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

Release 2: The Widening Gap Between IT and End Users

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
Release 2: The Widening Gap Between IT and End Users

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 practitioners). The interviews were conducted in April and May 2016.

Results are compared with a similar study conducted in 2014 by the Ponemon Institute and also sponsored by Varonis. The interviews for the 2014 and 2016 reports were conducted approximately 18 months apart by Ponemon with participant pools that were similar in size, geography, roles and types of organizations.

The full 2016 report, issued August 9, 2016, can be found here. In that report, key findings included a sharp rise in the loss or theft of data, an increase in the percentage of employees with access to sensitive data, and the belief that insider negligence is now the #1 concern for organizations trying to prevent these losses.

Release 2, issued August 30, 2016, is titled “The Widening Gap Between IT and End Users” and highlights key findings in the examination of IT and end user practices and beliefs. This report is based on the same interviews and findings documented in the full report. This report includes Key Findings, Conclusions, Methods, and an Appendix with detailed comparison of IT and End User responses to 10 different questions.

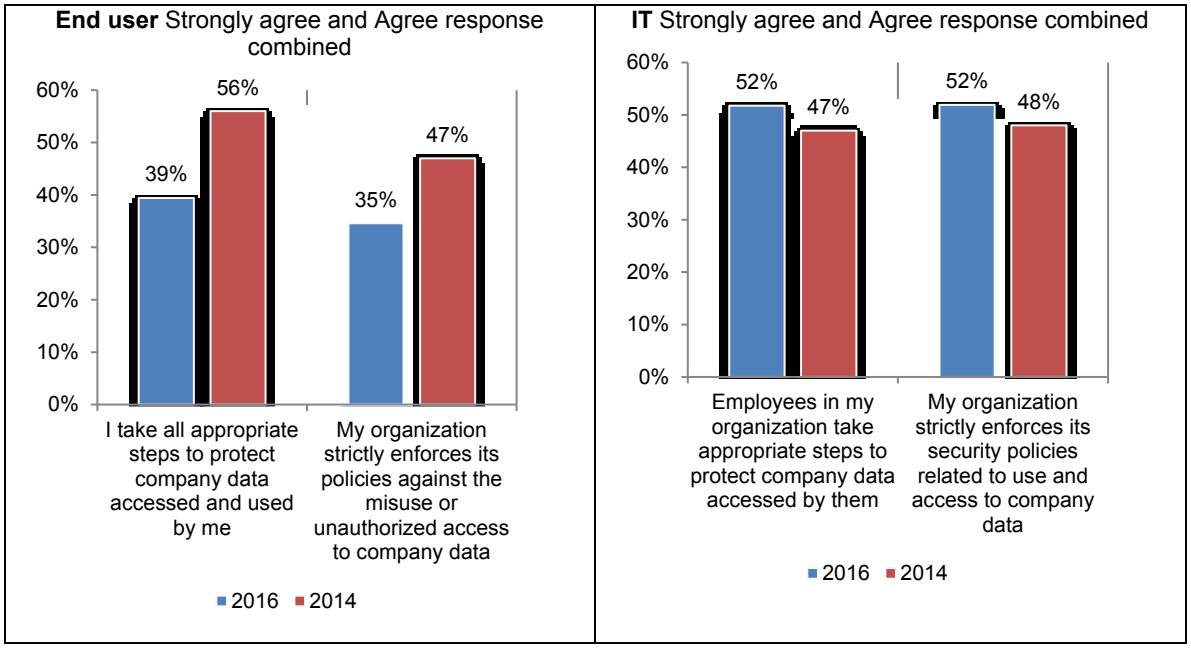
Part 2. Key Findings

A serious – and worsening – vulnerability is the end user who is not conscientious and careful to protect company data accessed by them. At a time when one would expect general improvement in end-user hygiene due to increased awareness of cyberattacks and security breaches, this survey instead finds a precipitous decline. As shown in Figure 1, only 39 percent of end user respondents say they take all appropriate steps to protect company data accessed and used by them, significantly worse than the 56 percent of respondents who gave the same response in the 2014 study. In contrast, 52 percent of IT respondents believe employees in their organizations take appropriate steps. This is a significant disconnect between the IT security function and end users throughout the organizations they support.

