Closing Security Gaps to Protect Corporate Data: A Study of US and European Organizations

Release 1

Sponsored by Varonis

Independently conducted by Ponemon Institute LLC

Publication Date: August 2016

Closing Security Gaps to Protect Corporate Data:
A Study of US and European Organizations

Ponemon Institute, August 2016

Part 1. Introduction

Closing Security Gaps to Protect Corporate Data: A Study of US and European Organizations sponsored by Varonis, was conducted to determine the security gaps within organizations that can lead to data breaches and security incidents such as ransomware.

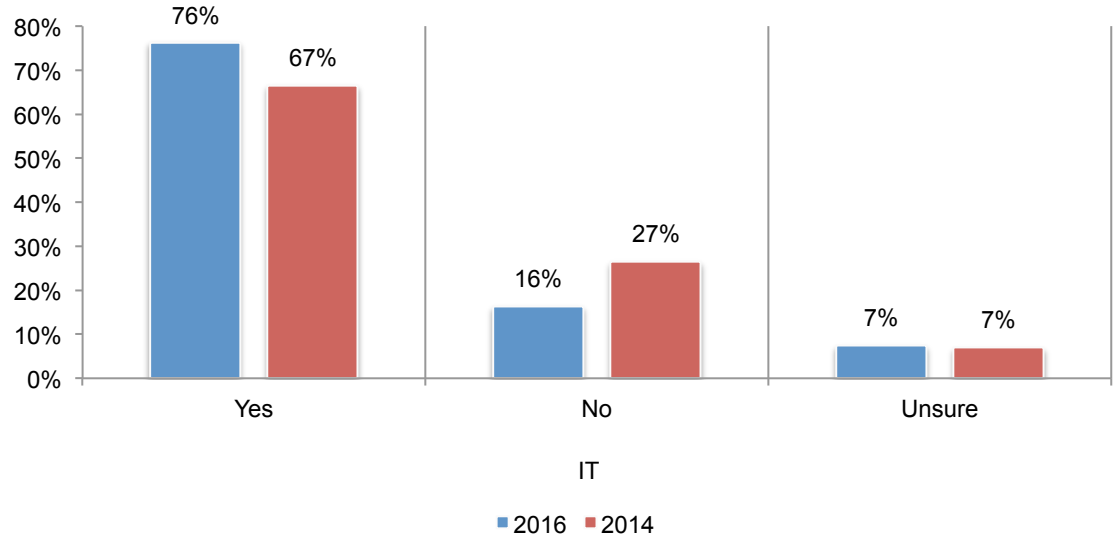
The study surveyed a total of 3,027 employees in US and European organizations (United Kingdom, Germany and France), including 1,371 individuals (hereafter referred to as end users) who work in such areas as sales, finance and accounting, corporate IT, and business operations, and 1,656 individuals who work in IT and IT security (hereafter referred to as IT).

This report includes Key Findings, Conclusions, Methods, and an Appendix with detailed survey questions and results.

Part 2. Key Findings

Loss or theft of data is up sharply, and the leading cause is insider negligence. Seventy-six percent of IT practitioners say their organization experienced the loss or theft of company data over the past two years. This is a significant increase from 67 percent of respondents who participated in the 2014 study, as shown in Figure 1.

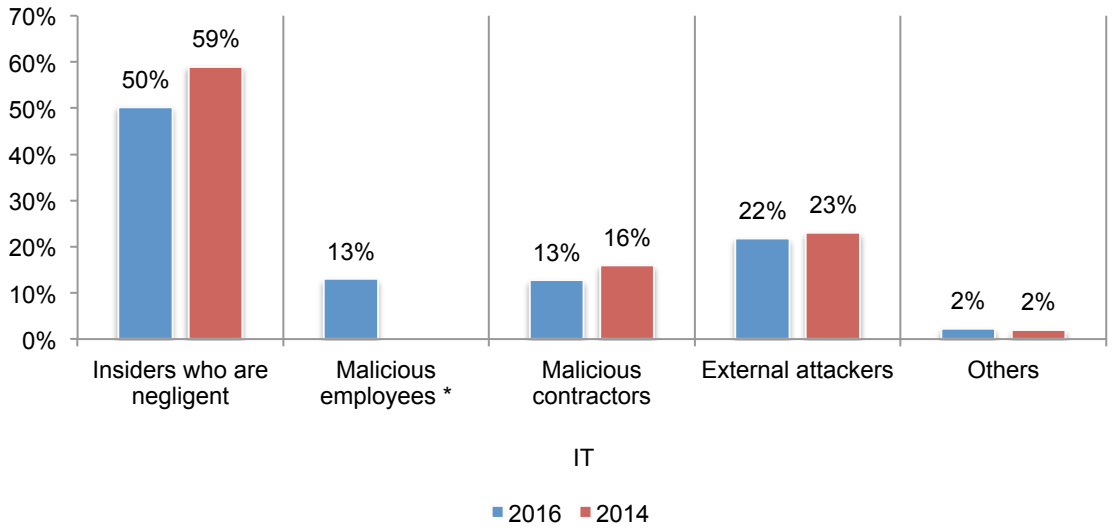
Figure 1. Has your organization experienced the loss or theft of company data over the past two years?



IT respondents say insider negligence is more than twice as likely to cause the compromise of insider accounts as any other culprits, including external attackers, malicious employees or contractors. When a data breach occurs, 50 percent of IT respondents say insiders who are negligent and most likely to cause a compromise, as shown in Figure 2.

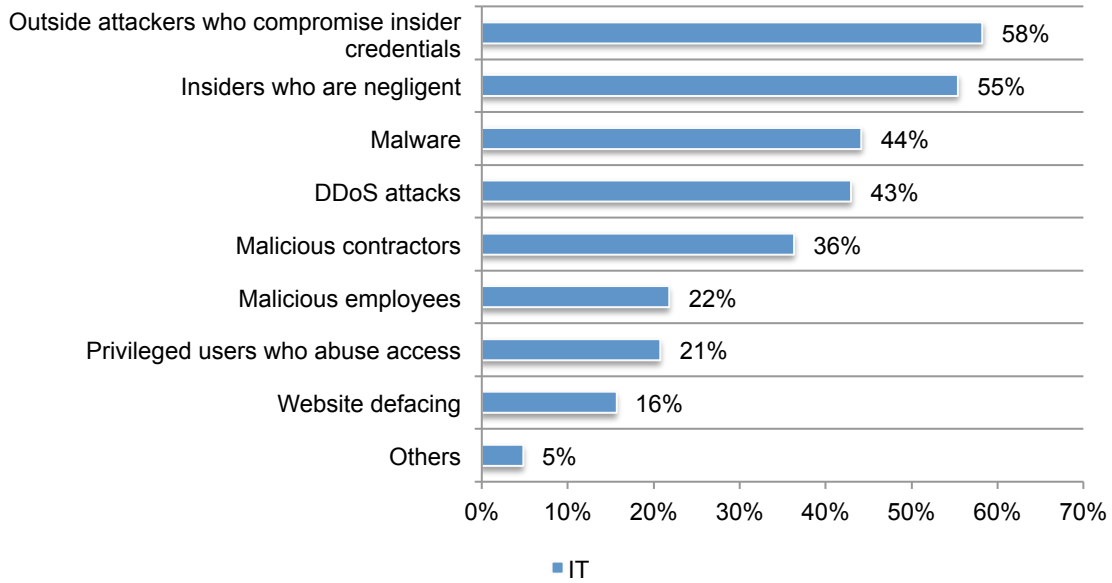
Figure 2. Who is most likely to cause the compromise of insider accounts within your organization?

* Not a response in 2014



Compromised and negligent insiders are a serious concern for IT respondents. As shown in Figure 3, outside attackers who compromise insider credentials worry 58 percent of IT respondents, followed by 55 percent of respondents who say insiders are negligent.

Figure 3. Which security threats does your organization worry about most?



Ransomware is a growing nightmare for companies. Ransomware is the one type of attack that announces its presence. The vast majority of attempts to steal or gain access to valuable data are designed to be undetected. Given the rise of these threats and their sophistication, are organizations becoming more prepared and more vigilant? Is ransomware only the tip of the iceberg?

How ransomware is affecting organizations. In the context of this research, ransomware is defined as a type of malicious software designed to block access to a computer system until a sum of money is paid. According to Figure 4, 78 percent of IT respondents are extremely or very concerned about the threat of ransomware (32 percent + 46 percent).

