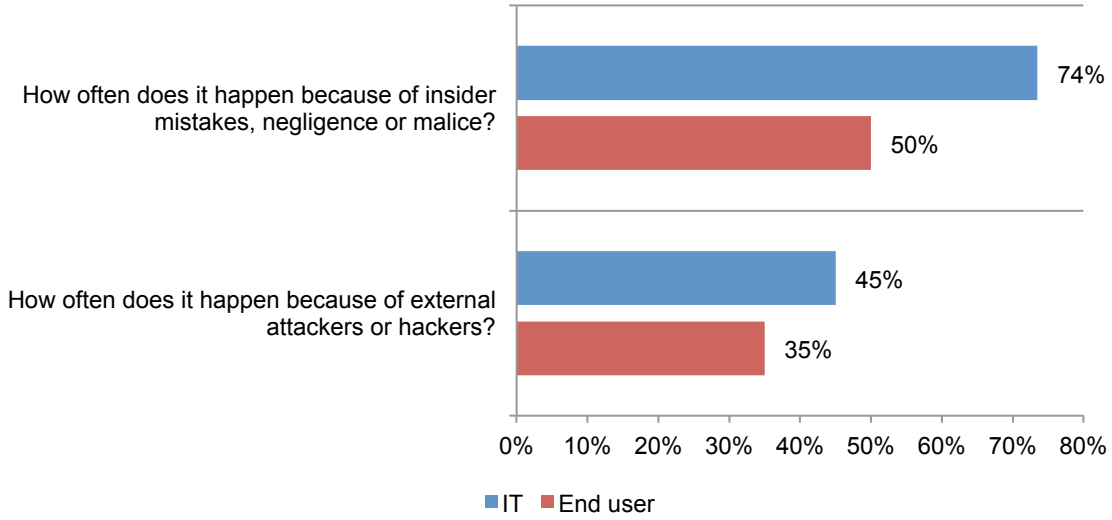
End users and IT practitioners agree that the compromise of insider accounts is likely insiders' fault. As shown in Figure 15, 59 percent of IT practitioners and 64 percent of end users believe the compromise of insider accounts is due to negligent insiders. A smaller percentage of IT practitioners (23 percent) and end users (22 percent) believe external attackers are most likely to cause this type of incident.

Figure 15. Who is most likely to cause the compromise of insider accounts?



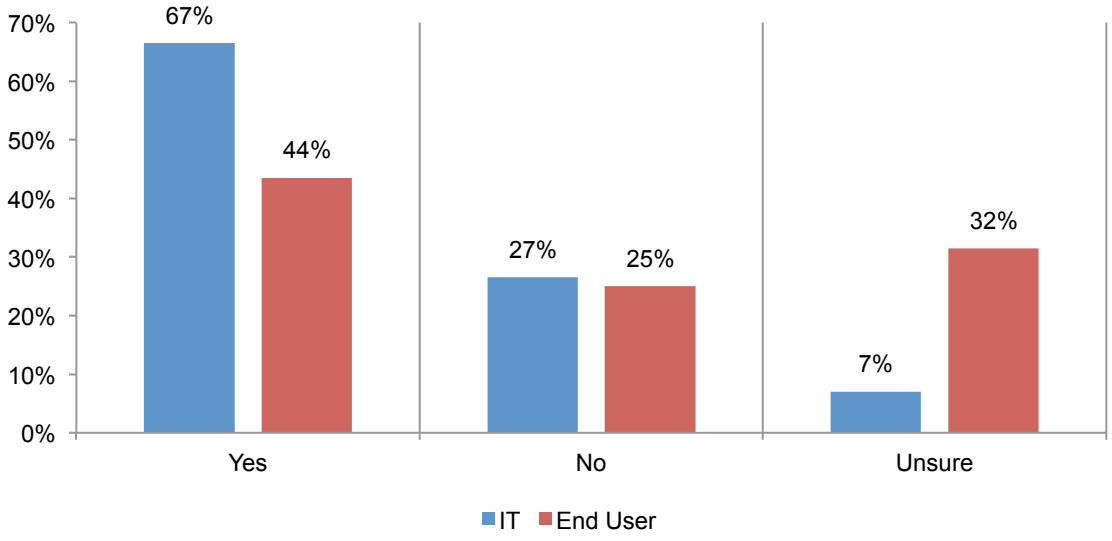
IT practitioners blame data breaches on insiders. As shown in Figure 16, a far greater percentage of IT practitioners (74 percent vs. 50 percent) believe insiders are to blame for the leakage of company data. IT practitioners are also more likely to believe an external attacker was the source of the breach.