One apparent reason for the disconnect between IT and end users is their respective perceptions of company leadership. Asked to agree or disagree that the protection of company data is a top priority for their CEO and other C-level executives, only 35% of end users agreed while 53% of IT professionals chose the more optimistic response.

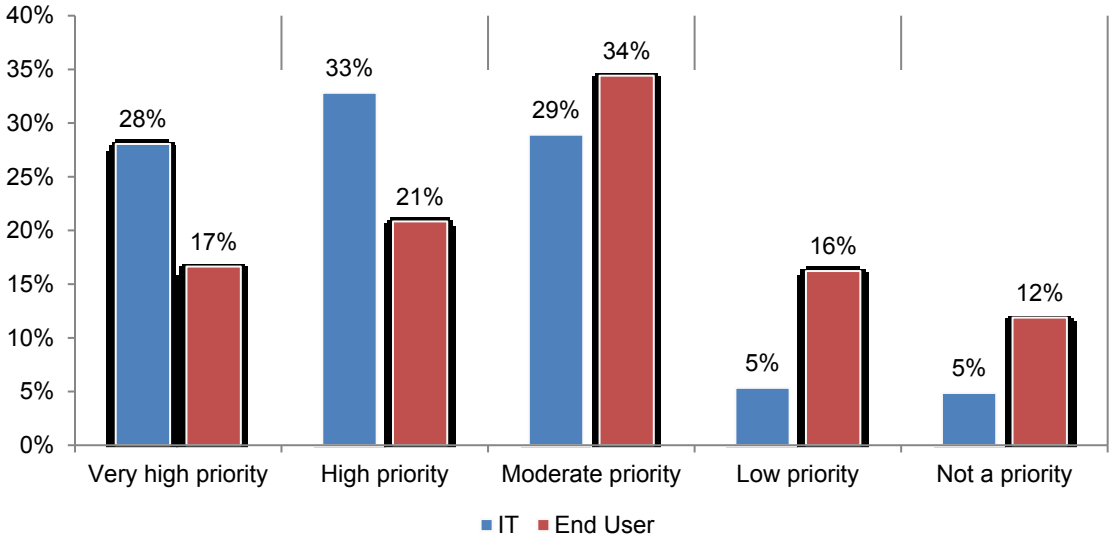
Moreover, while 52 percent of IT respondents believe that policies against the misuse or unauthorized access to company data are being enforced and followed, only 35 percent of end user respondents say their organizations strictly enforce those policies.

Figure 1. The end-user and IT practitioner gap in data protection practices



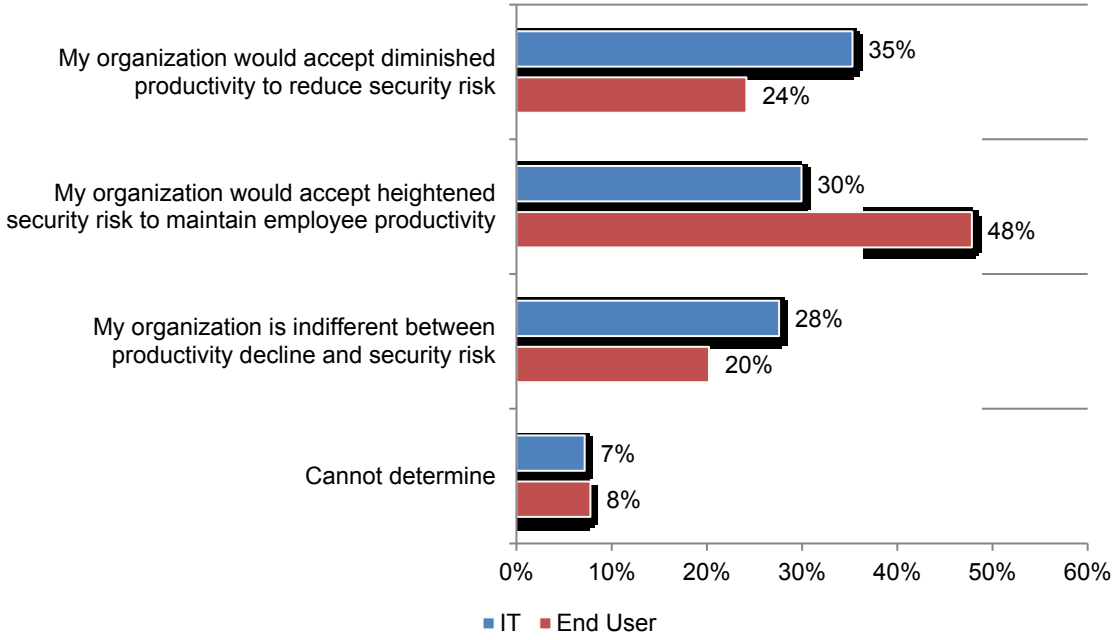
IT is most likely to view data protection as a priority. As shown in Figure 2, 61 percent of respondents who work in IT security view the protection of critical company information a very high or high priority. In contrast, 38 percent of respondents who are considered end users of this data believe it is a very high or high priority.