Figure 4. How concerned are you about the threat of ransomware?
1 = no concern to 10 = very concerned

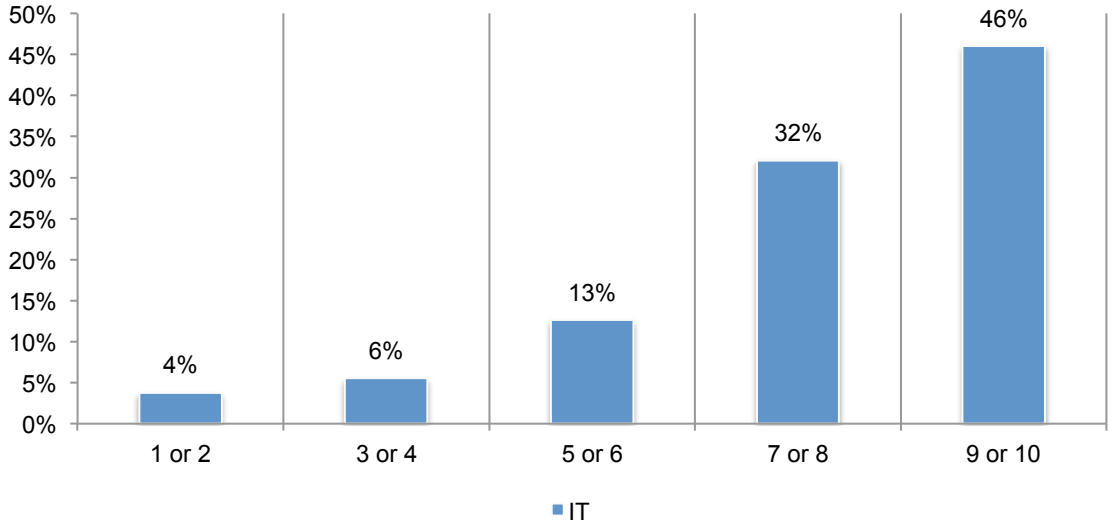
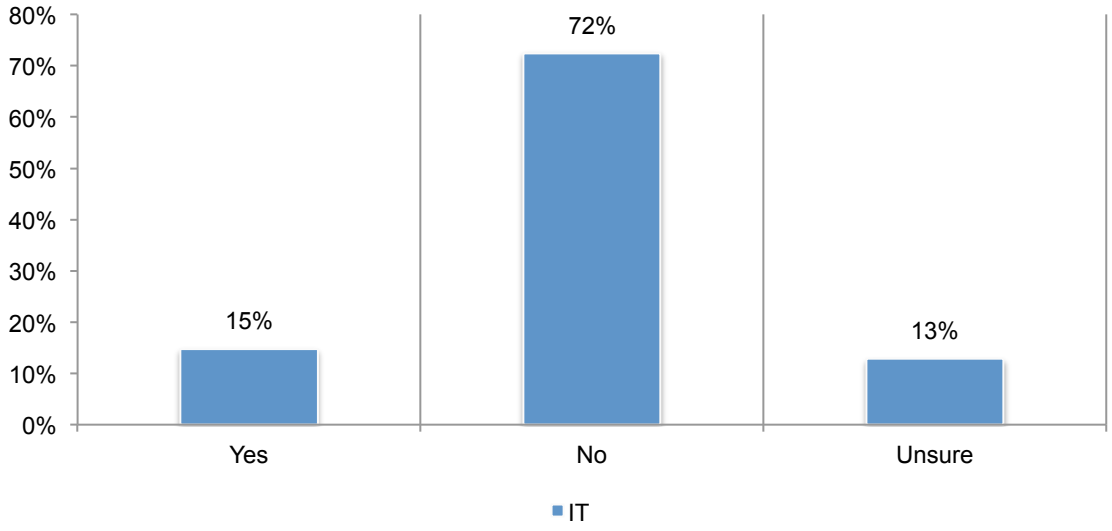


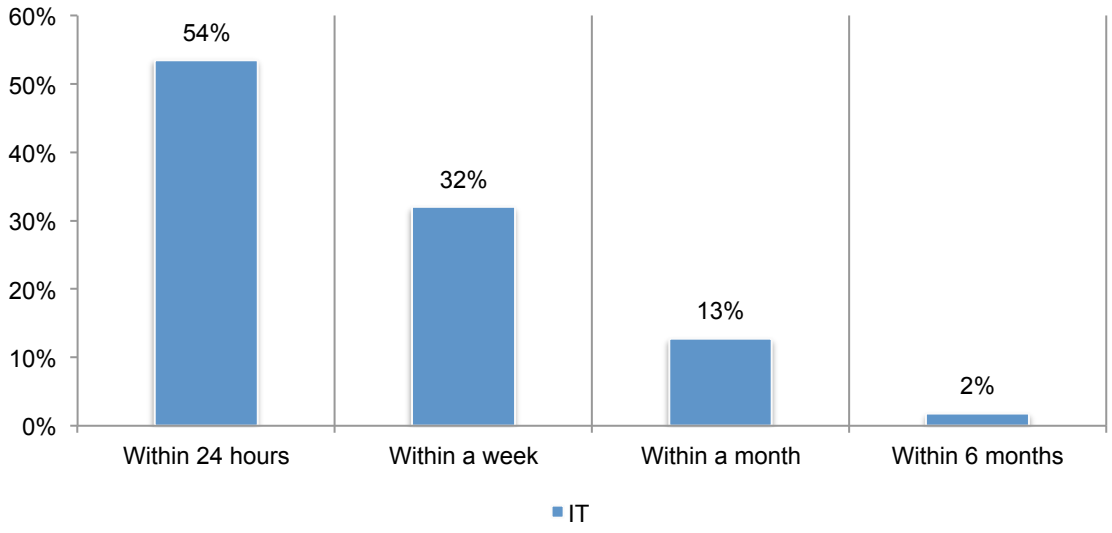
Figure 5 reports that 15 percent of the companies represented in this study have experienced ransomware.

Figure 5. Has your organization experienced ransomware?



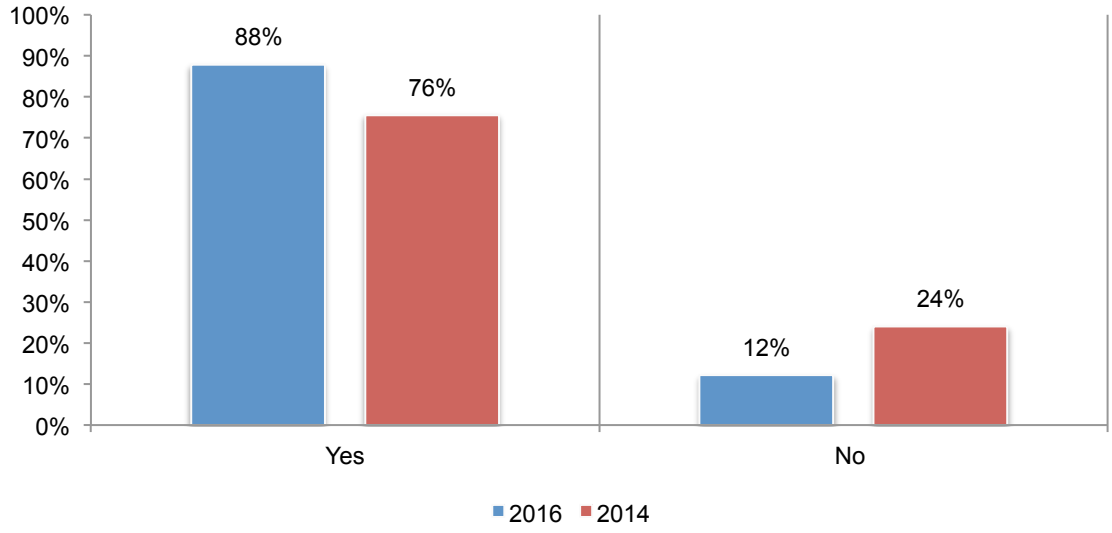
Slightly more than half of IT respondents (54 percent) were able to detect the attack within 24 hours, as shown in Figure 6.

Figure 6. If you experienced ransomware, how quickly was it detected?