Figure 16. When leakage of company data occurs, how often does it happen because of insider mistakes, negligence or malice?
Very frequently and frequently response combined



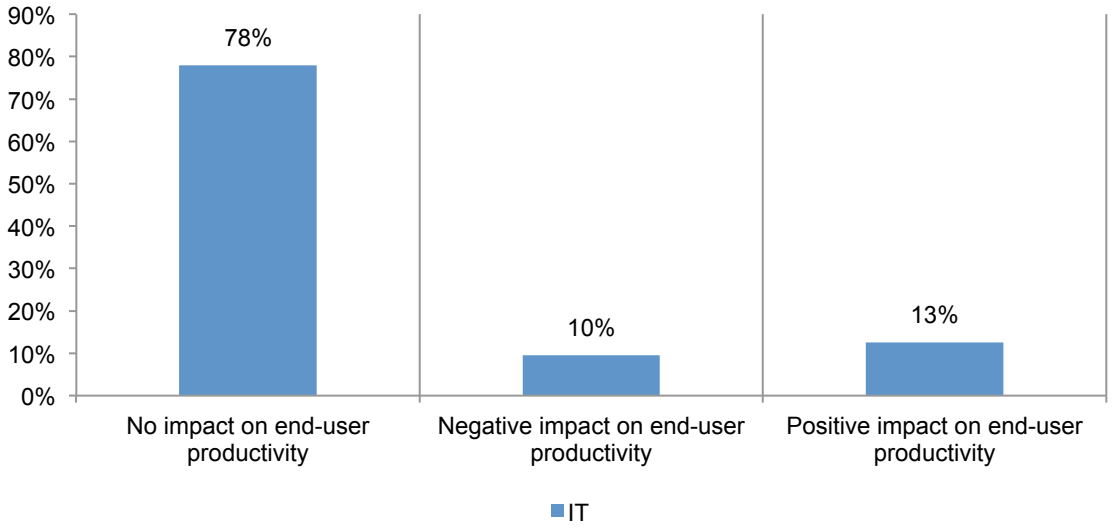
Are end users made aware of data breaches? Key to creating awareness of the importance of data protection is communicating the consequences of the misuse of confidential business information. While 67 percent of IT practitioners say their organization experienced the loss or theft of company data over the past two years, only 44 percent of employees think this has happened, as shown in Figure 17.

Figure 17. Did your organization have a data breach in the past two years?



In the past year, 67 percent of IT practitioners say their organization has tightened access to company data because of security requirements or concerns. Figure 18 reveals that of these respondents, 78 percent say such stricter access has not had an impact on productivity.

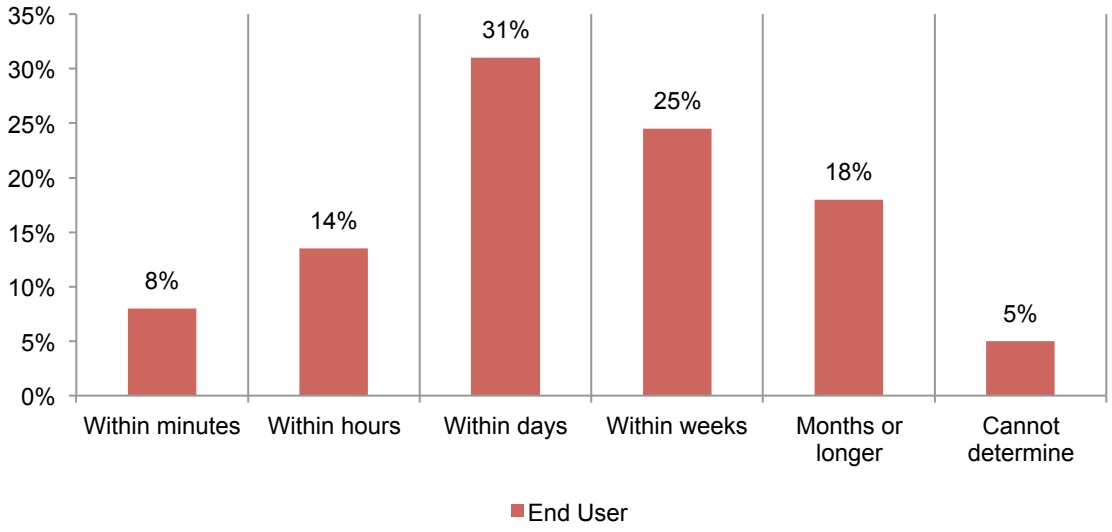
Figure 18. How has tightened security affected end user productivity?



Requests for greater access to company information is time consuming and diminishes productivity. As shown in Figure 19, end users say that if they need to access data they are not allowed to see, it can take weeks (25 percent of end users) or months (18 percent of end users) to have their request approved. Only 22 percent of end users say it is within minutes (8 percent) or hours (14 percent).

Generally it is the employee's supervisor or manager responsible for granting access (50 percent of respondents) followed by the IT department or help desk (20 percent of respondents) or IT security (16 percent of respondents).

Figure 19. How long does it take to gain access to company data?



Part 3. Conclusion

Companies face a significant challenge in keeping critical business information secure without diminishing the productivity of their employees. This is made more difficult because of the proliferation of business data that needs to be protected. The research also reveals there is a lack of oversight and control over who has access to potentially confidential and sensitive company data and how they share that information.