Figure 2. Is the protection of company critical information a priority?



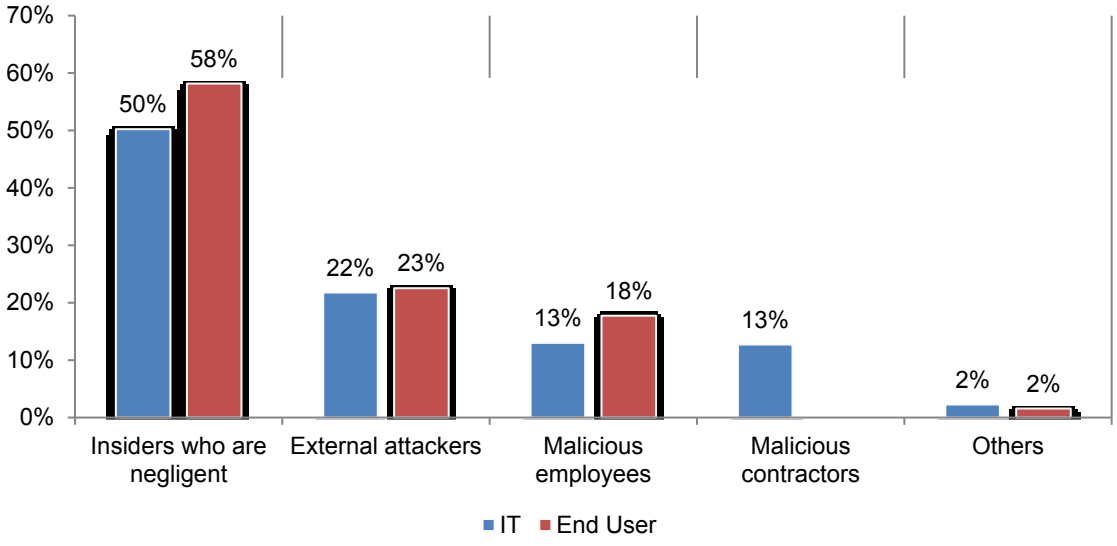
IT practitioners believe their organizations are more concerned about security than end users do. Thirty percent of IT practitioners and 48 percent of end users say in order to maintain productivity, their organizations would accept more risk to their corporate data. Only 24 percent of employees and 35 percent of IT practitioners say their management would accept a decline in their productivity to minimize security risks, according to Figure 3.

Figure 3. What IT practitioners & end users believe is their organizations' attitude about productivity and security