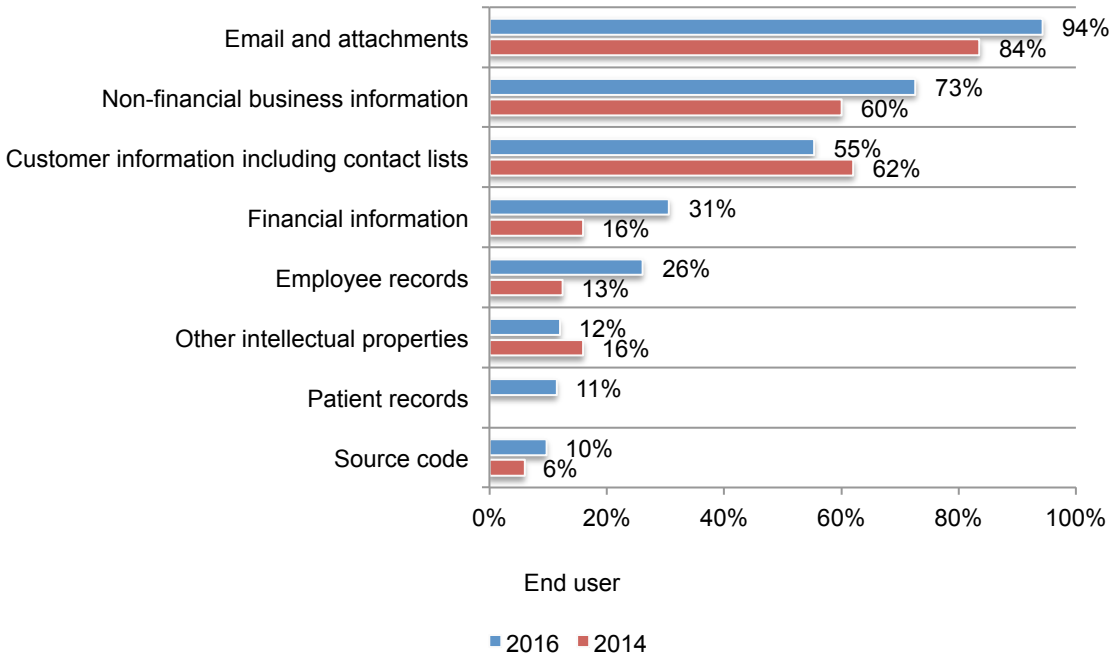
Increasingly, employees' jobs require them to access and use proprietary information. End users who participated in the survey report a sharp increase since 2014 in their access to sensitive and confidential information. As shown in Figure 7, in this year's study, 88 percent of respondents say their jobs require them 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. This is an increase from 76 percent of respondents in 2014.

Figure 7. Does your job require you to access and use proprietary information?



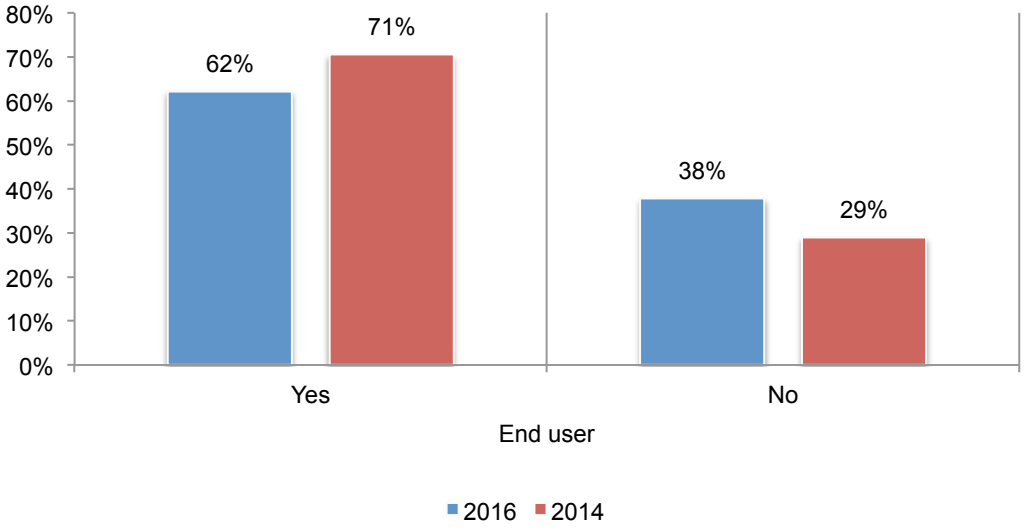
Companies need to improve their ability to track employees' access and use of confidential data. As shown in Figure 8, employees have access to such confidential information as email and attachments with sensitive information, non-financial business information and customer information including contact lists.

Figure 8. What types of sensitive or confidential information do you have access to in the normal course of your job?
More than one choice permitted



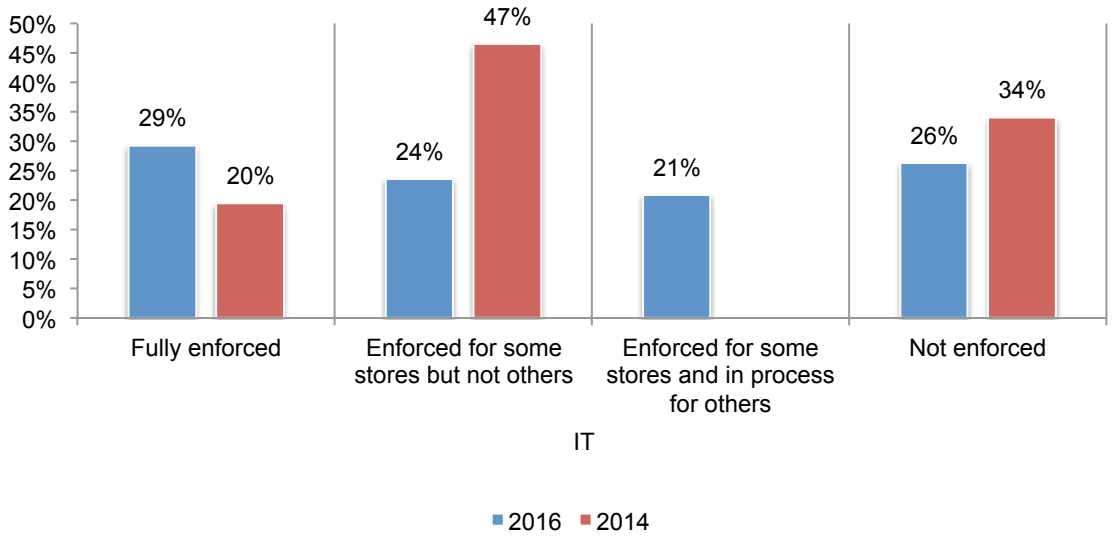
Too many end users still have access to data they should not see. As shown in Figure 9, 62 percent of end users say they have too much access to confidential corporate data. This is an improvement from 2014 when 71 percent of respondents said end users had too much access. In addition, 47 percent say such access happens very frequently or frequently.

Figure 9. Is there company data you have access to that you probably should not see?



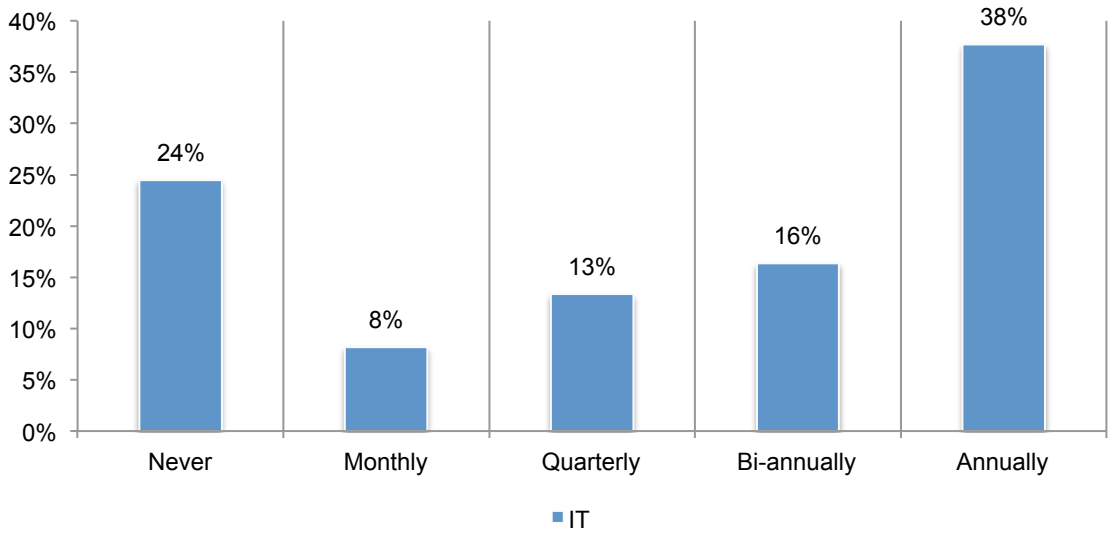
The state of progress in combatting these threats is not encouraging. As shown in Figure 10, only 29 percent of IT respondents say their companies fully enforce a strict least privilege model to ensure insiders have access to company data only on a need to know basis for file shares and other collaborative data stores. The list of individuals who have access to file shares and other collaborative data stores is rarely reviewed. Twenty-four percent of IT respondents say they never review the list. However, the majority of IT respondents say they review the lists twice (16 percent) or once a year (38 percent).