Based on the findings of this research, we have identified six areas that can be improved by having automation and data access policies and procedures that are understood and enforced throughout the organization:

1. If an organization's leadership does not make data protection a priority, it will be difficult to ensure end users' compliance with information security policies and procedures. In this study, end users say their supervisors are not taking appropriate steps to protect data and about half (51 percent) of IT practitioners do not believe the CEO and other C-level executives take data protection seriously.

2. Inconsistent messages about productivity and the importance of information security cause confusion among employees as to what their responsibilities are in protecting company data. In this study, most end users and IT practitioners believe their organization would overlook security risks before they would sacrifice productivity.

3. Major differences between the IT function and end users about appropriate data access and usage practices make it harder to reduce security risks related to mobile devices, the cloud and document collaboration. According to the findings, end users seem to be taking matters into their own hands, as they believe it is acceptable to transfer documents to their personal computer, tablet, smart phone or public cloud. IT practitioners disagree.

4. An organization with a lack of controls and oversight is fertile ground for attacks by or through insiders. Forty-seven percent of end users say the organization does not enforce its policies against the misuse or unauthorized access to company data.

5. An organization's future growth and profitability as well as its reputation are in peril if a data breach occurs as a result of negligent insiders. Only 47 percent of IT practitioners believe employees in their organizations are taking appropriate steps to protect company data they have access to.

6. An organization that reduces the amount of data employees have access to (by implementing a least-privilege access model, improving data disposition policies or ideally both) and streamlines their processes for granting access will likely benefit from more productive employees.

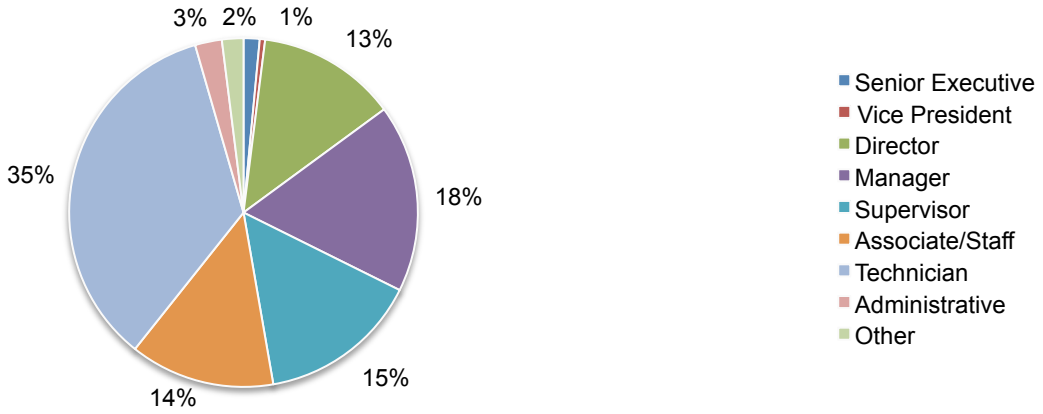
Part 4. Methods

A sampling frame composed of 34,990 IT and IT security practitioners located in the United States and Europe (United Kingdom, Germany and France) and 33,045 end users also located in the United States and Europe were selected for participation in this survey. As shown in the Table 1, 1,328 IT respondents and 1,269 end user respondents completed the survey. Screening removed 162 IT respondent surveys and 159 end user surveys. The final sample was 1,166 IT respondent surveys (or a 3.3 percent response rate) and 1,110 end user respondent surveys (or a 3.4 percent response rate).

Table 1. Sample response	IT	End user
Total sampling frame	34,990	33,045
Total returns	1,328	1,269
Rejected or screened surveys	162	159
Final sample	1,166	1,110
Response rate	3.33%	3.36%

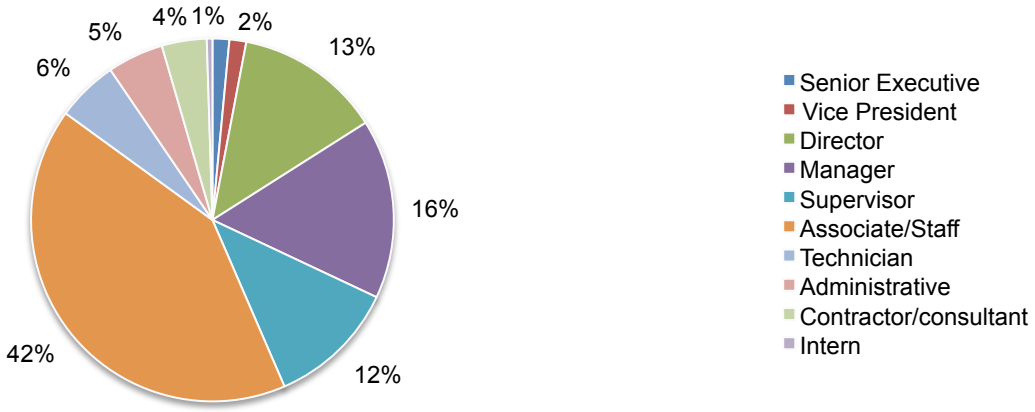
Pie chart 1 reports the current position or organization level of IT respondents. Almost half (48 percent) of IT respondents reported their current position is at or above the supervisory level.

