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

Release 3: Differences in Security Practices and Vigilance Across UK, France, Germany and US

Sponsored by Varonis

Independently conducted by Ponemon Institute LLC

Publication Date: October 2016

Closing Security Gaps to Protect Corporate Data:
A Study of US and European Organizations
Release 3: Differences in Security Practices and Vigilance Across UK, France, Germany and US

Ponemon Institute, October 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.

Release 1 of the 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, was titled "The Widening Gap Between IT and End Users," can be found here. Release 2 highlighted key findings in the examination of IT and end user practices and beliefs.

This report, the third and final release, issued October 3, 2016, is titled "Differences in Security Practices and Vigilance Across UK, France, Germany and US." Release 3 compares responses among the four countries.

All three releases are based on the same interviews and findings documented in the full report. This report includes Key Findings, Methods, and an Appendix with detailed comparisons of responses from end user employees and IT professionals in the US, UK, France, and Germany to a total of 42 questions.

Part 2. Key Findings

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.

Despite the differences among the four countries in this survey, employees and IT professionals indicate broadly consistent challenges and gaps.

Country-specific highlights:

Fifty percent of German employees say they take all appropriate steps to protect the company data they access and use, compared with 39 percent of UK employees, 37 percent of French employees and 35 percent of US employees.

Forty-four percent of German employees say their organizations strictly enforce policies against the misuse or unauthorized access to company data, well above the responses to the same question in the UK (35 percent), US (32 percent) and France (29 percent).

Thirty-nine percent of IT professionals in Germany say their organizations fully enforce a strict least privilege model (which means access to company data only on a need-to-know basis) for file shares and other collaborative data stores, much higher than the US (29 percent), France (25 percent) and UK (23 percent).

Although German IT pros are least likely to say their organizations have experienced ransomware (12 percent compared with 17 percent in the US, 16 percent in France and 13 percent in the UK), they express the highest levels of concern about the threat of ransomware (83 percent very or extremely concerned in Germany compared with 80 percent in France, 77 percent in the US and 63 percent in the UK).

Asked if their organizations have experienced the loss or theft of data in the last two years, the highest positive response among IT people was in the US (82 percent), followed by France (80 percent), UK (76 percent), and Germany (64 percent).

In Germany, both employee end users (30 percent) and IT staff (45 percent) are more likely than in the other countries to believe their management would accept a decline in productivity in order to prevent security risks. The same question produced less optimism about this balance in the UK (25 percent of employees, 34 percent of IT), France (23 percent of employees, 35 percent of IT), and the US (21 percent of employees, 30 percent of IT).

Employees in all four countries say insiders who are negligent are more likely to put the organization's data at risk than external attackers or insiders acting with malicious intent.

The top three security threats that most concern IT professionals differ in each country:

France: Insiders who are negligent: 67 percent, outside attackers who compromise insider credentials: 53 percent, malicious contractors: 40 percent
UK: Insiders who are negligent: 61 percent, outside attackers who compromise insider credentials: 55 percent, malware: 47 percent
US: Insiders who are negligent: 61 percent, outside attackers who compromise insider credentials: 55 percent, malware: 47 percent
Germany: Outside attackers who compromise insider credentials: 66 percent, malware: 46 percent, malicious contractors: 41 percent (insiders who are negligent was fourth: 36 percent)

Part 3. Conclusions

While cultural and business norms vary from country to country and can affect attitudes, preparedness and resistance to insider threats and cyberattacks, the continuing increase in data loss and theft is due in large part to these 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

- The lack of executive leadership in communicating the important responsibilities that every employee and contractor have in contributing to the protection of important and sensitive data
- The inadequate pace of modernization among IT and security professionals who have for years invested in protecting the perimeters of their networks and failed to adopt inside-out security technologies that protect the data itself and monitor its appropriate movement and use