Figure 10. Does your organization enforce a strict least privilege model?



Further, the list of individuals who have access to file shares and other collaborative data stores is not reviewed frequently. Only 8 percent of IT respondents say monthly and 24 percent of IT respondents say they never review the list, as shown in Figure 11.

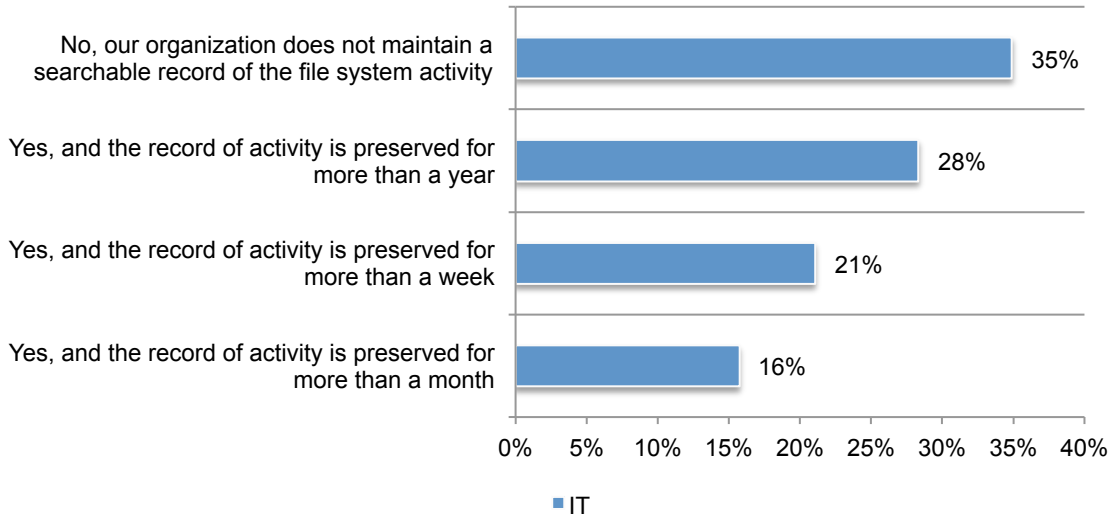
Figure 11. How often does the organization review the list of individuals who have access to file shares and other collaborative data stores?



Thirty-five percent of organizations have no searchable records of file system activity, as shown in Figure 12. Failure to audit this activity is a significant vulnerability, especially with regard to ransomware. Without an audit trail there is no way to determine which files have been encrypted by ransomware.

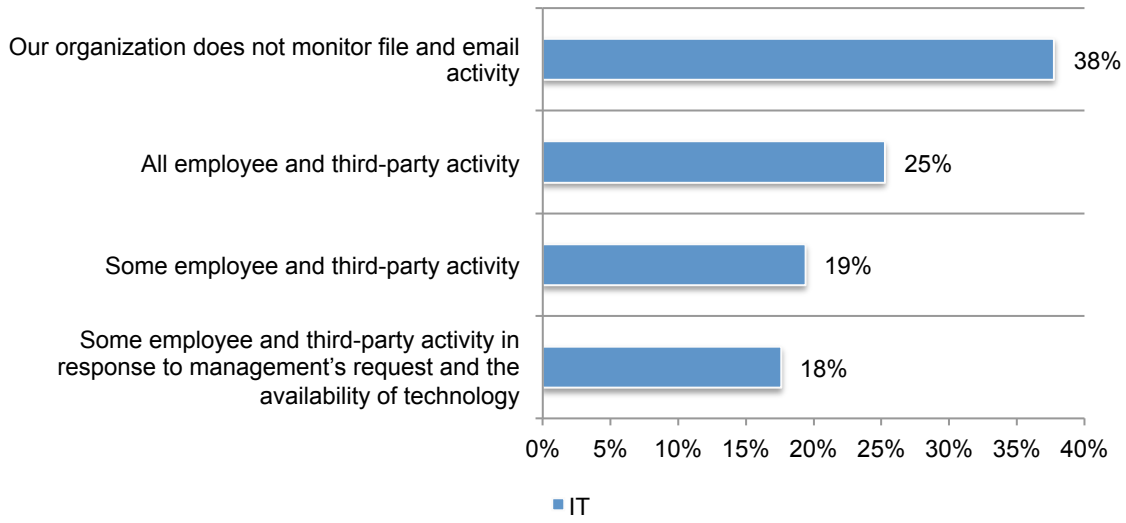
Records of activity are preserved for more than a year (28 percent of respondents), more than a week (21 percent of respondents), more than a month (16 percent of respondents). However, 35 percent of respondents say their companies do not maintain a searchable record of the file system activity.

Figure 12. Does your organization have searchable records of file system activity for company documents and files stored in file shares?



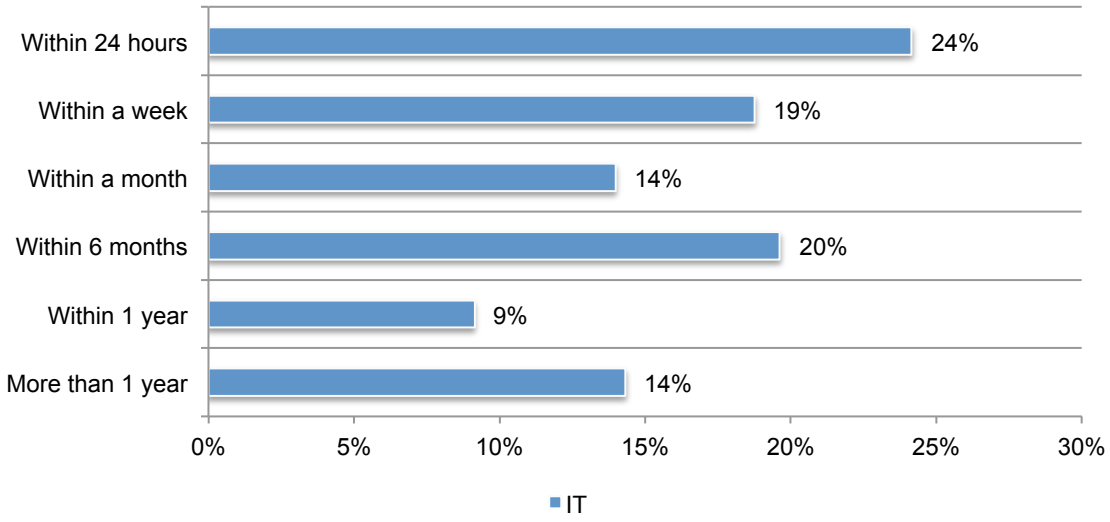
According to Figure 13, only 25 percent of respondents say their company monitors all employee and third-party file and email activity and 38 percent say their company does not monitor file and email activity at all.

Figure 13. How much file and email activity do you monitor?