Pie Chart 1. Current position or organizational level of IT respondent



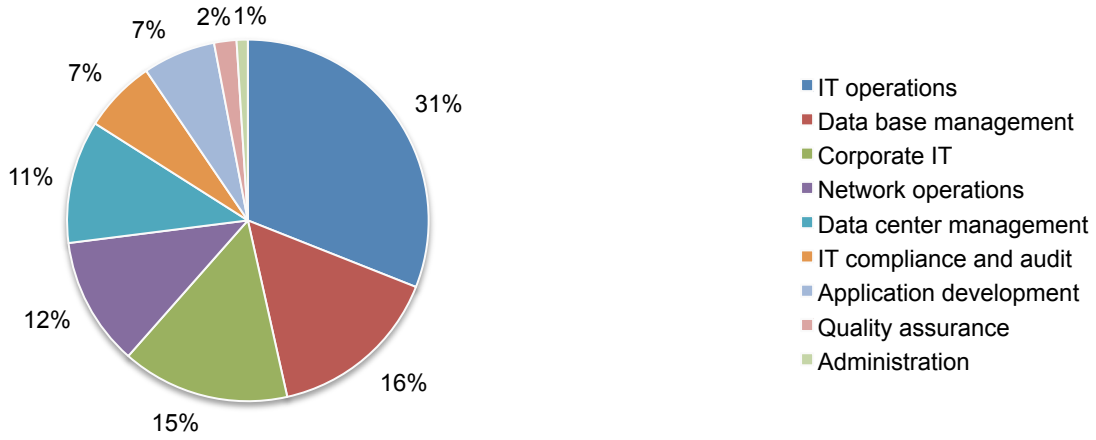
Pie chart 2 reports the current position or organization level of end user respondents. Forty-four percent of end user respondents reported their current position is at or above the supervisory level.

Pie Chart 2. Current position or organizational level of end user respondent



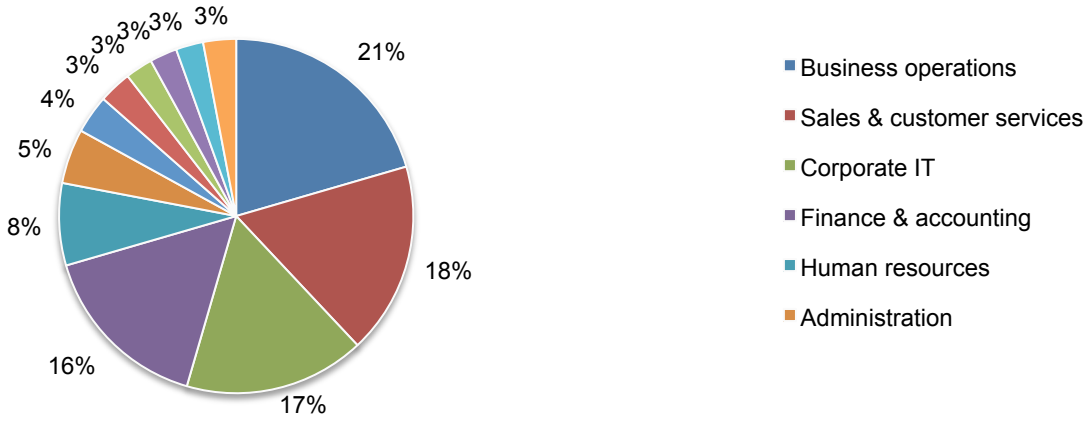
Pie chart 3 reveals the current department or function that best defines the role of the IT respondent. Thirty-one percent indicated IT operations, 16 percent reported data base management and another 15 percent identified corporate IT as their current role.

Pie Chart 3. Current role or department of IT respondent



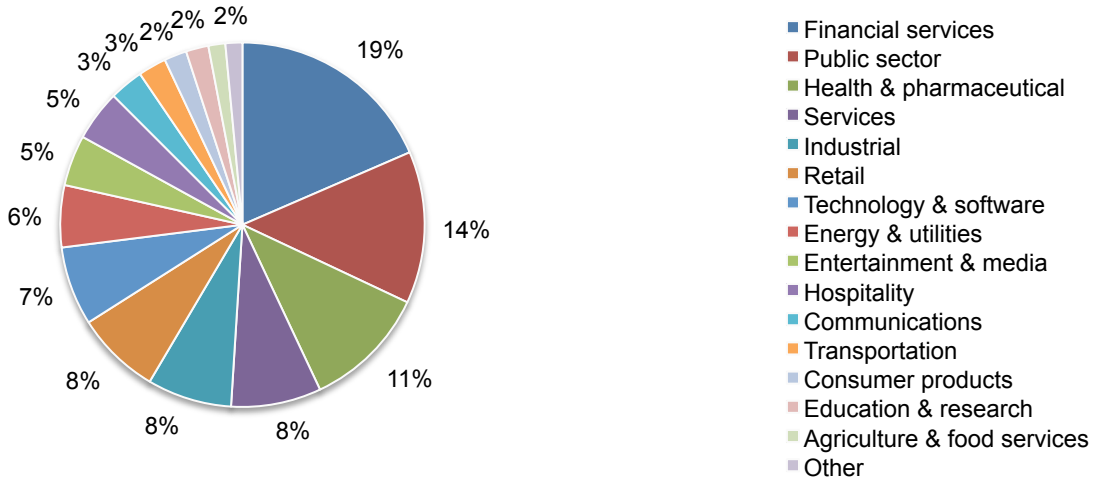
Pie chart 4 reveals the current department or function that best defines the role of the end user respondent. Twenty-one percent indicated business operations, 18 percent reported sales and customer service and another 17 percent identified corporate IT as their current role.