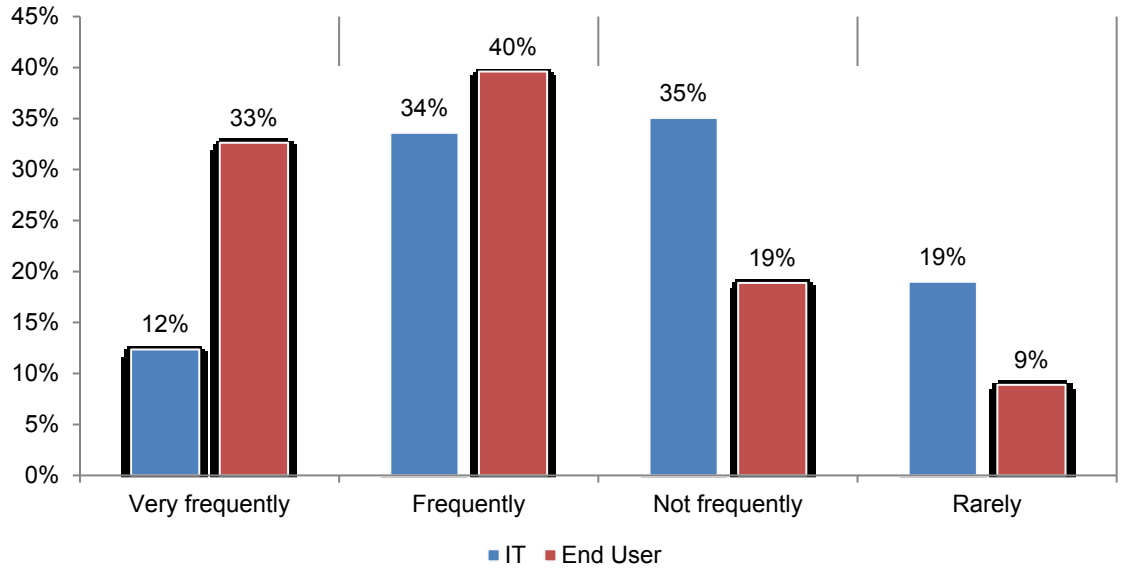
End users are more inclined to believe the compromise of insider accounts is likely insiders' fault. As shown in Figure 4, 50 percent of IT practitioners and 58 percent of end users believe the compromise of insider accounts is due to negligent insiders – by far the most common response. External attackers and malicious employees are considered much less likely to be the cause.

Figure 4. Who is most likely to cause the compromise of insider accounts?



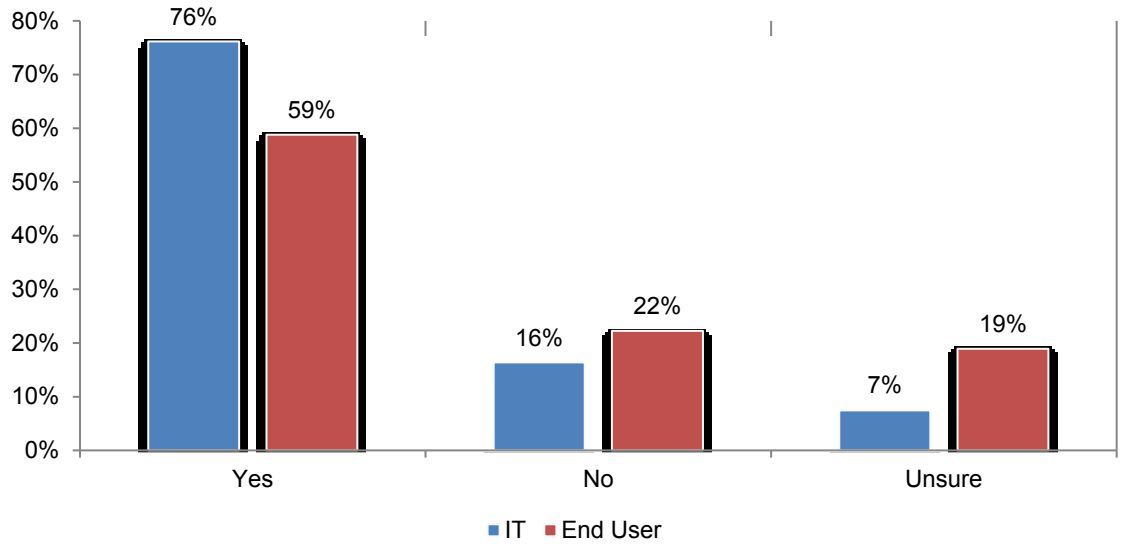
End users believe data breaches are frequently due to insider mistakes, but most IT people do not. When a data breach occurs, a far greater percentage of end users (73 percent vs. 46 percent) say it is very frequently or frequently due to insider mistakes, negligence or malice.