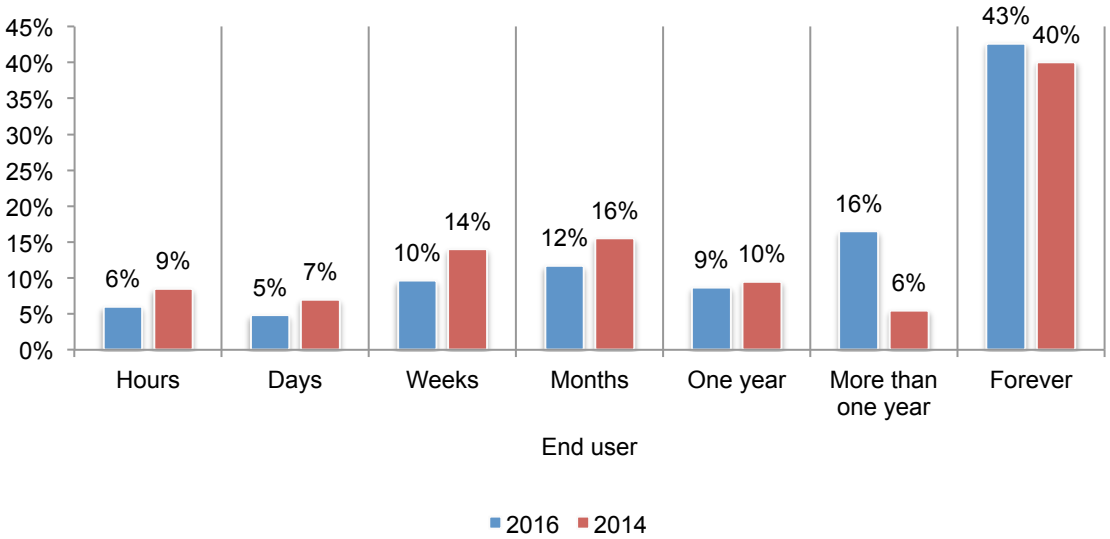
Companies are slow to detect employees accessing files and emails they are not authorized to see. According to Figure 14, only 24 percent of respondents say they are able to determine if employees are accessing information they are not authorized to see.

Figure 14. How quickly was your organization able to detect employees accessing files and emails they were not authorized to see?



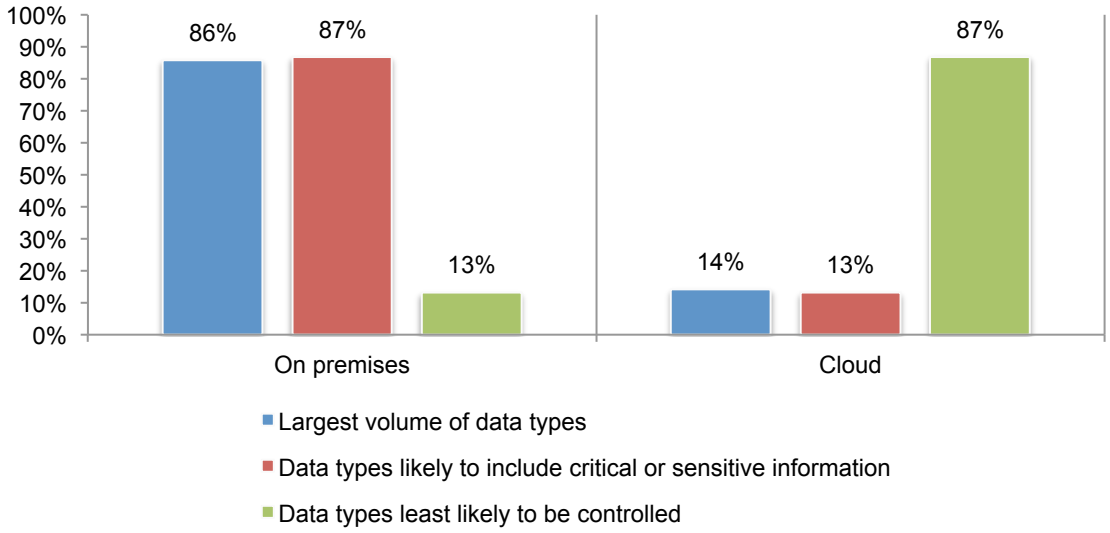
End users are not deleting files, thus exacerbating this extraordinary level of vulnerability. As shown in Figure 15, 43 percent of respondents say they retain and store document or files they created or worked on forever. Another 25 percent of respondents say they keep documents or files one year or longer.

Figure 15. How long do you retain or store documents or files you have created or worked on?



Given the value and growth of business data, moving to the cloud is happening much more slowly than expected. Crown-jewel data continues to be stored on premises. As shown in Figure 16, 86 percent of respondents say their organizations have most of their data stored on premises. In contrast, 13 percent of respondents say most of their information is stored in the cloud.

Figure 16. Where is your largest volume of data stored? Is your critical or sensitive data more likely to be on premises or in the cloud? Which is the least likely to be controlled by the company?



Part 3. Conclusions

Despite the technology available and the continued rise of data loss and theft, it is clear that most organizations are not taking the threat of major disruption in business and reputation seriously enough. Every company relies on – and is entrusted to protect -- valuable, confidential and private data.

The most valuable data featured in most breaches is unstructured data such as emails and documents. This is the data that most organizations have the most of, and know the least about. When emails and files are surfaced publicly, they tend to cause scandal, forcing the breach to have a lasting effect on the company's reputation.

Among this report's most significant findings:

Three out of every four organizations have been hit by the loss or theft of important data over the past two years, a sharp increase since 2014.

Eighty-eight percent of end users say their jobs require them to access and use proprietary information such as customer data, contact lists, employee records, financial reports, confidential business documents, or other sensitive information assets. This is sharply higher than the 76 percent recorded in the 2014 study.

Sixty-two percent of end users say they have access to company data they probably shouldn't see.

IT practitioners say insider negligence is more than twice as likely to cause the compromise of insider accounts as any other culprits, including external attackers, malicious employees or contractors.

Even though only 15% of organizations say they have been hit by ransomware, 78 percent of IT people are very concerned about it. Of those who have been hit, Fifteen percent of organizations have experienced ransomware and barely half of those detected the attack in the first 24 hours.

Thirty-five percent of organizations have no searchable records of file system activity, leaving them unable to determine, among other things, which files have been encrypted by ransomware.

Only 29 percent of IT respondents report that their organizations enforce a strict least-privilege model to ensure insiders have access to company data on a need-to-know basis.

Only 25 percent of organizations monitor all employee and third-party email and file activity -- while 38 percent do not monitor any file and email activity.

The inescapable conclusion is that the continuing increase in data loss and theft is due in large part to two troubling factors:

- Compromises in insider accounts that are exacerbated by far wider employee and third-party access to sensitive information than is necessary
- The continued failure to monitor access and activity around email and file systems – where most confidential and sensitive data moves and lives.

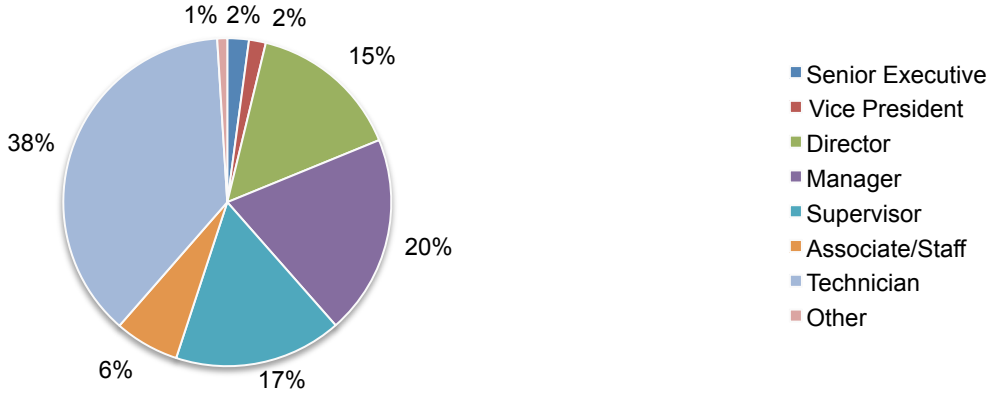
Part 4. Methods

A sampling frame composed of 49,770 IT and IT security practitioners located in the United States and Europe (United Kingdom, Germany and France) and 43,736 end users also located in the United States and Europe were selected for participation in this survey. As shown in Table 1, 1,842 IT respondents and 1,494 end user respondents completed the survey. Screening removed 186 IT respondent surveys and 123 end user surveys. The final sample was 1,656 IT respondent surveys (or a 3.3 percent response rate) and 1,371 end user respondent surveys (or a 3.1 percent response rate).