Pie Chart 4. Current role or department of end user respondent



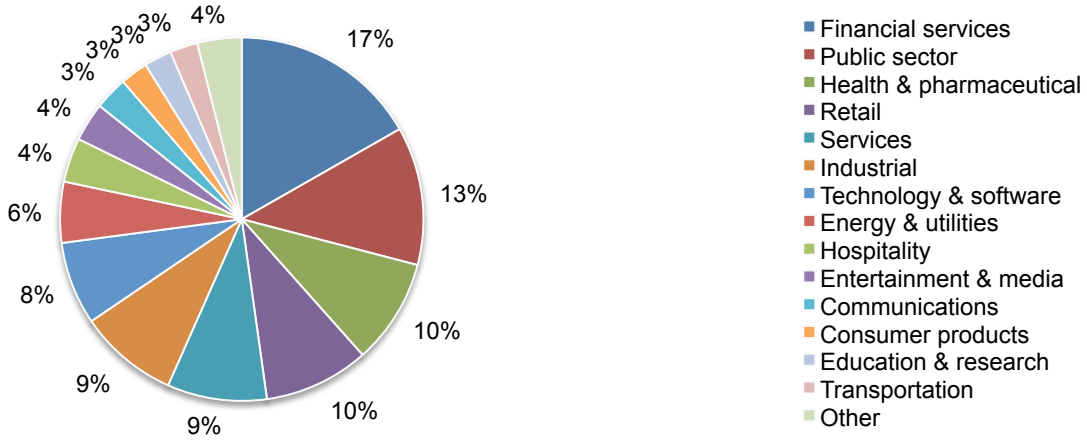
Pie Chart 5 reports the primary industry classification for the IT respondents' organizations. This chart identifies financial services (19 percent) as the largest segment, followed by public sector (14 percent) and health and pharmaceutical (11 percent).

Pie Chart 5. The primary industry classification for the IT respondent



Pie Chart 6 reports the primary industry classification for the end user respondents' organizations. This chart identifies financial services (17 percent) as the largest segment, followed by public sector (13 percent) and health and pharmaceutical (10 percent).

Pie Chart 6. The primary industry classification for end users



According to Table 2, 65 percent of the IT respondents and end user respondents are from organizations with a global headcount of 1,000 or less employees.

Table 2. The worldwide headcount of the organization	IT	End user
Fewer than 500	33%	34%
500 to 1,000	32%	31%
1,001 to 5,000	16%	14%
5,001 to 25,000	8%	9%
25,001 to 75,000	7%	8%
More than 75,000	5%	6%
Total	100%	100%

Part 5. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners and end users located in various organizations in the United States and Europe (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 in November 2014.

Survey response	IT
Total sampling frame	34,990
Total returns	1,328
Rejected or screened surveys	162
Final sample	1,166
Response rate	3.33%

Part 1. Attributions: Please rate the following statements using the scale provided below each item.

Q1. Employees in my organization take appropriate steps to protect company data accessed by them.	IT
Strongly agree	20%
Agree	27%
Unsure	19%
Disagree	22%
Strongly disagree	13%
Total	100%

Q2. The protection of company data is a top priority for our IT department.	IT
Strongly agree	36%
Agree	37%
Unsure	16%
Disagree	9%
Strongly disagree	3%
Total	100%

Q3. The protection of company data is a top priority for our CEO and other C-level executives.	IT
Strongly agree	22%
Agree	29%
Unsure	19%
Disagree	22%
Strongly disagree	9%
Total	100%

Q4. My organization strictly enforces its security policies related to use and access to company data.	IT
Strongly agree	19%
Agree	29%
Unsure	22%
Disagree	21%
Strongly disagree	11%
Total	100%

Part 2. General questions

Q5. What best describes the support and/or resources provided to the IT department to secure company data?	IT
Generous	10%
Adequate	48%
Insufficient	43%
Total	100%

Q6. Does your organization enforce a strict least privilege model (i.e., access to company data only on a need to know basis)?	IT
Fully enforced	20%
Partially enforced (in process)	47%
Not enforced	34%
Total	100%

Q7. Does your organization have an internal enterprise search capability so employees can find and retrieve company files?	IT
Yes, fully deployed	34%
Yes, partially deployed	39%
No, not deployed	28%
Total	100%

Q8. In your opinion, how difficult is it for end users in your organization to search and find company data or files they or their co-workers have created that isn't stored on their individual PC/workstations?	IT
Very difficult	15%
Difficult	45%
Not difficult	33%
Easy	8%
Total	100%