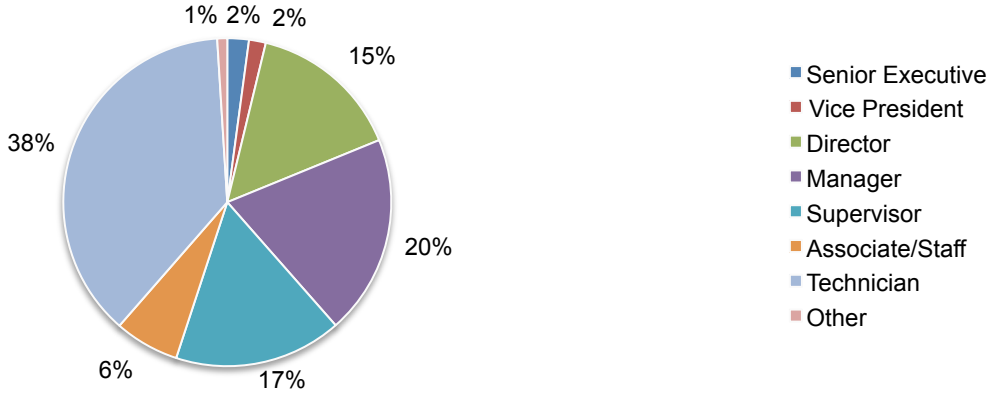
Part 4. Methods

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%

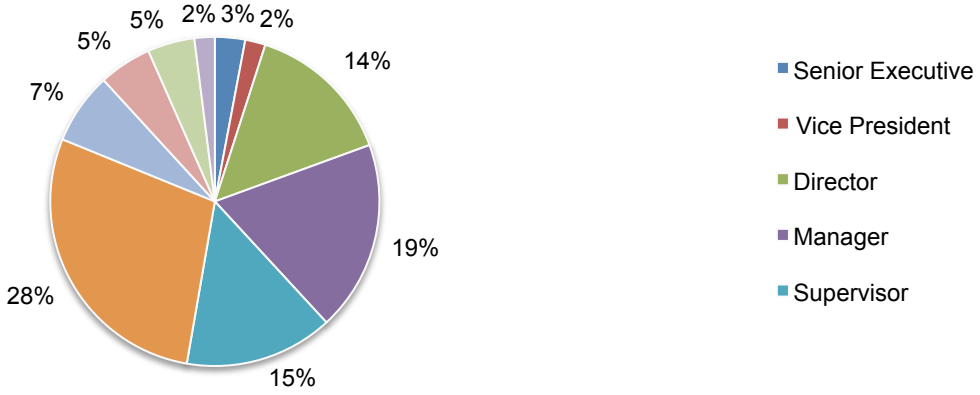
Pie chart 1 reports the current position or organization level of IT respondents. More than half (55 percent) of IT respondents reported their current position is at or above the supervisory level.

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



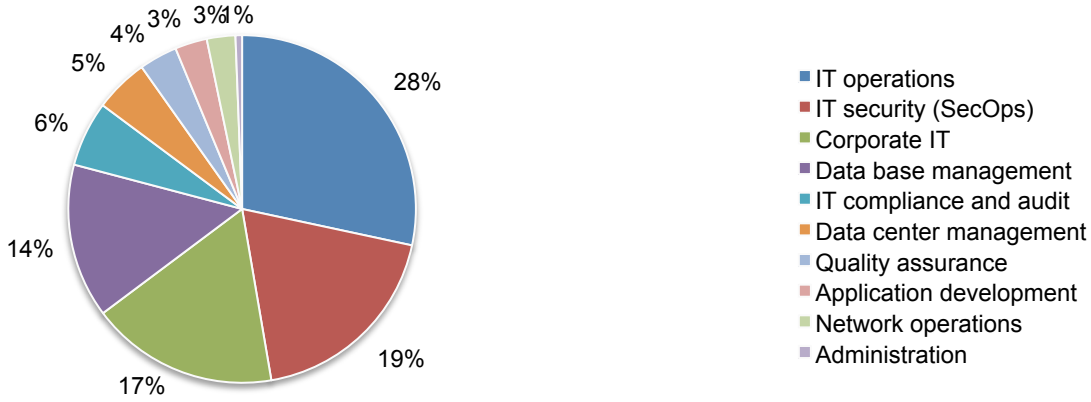
Pie chart 2 reports the current position or organization level of end user respondents. Fifty-three percent of end user respondents reported their current position is at or above the supervisory level.