Table 1. Sample response	IT	End user
Total sampling frame	49,770	43,736
Total returns	1,842	1,494
Rejected or screened surveys	186	123
Final sample	1,656	1,371
Response rate	3.3%	3.1%

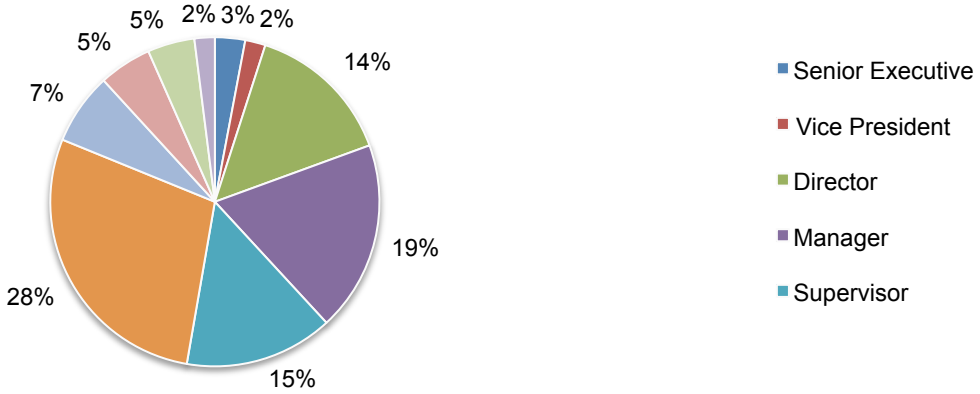
Pie chart 1 reports the current position or organization level of IT respondents. More than half (55 percent) of IT respondents reported their current position is at or above the supervisory level.

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



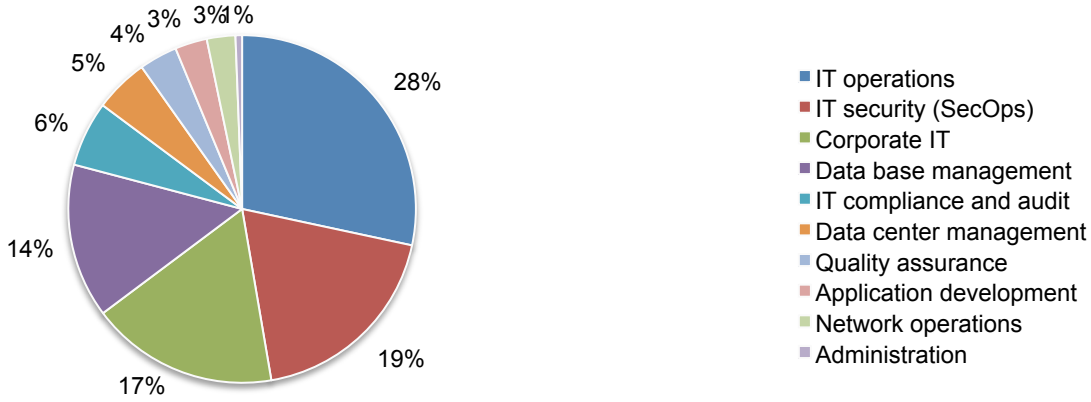
Pie chart 2 reports the current position or organization level of end user respondents. Fifty-three percent of end user respondents reported their current position is at or above the supervisory level.

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



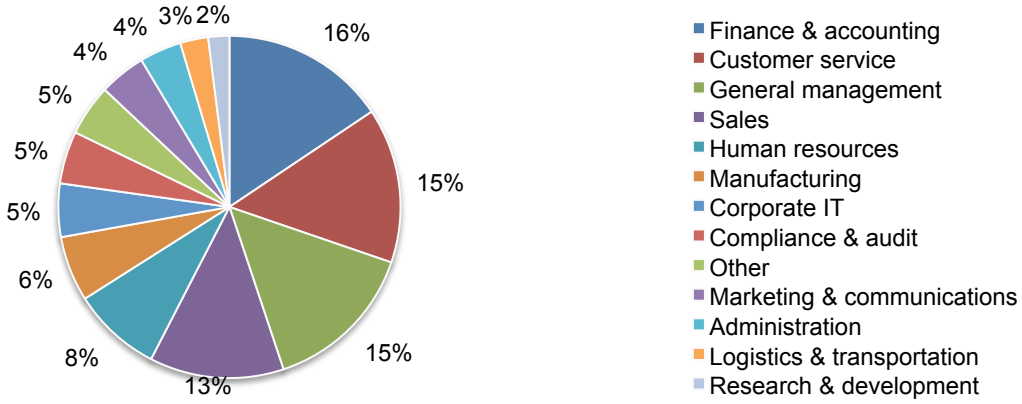
Pie chart 3 reveals the current department or function that best defines the role of the IT respondent. Twenty-eight percent indicated IT operations, 19 percent reported IT security and 17 percent identified corporate IT as their current role.

Pie Chart 3. Current role or department of IT respondent



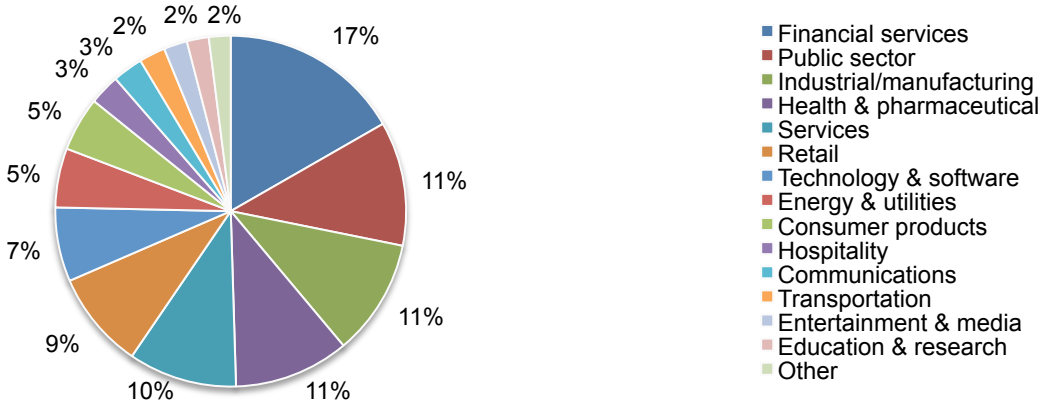
Pie chart 4 reveals the current department or function that best defines the role of the end user respondent. Sixteen percent indicated finance and accounting, 15 percent reported customer service and another 15 percent identified general management as their current role.

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



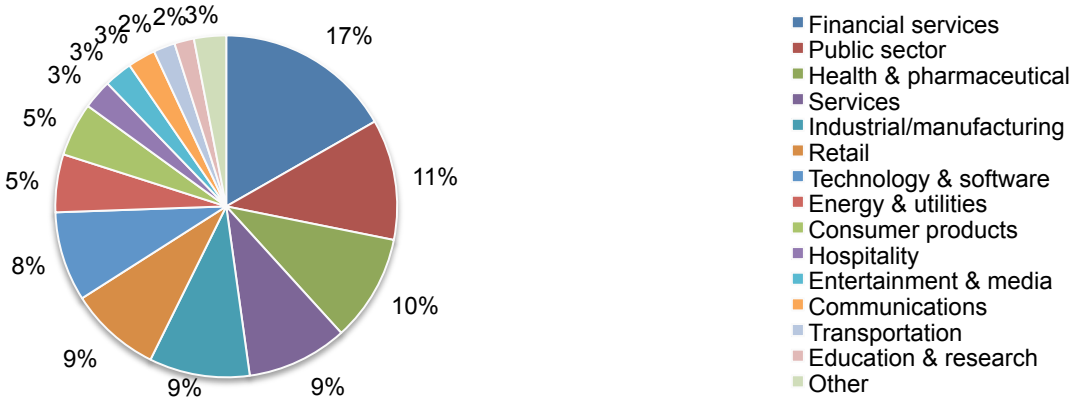
Pie Chart 5 reports the primary industry classification for the IT respondents' organizations. This chart identifies financial services (17 percent of respondents) as the largest segment, followed by public sector (11 percent) and health and industrial/manufacturing (11 percent).

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 (11 percent) and health and pharmaceutical (10 percent).

Pie Chart 6. The primary industry classification for end users



According to Table 2, 76 percent of the IT respondents and end user respondents are from organizations with a global headcount of more than 1,000 employees.