Q9. What's the way most employees share company data or files with co-workers?	IT
Email	56%
File shares	26%
SharePoint	20%
Public cloud services such as Dropbox, etc.	29%
Other (please specify)	4%
Total	135%

Q10. In your opinion, other than using email, how difficult is it for end users in your organization to share documents or files with outside parties such as business partners or vendors?	IT
Very difficult	22%
Difficult	46%
Not difficult	29%
Easy	4%
Total	100%

Q11. How often does your organization delete company data after this information is no longer considered necessary for business or statutory (legal) requirements?	IT
Hourly	4%
Daily	12%
Weekly	15%
Monthly	27%
Yearly	24%
More than one year	8%
Retained forever (no time limit or plan to delete)	13%
Total	100%

Q12a. Does your organization permit end users to use public cloud file sync services (such as Dropbox)?	IT
Yes	25%
No	53%
Permission is not necessary	23%
Total	100%

Q12b. If no, does your organization offer an alternative solution that is approved by the IT or IT security function?	IT
Yes	58%
No	42%
Total	100%

Q13. Does your organization have searchable records of all opens, deletes, modifieds, etc. for company documents and files?	IT
Yes	35%
No	65%
Total	100%

Q14. Do you believe there are times when is it acceptable for end users to transfer work documents to their personal computer, tablet, smart phone or public cloud?	IT
Yes	13%
No	67%
Unsure	21%
Total	100%

Q15. Which one statement best describes end user access privileges to company data?	IT
Access privileges are too limited and at times prevent end users from doing their job.	13%
Access privileges are appropriately set to allow end users to do their job.	50%
Access privileges at times allows end users to access more than necessary to do their job.	32%
Unsure	7%
Total	100%

Q16. On average, how long does it take to grant access privileges to end users who have a legitimate need to access company data, including the time it takes to determine who should approve the request, get approval, implement the changes, and then notify the user?	IT
Within minutes	29%
Within hours	32%
Within days	19%
Within weeks	9%
Months or longer	6%
Cannot determine	6%
Total	100%

Q17. Does your organization provide a way for end users to easily access company data (other than email) from mobile devices such as tablets or smart phones?	IT
Yes	45%
No	56%
Total	100%

Q18. Does your organization permit end users to retain/store documents or files in a public cloud (e.g., services such as Dropbox, GoogleDocs, Box.net, etc.)?	IT
Yes	24%
No	51%
Permission is not needed	26%
Total	100%

Q19. Does your organization restrict or limit the use of public cloud services (such as Dropbox, Google Docs, Box.net and Other (please specify)s)?	IT
Yes	70%
No	30%
Total	100%

Q20. When documents, files or emails get lost or change unexpectedly, how likely is your organization able to assess what happened to them?	IT
Very likely	20%
Likely	31%
Not likely	35%
No chance	14%
Total	100%

Q21. What best defines the level of priority your organization places on the protection of company data?	IT
Very high priority	22%
High priority	34%
Moderate priority	27%
Low priority	12%
Not a priority	6%
Total	100%

Q22. What best defines how the growth of emails, presentations, multimedia and other types of company data impacts your employees' ability to find and utilize data and IT"s ability to manage and protect it?	IT
Very significant impact	37%
Significant impact	25%
Moderate impact	21%
Insignificant impact	8%
No impact	11%
Total	100%

Q23a. In the past year, has access to company data tightened because of security requirements or concerns?	IT
Yes	67%
No	34%
Total	100%

Q23b. If yes, how has tightened security affected the productivity of end users?	IT
No impact on end-user productivity	78%
Negative impact on end-user productivity	10%
Positive impact on end-user productivity	13%
Total	100%

Q24. Please choose the one statement that best describes how your organization views productivity versus security challenges with respect to end user access and use of company data?	IT
My organization would accept heightened security risk to maintain employee productivity	33%
My organization would accept diminished productivity to prevent security risk	27%
My organization is indifferent between productivity decline and security risk	34%
Cannot determine	7%
Total	100%

Q25. Has your organization experienced the loss or theft of company data over the past two years?	IT
Yes	67%
No	27%
Unsure	7%
Total	100%

Q26. In your opinion, when leakage of company data occurs, how often does it happen because of insider mistakes, negligence or malice?	IT
Very frequently	50%
Frequently	24%
Not frequently	17%
Rarely	10%
Total	100%

Q27. In your opinion, when leakage of company data occurs, how often does it happen because of external attackers or hackers?	IT
Very frequently	21%
Frequently	24%
Not frequently	45%
Rarely	11%
Total	100%

Q28. In your opinion, when leakage of company data occurs, how often does it happen because of external attackers who are able to compromise insider accounts?	IT
Very frequently	14%
Frequently	25%
Not frequently	36%
Rarely	27%
Total	100%

Q29. Who is most likely to cause the compromise of insider accounts within your organization?	IT
Insiders who are negligent	59%
Insiders who have malice	16%
External attackers	23%
Other (please specify) (please specify)	2%
Total	100%