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



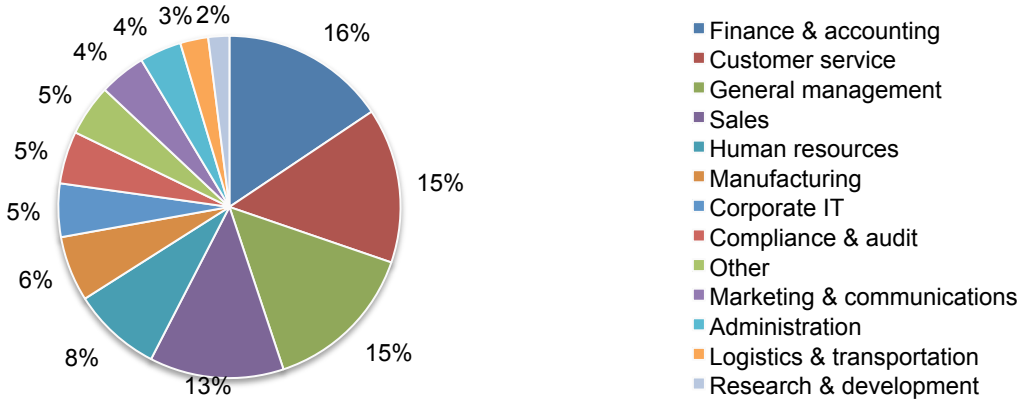
Pie chart 3 reveals the current department or function that best defines the role of the IT respondent. Twenty-eight percent indicated IT operations, 19 percent reported IT security and 17 percent identified corporate IT as their current role.

Pie Chart 3. Current role or department of IT respondent



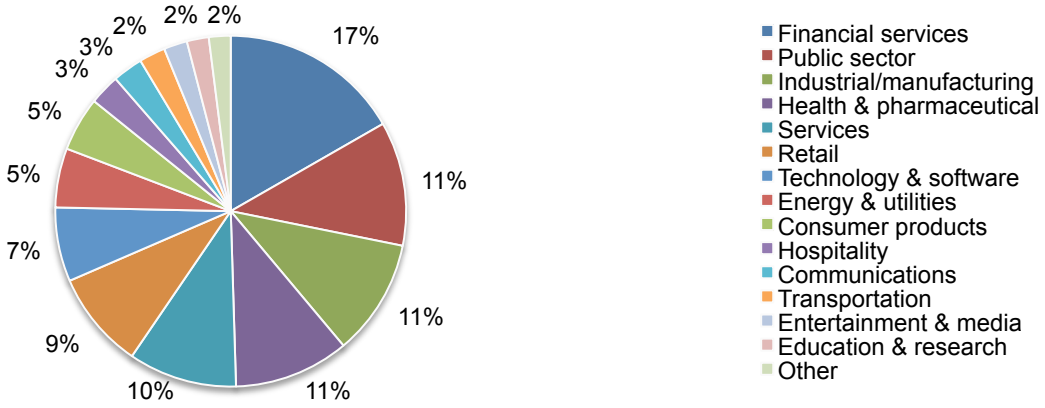
Pie chart 4 reveals the current department or function that best defines the role of the end user respondent. Sixteen percent indicated finance and accounting, 15 percent reported customer service and another 15 percent identified general management as their current role.