Figure 5. 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 76 percent of IT practitioners say their organization experienced the loss or theft of company data over the past two years, only 59 percent of employees are aware that this has happened, as shown in Figure 6.

Figure 6. Did your organization have a data breach in the past two years?



Part 3. Conclusions

Organizations of all types and sizes face a significant challenge in keeping confidential, sensitive or private business information secure without diminishing the productivity of their employees or processes that depend on contractors, vendors and business partners in their supply and demand chains. This is made more difficult because of the proliferation of business data that needs to be protected and the increasingly wide swath of people with access to that data. 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 five 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.

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 organizations would sacrifice security before they would accept diminished productivity.

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

4. 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.

5. 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 its processes for granting access will likely benefit from more productive employees.

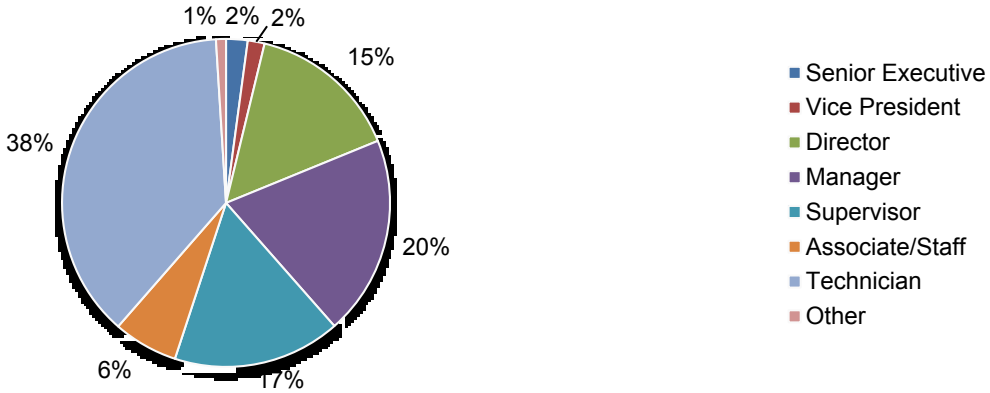
Part 4. Methods

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%

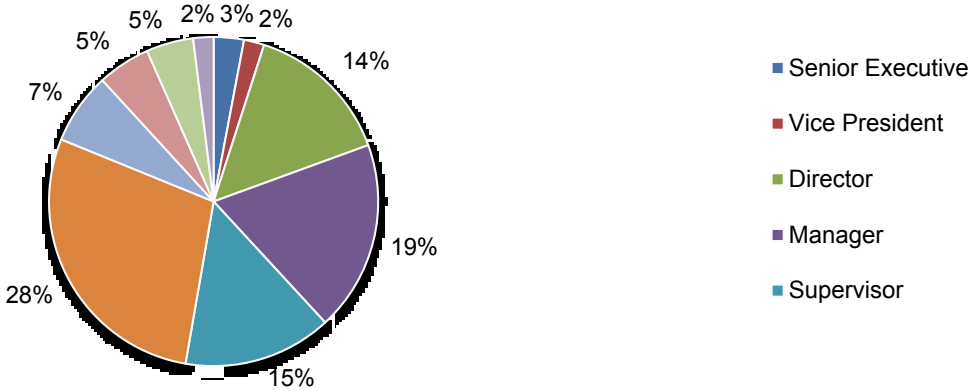
Pie chart 1 reports the current position or organization level of IT respondents. More than half (55 percent) of IT respondents reported their current position is at or above the supervisory level.