Part 3: Organizational characteristics and demographics

D1. What organizational level best describes your present position?	IT
Senior Executive	2%
Vice President	1%
Director	13%
Manager	18%
Supervisor	15%
Associate/Staff	14%
Technician	35%
Administrative	3%
Contractor/consultant	1%
Other (please specify)	1%
Total	100%

D2. Check the department or function that best defines your role.	IT
Corporate IT	15%
Data base management	16%
IT operations	31%
Network operations	12%
IT compliance and audit	7%
Application development	7%
Data center management	11%
Quality assurance	2%
Administration	1%
Total	100%

D3. What is the worldwide headcount of your organization?	IT
Fewer than 500	33%
500 to 1,000	32%
1,001 to 5,000	16%
5,001 to 25,000	8%
25,001 to 75,000	7%
More than 75,000	5%
Total	100%
Extrapolated value	9,412.5

D4. What defines your age range?	IT
21 to 28	24%
29 to 39	28%
40 to 50	24%
51 to 60	15%
60+	10%
Total	100%
Extrapolated value	40.0

D5. What best describes your organization's primary industry classification?	IT
Financial services	19%
Public sector	14%
Health & pharmaceutical	11%
Retail	8%
Industrial	8%
Technology & software	7%
Services	8%
Energy & utilities	6%
Entertainment & media	5%
Consumer products	2%
Hospitality	5%
Transportation	3%
Communications	3%
Education & research	2%
Agriculture & food services	2%
Other (please specify)	2%
Defense & aerospace	0%
Total	100%

Survey response	End user
Total sampling frame	33045
Total returns	1269
Rejected or screened surveys	159
Final sample	1110
Response rate	3.36%

Part 1. Attributions: Please rate the following statements using the scale provided below each item.

Q1. I take all appropriate steps to protect company data accessed and used by me.	End user
Strongly agree	25%
Agree	31%
Unsure	24%
Disagree	17%
Strongly agree	4%
Total	100%

Q2. My co-workers take all appropriate steps to protect company data accessed and used by them.	End user
Strongly agree	17%
Agree	25%
Unsure	22%
Disagree	25%
Strongly agree	12%
Total	100%

Q3. My supervisor or manager takes all appropriate steps to protect company data entrusted to them.	End user
Strongly agree	18%
Agree	27%
Unsure	20%
Disagree	25%
Strongly agree	12%
Total	100%

Q4. My organization strictly enforces its policies against the misuse or unauthorized access to company data.	End user
Strongly agree	21%
Agree	26%
Unsure	23%
Disagree	26%
Strongly agree	5%
Total	100%

Part 2. General questions

Q5. Does your job require you to access and use proprietary information such as customer data, contact lists, employee records, financial reports, confidential business documents, software tools, or other information assets?	End user
Yes	76%
No	25%
Total	100%

Q6. What computing devices do you use to access company data? Please select all that apply.	End user
Desktop/laptop the workplace	82%
Desktop/laptop in home office or remote location	40%
Tablet	33%
Smart phone	20%
Total	173%

Q7. Do you believe there are times when is it acceptable to transfer work documents to your personal computer, tablet, smart phone or public cloud?	End user
Yes	76%
No	18%
Unsure	7%
Total	100%

Q8. What types of sensitive or confidential information do you have access to in the normal course of your job? Please check all that apply.	End user
Customer information including contact lists	62%
Email and attachments	84%
Employee records	13%
Non-financial business information	60%
Financial information	16%
Source code	6%
Other intellectual properties	16%
Other (please specify)	5%
Total	260%

Q9a. Is there company data you have access to that you think you probably should not see?	End user
Yes	71%
No	29%
Total	100%

Q9b. If yes, how often does this happen to you or your co-workers?	End user
Very frequently	16%
Frequently	38%
Not frequently	27%
Rarely	20%
Total	100%

Q9c. If yes, how much data would you or your co-workers would likely see?	End user
A lot of data	38%
Some data	28%
A little data	30%
Unsure	6%
Total	100%

Q10. Which one statement best describes your access privileges to company data?	End user
My access privileges are too limited and at times prevent me from doing my job.	12%
My access privileges appropriately match what I need to do my job.	56%
My access privileges allow me to do more than necessary to do my job.	28%
Unsure	5%
Total	100%

Q11. If you need company data that you don't have access to see, how long does it take you to gain access to it, including the time it takes to make the request, receive the proper approvals, and to be notified that access has been granted?	End user
Within minutes	8%
Within hours	14%
Within days	31%
Within weeks	25%
Months or longer	18%
Cannot determine	5%
Total	100%

Q12. Who is involved with the decision about whether to grant you access to company data? Please check all that apply.	End user
IT department / help desk	22%
IT security	15%
Your supervisor or manager	49%
Executive management	2%
Data owner	14%
Other (please specify)	0%
Total	100%

Q13. How difficult is it for you to search/find company data or files you or your co-workers have created (other than those stored on your PC/workstation)?	End user
Very difficult	30%
Difficult	33%
Not difficult	30%
Easy	8%
Total	100%