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



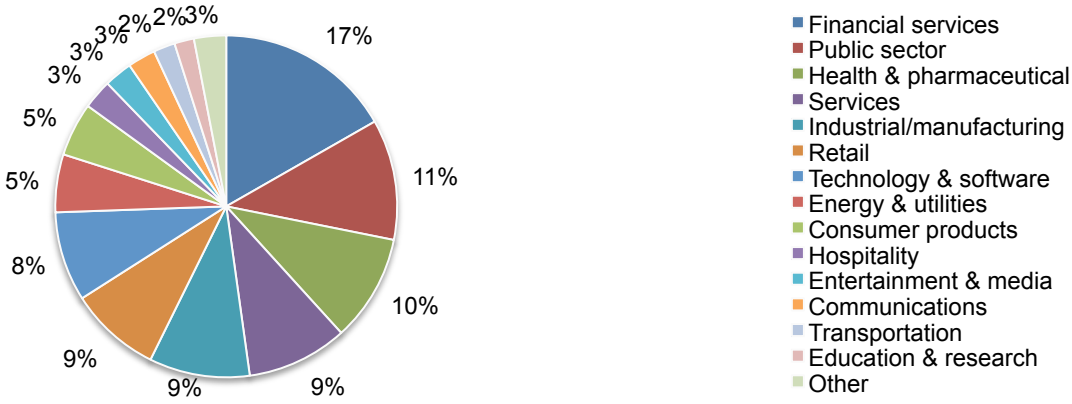
Pie Chart 5 reports the primary industry classification for the IT respondents' organizations. This chart identifies financial services (17 percent of respondents) as the largest segment, followed by public sector (11 percent) and health and industrial/manufacturing (11 percent).

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 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.

IT and IT security respondents by geography

	United States	United Kingdom	Germany	France	
Survey response IT GEO	US	UK	DE	FR	Combined
Total sampling frame	15,788	11,150	12,030	10,802	49,770
Total returns	646	403	415	378	1,842
Rejected or screened surveys	55	47	34	50	186
Final sample	591	356	381	328	1,656
Response rate	3.7%	3.2%	3.2%	3.0%	3.3%
Country weighting	0.36	0.21	0.23	0.20	1.00

Part 1. Attributions: % Strongly agree and Agree responses combined.	US	UK	DE	FR	Combined
Q1. Employees in my organization take appropriate steps to protect company data accessed by them.	49%	51%	60%	48%	52%
Q2. The protection of company data is a top priority for our CEO and other C-level executives.	52%	53%	58%	50%	53%
Q3. My organization strictly enforces its security policies related to use and access to company data.	47%	49%	63%	51%	52%

Part 2. General questions

Q4. What best describes the support and/or resources provided to the IT department to secure company data?	US	UK	DE	FR	Combined
Generous	14%	16%	15%	10%	14%
Adequate	46%	53%	66%	43%	52%
Insufficient	40%	31%	19%	47%	35%
Total	100%	100%	100%	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?	US	UK	DE	FR	Combined
Fully enforced	29%	23%	39%	25%	29%
Enforced for some stores but not others	23%	22%	30%	19%	24%
Enforced for some stores and in process for others	20%	26%	20%	18%	21%
Not enforced	28%	29%	11%	38%	26%
Total	100%	100%	100%	100%	100%

Q6. How often does the organization review the list of individuals who have access to file shares and other collaborative data stores?	US	UK	DE	FR	Combined
Never	25%	22%	16%	36%	24%
Monthly	9%	12%	6%	5%	8%
Quarterly	12%	21%	12%	9%	13%
Bi-annually	15%	10%	29%	11%	16%
Annually	39%	35%	37%	39%	38%
Total	100%	100%	100%	100%	100%

Q7. Does your organization have searchable records of file system activity (for example, opens, deletes, modifieds, renames) for company documents and files stored in file shares?	US	UK	DE	FR	Combined
Yes, and the record of activity is preserved for more than a year	30%	26%	23%	34%	28%
Yes, and the record of activity is preserved for more than a month	16%	15%	21%	10%	16%
Yes, and the record of activity is preserved for more than a week	20%	20%	28%	16%	21%
No, our organization does not maintain a searchable record of the file system activity	34%	39%	28%	40%	35%
Total	100%	100%	100%	100%	100%

Q8. In terms of volume, what data types does your organization have the most of?	US	UK	DE	FR	Combined
Application data, file shares and email stored on premises	85%	89%	88%	81%	86%
Application data, files shares and email stored in the cloud	15%	11%	12%	19%	14%
Total	100%	100%	100%	100%	100%