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



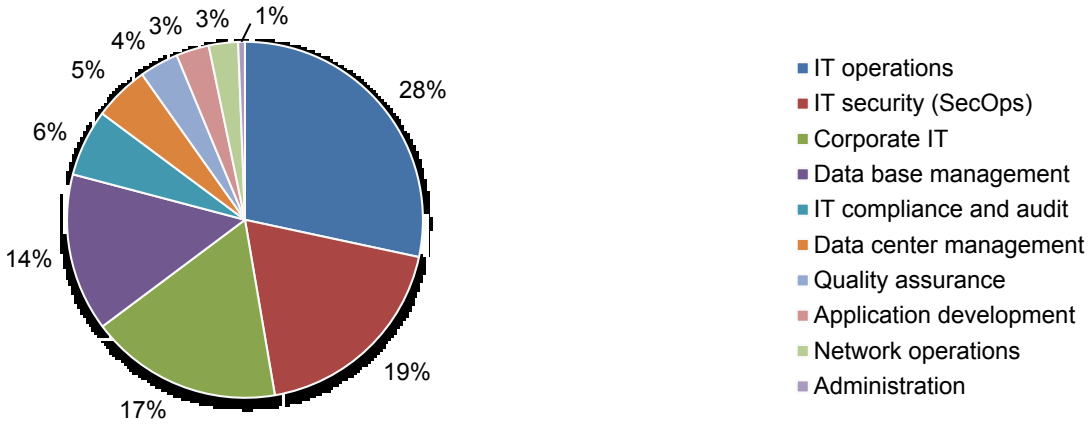
Pie chart 2 reports the current position or organization level of end user respondents. Fifty-three percent of end user respondents reported their current position is at or above the supervisory level.

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



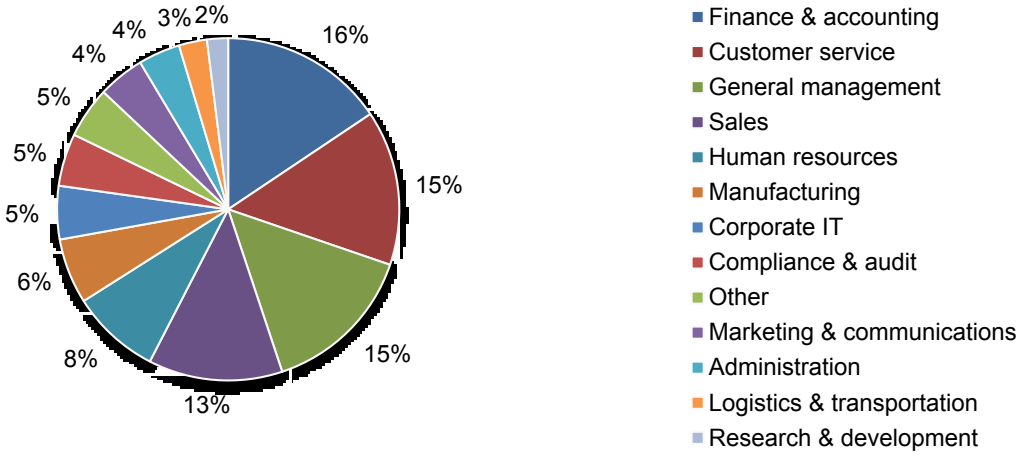
Pie chart 3 reveals the current department or function that best defines the role of the IT respondent. Twenty-eight percent indicated IT operations, 19 percent reported IT security and 17 percent identified corporate IT as their current role.

Pie Chart 3. Current role or department of IT respondent



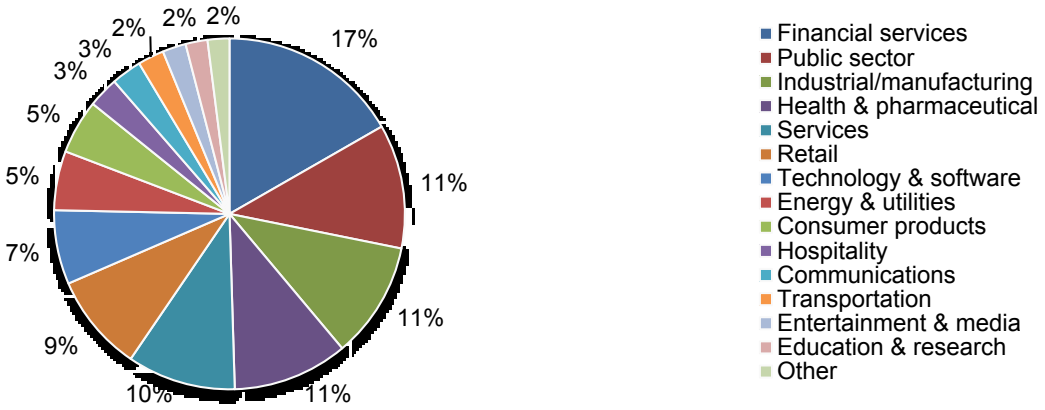
Pie chart 4 reveals the current department or function that best defines the role of the end user respondent. Sixteen percent indicated finance and accounting, 15 percent reported customer service and another 15 percent identified general management as their current role.