Q14. Typically, how long do you retain/store documents or files you have created or worked on?	End user
Hours	9%
Days	7%
Weeks	14%
Months	16%
One year	10%
More than one year	6%
Forever (no time limit or plan to delete)	40%
Total	100%

Q15. How often do you delete files?	End user
Daily, or as I finish with them	15%
Weekly	15%
Monthly	16%
Yearly	10%
Rarely, or less often than once a year	5%
Never	40%
Total	100%

Q16. Does your company provide a way for you to easily access company data (other than email) from mobile devices such as your tablet or smart phone?	End user
Yes	61%
No	39%
Total	100%

Q17. What are your preferred ways to share company data or files with your co-workers? Select no more than two.	End user
Email	52%
File shares	42%
SharePoint	20%
Public cloud services such as Dropbox, etc.	43%
Other	3%
Total	160%

Q18. How difficult is it to share company data or files with business partners (customers, vendors, etc.)?	End user
Very difficult	26%
Difficult	41%
Not difficult	26%
Easy	7%
Total	100%

Q19. Does your organization permit you to retain/store company data or files in a public cloud (services such as Dropbox, GoogleDocs, Box.net, etc.)?	End user
Yes	29%
No	48%
Permission is not needed	24%
Total	100%

Q21. Does your organization restrict or limit the use of public cloud services (such as Dropbox, Google Docs, Box.net and others)?	End user
Yes	52%
No	49%
Total	

Q22. When company data, files or emails get lost or change unexpectedly, is your employer able to tell you about what happened to them?	End user
Yes	28%
No	72%
Total	

Q23. What best defines the level of priority your organization places on the protection of company data?	End user
Very high priority	22%
High priority	26%
Moderate priority	20%
Low priority	14%
Not a priority	19%
Total	100%

Q24. What best defines how the growth of emails, presentations, multimedia and other types of company data impacts your ability to find and access data?	End user
Very significant impact	43%
Significant impact	30%
Moderate impact	17%
Insignificant impact	9%
No impact	3%
Total	100%

Q25. In the past year, has access to company data tightened because of security requirements or concerns?	End user
Yes	52%
No	48%
Total	100%

Q26. If yes, what best defines how tightened security impacts your job productivity?	End user
Very significant impact	25%
Significant impact	30%
Moderate impact	23%
Insignificant impact	18%
No impact	5%
Total	100%

Q27. Please choose the one statement that best describes how your supervisor or manager views productivity versus security challenges when you or your co-workers access and use company data?	End user
My management would accept heightened security risk to maintain employee productivity	38%
My management would accept productivity decline to prevent security risk	16%
My management would be indifferent between security risks and productivity decline	37%
Cannot determine	10%
Total	100%

Q28. Has your organization experienced the loss or theft of company data over the past two years?	End user
Yes	44%
No	25%
Unsure	32%
Total	100%

Q29. In your opinion, when leakage of company data occurs, how often does it happen because of insider mistakes, negligence or malice?	End user
Very frequently	14%
Frequently	36%
Not frequently	42%
Rarely	9%
Total	100%

Q30. In your opinion, when leakage of company data occurs, how often does it happen because of external attackers or hackers?	End user
Very frequently	7%
Frequently	28%
Not frequently	55%
Rarely	11%
Total	100%

Q31. Who is most likely to cause the compromise of insider accounts within your organization?	End user
Insiders who are negligent	64%
Insiders who have malice	12%
External attackers	22%
Other (please specify)	3%
Total	100%

Part 3: Organizational characteristics and demographics

D1. What organizational level best describes your present position?	End user
Senior Executive	2%
Vice President	2%
Director	13%
Manager	16%
Supervisor	12%
Associate/Staff	42%
Technician	6%
Administrative	5%
Contractor/consultant	4%
Intern	1%
Other	0%
Total	100%

D2. Check the department or function that best defined your role.	End user
Sales & customer services	18%
Business operations	21%
Finance & accounting	16%
Corporate IT	17%
Human resources	8%
Research & development	3%
Administration	5%
Marketing & communications	3%
Logistics & transportation	4%
General management	3%
Compliance & audit	3%
Other (please specify)	3%
Total	100%

D3. What is the worldwide headcount of your organization?	End user
Fewer than 500	34%
500 to 1,000	31%
1,001 to 5,000	14%
5,001 to 25,000	9%
25,001 to 75,000	8%
More than 75,000	6%
Total	100%
Extrapolated value	10408

D4. What defines your age range?	End user
21 to 28	27%
29 to 39	30%
40 to 50	21%
51 to 60	16%
60+	8%
Total	100%
Extrapolated value	38.7

D5. What best describes your organization's primary industry classification?	End user
Financial services	17%
Public sector	13%
Health & pharmaceutical	10%
Retail	10%
Services	9%
Industrial	9%
Technology & software	8%
Energy & utilities	6%
Communications	3%
Consumer products	3%
Education & research	3%
Entertainment & media	4%
Hospitality	4%
Transportation	3%
Agriculture & food services	2%
Defense & aerospace	1%
Other (please specify)	1%
Total	100%

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.