Table 2. The worldwide headcount of the organization	IT	End user
Fewer than 500	9%	10%
500 to 1,000	15%	14%
1,001 to 5,000	37%	36%
5,001 to 25,000	22%	23%
25,001 to 75,000	11%	12%
More than 75,000	6%	5%
Total	100%	100%

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 May 2016.

Survey response	2016 (IT)	2014 (IT)
Total sampling frame	49,770	34,990
Total returns	1,842	1,328
Rejected or screened surveys	186	162
Final sample	1,656	1,166
Response rate	3.3%	3.33%

Part 1. Attributions: % Strongly agree and Agree responses combined.	2016 (IT)	2014 (IT)
Q1. Employees in my organization take appropriate steps to protect company data accessed by them.	52%	47%
Q2. The protection of company data is a top priority for our CEO and other C-level executives.	53%	51%
Q3. My organization strictly enforces its security policies related to use and access to company data.	52%	48%

Part 2. General questions

Q4. What best describes the support and/or resources provided to the IT department to secure company data?	2016 (IT)	2014 (IT)
Generous	14%	10%
Adequate	52%	48%
Insufficient	35%	43%
Total	100%	100%

Q5. Does your organization enforce a strict least privilege model (i.e., access to company data only on a need to know basis) for file shares and other collaborative data stores?	2016 (IT)	2014 (IT)
Fully enforced	29%	20%
Enforced for some stores but not others	24%	47%
Enforced for some stores and in process for others	21%	
Not enforced	26%	34%
Total	100%	100%

* partially deployed response in 2014 (IT)

Q6. How often does the organization review the list of individuals who have access to file shares and other collaborative data stores?	2016 (IT)
Never	24%
Monthly	8%
Quarterly	13%
Bi-annually	16%
Annually	38%
Total	100%

Q7. Does your organization have searchable records of file system activity (for example, opens, deletes, modifies, renames) for company documents and files stored in file shares?	2016 (IT)
Yes, and the record of activity is preserved for more than a year	28%
Yes, and the record of activity is preserved for more than a month	16%
Yes, and the record of activity is preserved for more than a week	21%
No, our organization does not maintain a searchable record of the file system activity	35%
Total	100%

Q8. In terms of volume, what data types does your organization have the most of?	2016 (IT)
Application data, files shares and email stored on premises	86%
Application data, files shares and email stored in the cloud	14%
Total	100%

Q9. Which data types are likely to include the most critical or sensitive information?	2016 (IT)
Application data, files shares and email stored on premises	87%
Application data, files shares and email stored in the cloud	134%
Total	100%

Q10. Which data types are least likely to be controlled by your organization?	2016 (IT)
Application data, files shares and email stored on premises	13%
Application data, files shares and email stored in the cloud	87%
Total	100%

Q11. What best defines the level of priority your organization places on the protection of company data?	2016 (IT)	2014 (IT)
Very high priority	28%	22%
High priority	33%	34%
Moderate priority	29%	27%
Low priority	5%	12%
Not a priority	5%	6%
Total	100%	100%

Q12. How much file and email activity do you monitor?	2016 (IT)
All employee and third-party activity	25%
Some employee and third-party activity	19%
Some employee and third-party activity in response to management's request and the availability of technology	18%
Our organization does not monitor file and email activity	38%
Total	100%

Q13a. Has your organization detected employees accessing files and emails they were not authorized to see?	2016 (IT)
Yes	61%
No	30%
Unsure	9%
Total	100%

Q13b. If yes, how quickly was this detected?	2016 (IT)
Within 24 hours	24%
Within a week	19%
Within a month	14%
Within 6 months	20%
Within 1 year	9%
More than 1 year	14%
Total	100%

Q14. Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid. Using the following 10-point scale, please rate your organization's concern about the threat of ransomware. 1 = not concerned to 10 = extremely concerned	2016 (IT)
1 or 2	4%

3 or 4	6%
5 or 6	13%
7 or 8	32%
9 or 10	46%
Total	100%
Extrapolated value	7.72

Q15a. Has your organization experienced ransomware (e.g. Cryptolocker)?	2016 (IT)
Yes	15%
No	72%
Unsure	13%
Total	100%

Q15b. If yes, how quickly was it detected?	2016 (IT)
Within 24 hours	54%
Within a week	32%
Within a month	13%
Within 6 months	2%
Within 1 year	0%
More than 1 year	0%
Total	100%

Q16a. In the past year, has access to company data tightened because of security requirements or concerns?	2016 (IT)	2014 (IT)
Yes	61%	67%
No	39%	34%
Total	100%	100%

Q16b. If yes, how has tightened security affected the productivity of end users?	2016 (IT)	2014 (IT)
No impact on end-user productivity	48%	78%
Negative impact on end-user productivity	29%	10%
Positive impact on end-user productivity	14%	13%
Do not know	10%	100%
Total	100%	

Q17. 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?	2016 (IT)	2014 (IT)
My organization would accept heightened security risk to maintain employee productivity	30%	33%
My organization would accept diminished productivity to reduce security risk	35%	27%
My organization is indifferent between productivity decline and security risk	28%	34%
Cannot determine	7%	7%
Total	100%	100%

Q18. What is the impact of compliance on your organization's security posture?	2016 (IT)
Significantly Improves security posture	33%
Improves security somewhat	35%
Purely a check the box activity	25%
Unsure	6%
Total	100%

Q19. Has your organization experienced the loss or theft of company data over the past two years?	2016 (IT)	2014 (IT)
Yes	76%	67%
No	16%	27%
Unsure	7%	7%
Total	100%	100%

Q20. In your opinion, when leakage of company data occurs, how often does it happen because of insider mistakes, negligence or malice?	2016 (IT)	2014 (IT)
Very frequently	12%	50%
Frequently	34%	24%
Not frequently	35%	17%
Rarely	19%	10%
Total	100%	100%

Q21. 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 through phishing, malware or other vectors?	2016 (IT)	2014 (IT)
Very frequently	8%	14%
Frequently	26%	25%
Not frequently	33%	36%
Rarely	33%	27%
Total	100%	100%

Q22. In your opinion, when leakage of company data occurs, how often does it happen because of external attackers who do not compromise insider accounts?	2016 (IT)	2014 (IT)
Very frequently	7%	21%
Frequently	12%	24%
Not frequently	50%	45%
Rarely	31%	11%
Total	100%	100%

2014 (IT) does not specify not able to compromise insider accounts

Q23. Who is most likely to cause the compromise of insider accounts within your organization?	2016 (IT)	2014 (IT)
Insiders who are negligent	50%	59%
Malicious employees	13%	
Malicious contractors	13%	16%
External attackers	22%	23%
Others	2%	2%
Total	100%	100%

Q24. Which of the following security threats does your organization worry most about? Please select the top three.	2016 (IT)
Insiders who are negligent	55%
Malicious employees	22%
Malicious contractors	36%
Outside attackers who compromise insider credentials	58%
Malware	44%
Privileged users who abuse access	21%
DDoS attacks	43%
Website defacing	16%
Others	5%
Total	300%

Part 3: Organizational characteristics and demographics

D1. What organizational level best describes your present position?	2016 (IT)	2014 (IT)
Senior Executive	2%	2%
Vice President	2%	1%
Director	15%	13%
Manager	20%	18%
Supervisor	17%	15%
Associate/Staff	6%	14%
Technician	38%	35%
Other	1%	5%
Total	100%	100%

D2. Check the department or function that best defined your role.	2016 (IT)	2014 (IT)
Corporate IT	17%	15%
IT security (SecOps)	19%	
Data base management	14%	16%
IT operations	28%	31%
Network operations	3%	12%
IT compliance and audit	6%	7%
Application development	3%	7%
Data center management	5%	11%
Quality assurance	4%	2%
Administration	1%	1%
Total	100%	100%

D3. What is the worldwide headcount of your organization?	2016 (IT)	2014 (IT)
Fewer than 500 people	9%	33%
500 to 1,000 people	15%	32%
1,001 to 5,000 people	37%	16%
5,001 to 25,000 people	22%	8%
25,001 to 75,000 people	11%	7%
More than 75,000 people	6%	5%
Total	100%	100%
		9,412.5