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



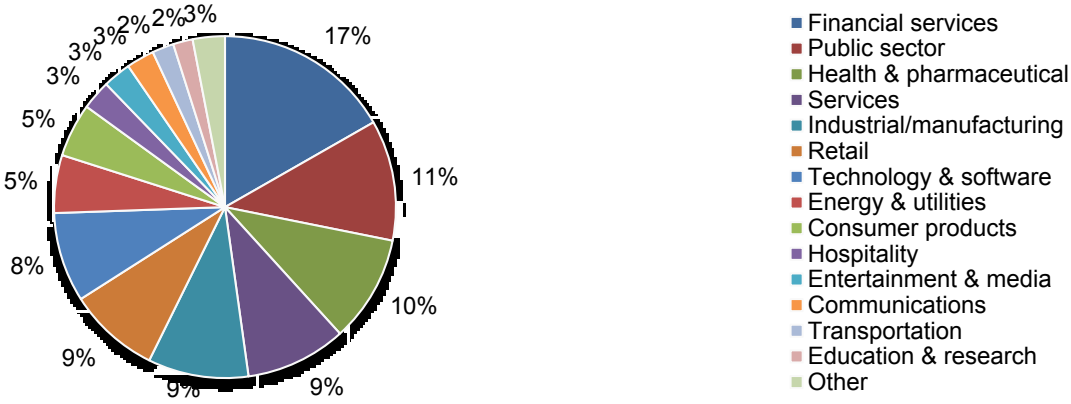
Pie Chart 5 reports the primary industry classification for the IT respondents' organizations. This chart identifies financial services (17 percent of respondents) as the largest segment, followed by public sector (11 percent) and health and industrial/manufacturing (11 percent).

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%

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 Comparison of IT and End User Survey Results

The following tables provide the frequency or percentage frequency of responses to survey questions that were asked of both IT and end user participants. All survey responses were captured in May and April 2016.

Survey 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%

Attributions: % Strongly agree and Agree responses combined.	IT	End User
Q1. Employees in my organization take appropriate steps to protect company data accessed by them.	52%	39%
Q2. The protection of company data is a top priority for our CEO and other C- level executives.	53%	35%

Q11. What best defines the level of priority your organization places on the protection of company data?	IT	End User
Very high priority	28%	17%
High priority	33%	21%
Moderate priority	29%	34%
Low priority	5%	16%
Not a priority	5%	12%
Total	100%	100%

Q13a. Has your organization detected employees accessing files and emails they were not authorized to see?	IT	End User
Yes	61%	62%
No	30%	38%
Unsure	9%	
Total	100%	100%

Q15a. Has your organization experienced ransomware (e.g. Cryptolocker)?	IT	End User
Yes	15%	9%
No	72%	78%
Unsure	13%	14%
Total	100%	100%

Q16a. In the past year, has access to company data tightened because of security requirements or concerns?	IT	End User
Yes	61%	43%
No	39%	57%
Total	100%	100%

Q19. Has your organization experienced the loss or theft of company data over the past two years?	IT	End User
Yes	76%	59%
No	16%	22%
Unsure	7%	19%
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?	IT	End User
Very frequently	12%	33%
Frequently	34%	40%
Not frequently	35%	19%
Rarely	19%	9%
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?	IT	End User
Very frequently	8%	9%
Frequently	26%	24%
Not frequently	33%	31%
Rarely	33%	36%
Total	100%	5%

Q23. Who is most likely to cause the compromise of insider accounts within your organization?	IT	End User
Insiders who are negligent	50%	58%
Malicious employees or contractors	16%	18%
External attackers	22%	23%
Others	2%	2%
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.