Q9. Which data types are likely to include the most critical or sensitive information?	US	UK	DE	FR	Combined
Application data, file shares and email stored on premises	86%	86%	91%	84%	86%
Application data, file shares and email stored in the cloud	14%	14%	9%	16%	14%
Total	100%	100%	100%	100%	100%

Q10. Which data types are least likely to be controlled by your organization?	US	UK	DE	FR	Combined
Application data, file shares and email stored on premises	14%	13%	7%	19%	13%
Application data, file shares and email stored in the cloud	86%	87%	93%	81%	87%
Total	100%	100%	100%	100%	100%

Q11. What best defines the level of priority your organization places on the protection of company data?	US	UK	DE	FR	Combined
Very high priority	31%	30%	26%	23%	28%
High priority	33%	28%	36%	34%	33%
Moderate priority	26%	31%	28%	33%	29%
Low priority	6%	6%	4%	5%	5%
Not a priority	4%	5%	6%	5%	5%
Total	100%	100%	100%	100%	100%

Q12. How much file and email activity do you monitor?	US	UK	DE	FR	Combined
All employee and third-party activity	34%	25%	19%	17%	25%
Some employee and third-party activity	19%	21%	18%	20%	19%
Some employee and third-party activity in response to management's request and the availability of technology	15%	19%	20%	18%	18%
Our organization does not monitor file and email activity	32%	35%	43%	45%	38%
Total	100%	100%	100%	100%	100%

Q13a. Has your organization detected employees accessing files and emails they were not authorized to see?	US	UK	DE	FR	Combined
Yes	66%	63%	56%	55%	61%
No	25%	24%	40%	36%	30%
Unsure	9%	13%	4%	9%	9%
Total	100%	100%	100%	100%	100%

Q13b. If yes, how quickly was this detected?	US	UK	DE	FR	Combined
Within 24 hours	25%	20%	32%	18%	24%
Within a week	19%	21%	23%	11%	19%
Within a month	12%	11%	19%	15%	14%
Within 6 months	22%	18%	18%	19%	20%
Within 1 year	8%	11%	5%	14%	9%
More than 1 year	14%	19%	3%	23%	14%
Total	100%	100%	100%	100%	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	US	UK	DE	FR	Combined
1 or 2	5%	7%	2%	0%	4%
3 or 4	6%	7%	3%	6%	6%
5 or 6	12%	13%	12%	14%	13%
7 or 8	36%	33%	27%	30%	32%
9 or 10	41%	40%	56%	50%	46%
Total	100%	100%	100%	100%	100%
Extrapolated value	7.54	7.34	8.14	7.98	7.72

Q15a. Has your organization experienced ransomware (e.g. Cryptolocker)?	US	UK	DE	FR	Combined
Yes	17%	13%	12%	16%	15%
No	69%	72%	80%	70%	72%
Unsure	14%	15%	8%	14%	13%
Total	100%	100%	100%	100%	100%

Q15b. If yes, how quickly was it detected?	US	UK	DE	FR	Combined
Within 24 hours	50%	51%	60%	55%	54%
Within a week	34%	35%	26%	32%	32%
Within a month	16%	11%	9%	13%	13%
Within 6 months	0%	3%	5%	0%	2%
Within 1 year	0%	0%	0%	0%	0%
More than 1 year	0%	0%	0%	0%	0%
Total	100%	100%	100%	100%	100%

Q16a. In the past year, has access to company data tightened because of security requirements or concerns?	US	UK	DE	FR	Combined
Yes	65%	63%	58%	55%	61%
No	35%	37%	42%	45%	39%
Total	100%	100%	100%	100%	100%

Q16b. If yes, how has tightened security affected the productivity of end users?	US	UK	DE	FR	Combined
No impact on end-user productivity	46%	46%	53%	46%	48%
Negative impact on end-user productivity	31%	29%	23%	30%	29%
Positive impact on end-user productivity	13%	14%	16%	11%	14%
Do not know	10%	11%	8%	13%	10%
Total	100%	100%	100%	100%	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?	US	UK	DE	FR	Combined
My organization would accept heightened security risk to maintain employee productivity	32%	31%	24%	32%	30%
My organization would accept diminished productivity to reduce security risk	30%	34%	45%	35%	35%
My organization is indifferent between productivity decline and security risk	31%	26%	26%	25%	28%
Cannot determine	7%	9%	5%	8%	7%
Total	100%	100%	100%	100%	100%