D4. What industry best describes your organization's industry concentration or focus?	2016 (IT)	2014 (IT)
Agriculture & food services	1%	2%
Communications	3%	3%
Consumer products	5%	2%
Defense & aerospace	0%	0%
Education & research	2%	2%
Energy & utilities	5%	6%
Entertainment & media	2%	5%
Financial services	17%	19%
Health & pharmaceutical	11%	11%
Hospitality	3%	5%
Industrial/manufacturing	11%	8%
Public sector	11%	2%
Retail	9%	14%
Services	10%	8%
Technology & software	7%	8%
Transportation	2%	7%
Other	1%	3%
Total	100%	100%

Survey response End Users	2016 (End user)	2014 (End user)
Total sampling frame	43,736	33045
Total returns	1,494	1269
Rejected or screened surveys	123	159
Final sample	1,371	1110
Response rate	3.1%	**3.36%**

Part 1. Attributions: % Strongly agree and Agree response combined	2016 (End user)	2014 (End user)
Q1. I take all appropriate steps to protect company data accessed and used by me.	39%	56%
Q2. My organization strictly enforces its policies against the misuse or unauthorized access to company data.	35%	47%
Q3. My organization's IT function knows where my sensitive information is stored.	33%	
Not a question in 2014 (End user)		

Part 2. General questions

Q4. 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?	2016 (End user)	2014 (End user)
Yes	88%	76%
No (stop)	12%	24%
Total	100%	100%

Q5. What types of sensitive or confidential information do you have access to in the normal course of your job? Please check all that apply.	2016 (End user)	2014 (End user)
Customer information including contact lists	55%	62%
Email and attachments	94%	84%
Employee records	26%	13%
Student records	2%	
Patient records	11%	
Non-financial business information	73%	60%
Financial information	31%	16%
Source code	10%	6%
Other intellectual properties	12%	16%
Other		5%
Total	314%	260%
Not a question in 2014		

Q6a. Is there company data you have access to that you think you probably should not see?	2016 (End user)	2014 (End user)
Yes	62%	71%
No	38%	30%
Total	100%	100%

Q6b. If yes, how often does this happen to you or your co-workers?	2016 (End user)	2014 (End user)
Very frequently	17%	16%
Frequently	30%	38%
Not frequently	45%	27%
Rarely	8%	20%
Total	100%	100%

Q6c. If yes, how much data would you or your co-workers likely see?	2016 (End user)	2014 (End user)
A lot of data	37%	38%
Some data	25%	28%
A little data	32%	30%
Unsure	6%	6%
Total	100%	100%

Q7. Which one statement best describes your access privileges to company data?	2016 (End user)	2014 (End user)
My access privileges are too limited and at times prevent me from doing my job.	39%	12%
My access privileges appropriately match what I need to do my job.	39%	56%
My access privileges are broader than what is necessary to do my job.	17%	28%
Unsure	5%	5%
Total	100%	100%

Q8. Typically, how long do you retain/store documents or files you have created or worked on?	2016 (End user)	2014 (End user)
Hours	6%	9%
Days	5%	7%
Weeks	10%	14%
Months	12%	16%
One year	9%	10%
More than one year	16%	6%
Forever (no time limit or plan to delete)	43%	40%
Total	100%	100%

Q9. How often do you delete files?	2016 (End user)	2014 (End user)
Daily, or as I finish with them	11%	15%
Weekly	9%	15%
Monthly	12%	16%
Yearly	9%	10%
Rarely, or less often than once a year	16%	5%
Never	43%	40%
Total	100%	100%

Q10. What best defines the level of priority your organization places on the protection of company data?	2016 (End user)	2014 (End user)
Very high priority	17%	22%
High priority	21%	26%
Moderate priority	34%	20%
Low priority	16%	14%
Not a priority	12%	19%
Total	100%	100%

Q11 In the past year, has access to company data tightened because of security requirements or concerns?	2016 (End user)	2014 (End user)
Yes	43%	52%
No	57%	48%
Total	100%	100%

Q12. 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?	2016 (End user)	2014 (End user)
My management would accept heightened security risk to maintain employee productivity	48%	38%
My management would accept productivity decline to prevent security risk	24%	16%
My management would be indifferent between security risks and productivity decline	20%	37%
Cannot determine	8%	10%
Total	100%	100%

Q13. Has your organization experienced the loss or theft of company data over the past two years?	2016 (End user)	2014 (End user)
Yes	59%	44%
No	22%	25%
Unsure	19%	32%
Total	100%	100%

Q14. In your opinion, when leakage of company data occurs, how often does it happen because of insider mistakes, negligence or malice?	2016 (End user)	2014 (End user)
Very frequently	33%	14%
Frequently	40%	36%
Infrequently	19%	42%
Rarely	9%	9%
Total	100%	100%

Q15. In your opinion, when leakage of company data occurs, how often does it happen because of external attackers or hackers?	2016 (End user)	2014 (End user)
Very frequently	9%	7%
Frequently	24%	28%
Infrequently	31%	55%
Rarely	36%	11%
Total	100%	100%

Q16. Who is most likely to put your organization's data at risk?	2016 (End user)	2014 (End user)
Insiders who are negligent	58%	64%
Insiders who have malice	18%	12%
External attackers	23%	22%
Other (please specify)	2%	3%
Total	100%	100%

Q17a. Does your organization's IT department monitor all file and email activity in order to know what files have been deleted or moved and when?	2016 (End user)
Yes	43%
No	44%
Unsure	13%
Total	100%

Q17b. If yes, does knowing that make you less likely to take company data with you if you left your job?	2016 (End user)
Yes	54%
No	36%
Unsure	10%
Total	100%

Q18a. Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid. Have you or one of your coworkers experienced ransomware that encrypts your files and asks for compensation in order to decrypt?	2016 (End user)
Yes	9%
No	78%
Unsure	14%
Total	100%

Q18b. If yes, how was the infection detected?	2016 (End user)
Ransomware notice prompting user to pay	19%
Detected by IT before it became a significant issue	71%
Unsure	10%
Total	100%

Q18c. If IT detected the ransomware, how successful was the recovery?	2016 (End user)
Files were restored promptly with minimal disruption to productivity	12%
Files took days or weeks to recover	25%
We never got our files back	47%
Unsure	16%
Total	100%

Q18d. If a notice to pay was received, did your organization pay the ransom?	2016 (End user)
Yes	13%
No	87%
Total	100%

Part 3: Organizational characteristics and demographics

D1. What organizational level best describes your present position?	2016 (End user)	2014 (End user)
Senior Executive	3%	2%
Vice President	2%	2%
Director	14%	13%
Manager	19%	16%
Supervisor	15%	12%
Associate/staff	28%	42%
Technician	7%	6%
Administrative	5%	5%
Contractor/consultant	5%	4%
Intern	1%	1%
Other	1%	0%
Total	100%	100%

D2. Check the department or function that best defined your role.	2016 (End user)	2014 (End user)
Administration	4%	5%
Business operations		21%
Compliance & audit	5%	3%
Corporate IT	5%	17%
Customer service	15%	18%
Finance & accounting	16%	16%
General management	15%	3%
Human resources	8%	8%
Logistics & transportation	3%	4%
Manufacturing	6%	
Marketing & communications	4%	3%
Other	5%	3%
Research & development	2%	3%
Sales	13%	
Total	100%	

D3. What is the worldwide headcount of your organization?	2016 (End user)	2014 (End user)
Fewer than 500 people	10%	34%
500 to 1,000 people	14%	31%
1,001 to 5,000 people	36%	14%
5,001 to 25,000 people	23%	9%
25,001 to 75,000 people	12%	8%
More than 75,000 people	5%	6%
Total	100%	100%
		10408

D4. What defines your age range?	2016 (End user)	2014 (End user)
18 to 28	26%	27%
29 to 39	36%	30%
40 to 50	21%	21%
51 to 60	12%	16%
60+	4%	8%
Total	100%	100%

D5. What industry best describes your organization's industry concentration or focus?	2016 (End user)	2014 (End user)
Agriculture & food services	1%	2%
Communications	3%	3%
Consumer products	5%	3%
Defense & aerospace	0%	1%
Education & research	2%	3%
Energy & utilities	5%	6%
Entertainment & media	3%	4%
Financial services	17%	17%
Health & pharmaceutical	10%	10%
Hospitality	3%	4%
Industrial/manufacturing	9%	9%
Public sector	11%	13%
Retail	9%	10%
Services	9%	9%
Technology & software	8%	8%
Transportation	2%	3%
Other	2%	1%
Total	100%	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.