Q18. What is the impact of compliance on your organization's security posture?	US	UK	DE	FR	Combined
Significantly Improves security posture	30%	32%	39%	33%	33%
Improves security somewhat	36%	35%	36%	34%	35%
Purely a check the box activity	26%	25%	23%	28%	25%
Unsure	8%	8%	2%	5%	6%
Total	100%	100%	100%	100%	100%

Q19. Has your organization experienced the loss or theft of company data over the past two years?	US	UK	DE	FR	Combined
Yes	82%	76%	64%	80%	76%
No	11%	12%	30%	15%	16%
Unsure	7%	12%	6%	5%	7%
Total	100%	100%	100%	100%	100%

Q20. In your opinion, when leakage of company data occurs, how often does it happen because of insider mistakes, negligence or malice?	US	UK	DE	FR	Combined
Very frequently	14%	12%	7%	16%	12%
Frequently	37%	32%	26%	38%	34%
Not frequently	30%	35%	43%	35%	35%
Rarely	19%	21%	24%	11%	19%
Total	100%	100%	100%	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?	US	UK	DE	FR	Combined
Very frequently	8%	6%	8%	12%	8%
Frequently	26%	25%	24%	28%	26%
Not frequently	34%	35%	30%	31%	33%
Rarely	32%	34%	38%	29%	33%
Total	100%	100%	100%	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?	US	UK	DE	FR	Combined
Very frequently	5%	7%	8%	11%	7%
Frequently	13%	12%	9%	15%	12%
Not frequently	49%	50%	55%	45%	50%
Rarely	33%	31%	28%	29%	31%
Total	100%	100%	100%	100%	100%

Q23. Who is most likely to cause the compromise of insider accounts within your organization?	US	UK	DE	FR	Combined
Insiders who are negligent	54%	56%	40%	49%	50%
Malicious employees	12%	11%	13%	17%	13%
Malicious contractors	11%	10%	16%	15%	13%
External attackers	21%	20%	27%	19%	22%
Others	2%	3%	4%	0%	2%
Total	100%	100%	100%	100%	100%

Q24. Which of the following security threats does your organization worry most about? Please select the top three.	US	UK	DE	FR	Combined
Insiders who are negligent	61%	56%	36%	67%	55%
Malicious employees	21%	22%	20%	25%	22%
Malicious contractors	35%	30%	41%	40%	36%
Outside attackers who compromise insider credentials	55%	60%	66%	53%	58%
Malware	47%	44%	46%	37%	44%
Privileged users who abuse access	24%	19%	18%	20%	21%
DDoS attacks	38%	48%	51%	37%	43%
Website defacing	15%	16%	17%	15%	16%
Others	4%	5%	5%	6%	5%
Total	300%	300%	300%	300%	300%

Part 3: Organizational characteristics and demographics

D1. What organizational level best describes your present position?	US	UK	DE	FR	Combined
Senior Executive	3%	2%	1%	2%	2%
Vice President	1%	1%	3%	2%	2%
Director	17%	14%	13%	15%	15%
Manager	22%	18%	20%	17%	20%
Supervisor	15%	18%	18%	16%	17%
Associate/Staff	6%	7%	5%	8%	6%
Technician	35%	38%	40%	39%	38%
Other	1%	2%	0%	1%	1%
Total	100%	100%	100%	100%	100%

D2. Check the department or function that best defined your role.	US	UK	DE	FR	Combined
Corporate IT	16%	15%	19%	21%	17%
IT security (SecOps)	23%	19%	16%	15%	19%
Data base management	15%	13%	14%	15%	14%
IT operations	29%	32%	26%	26%	28%
Network operations	2%	0%	5%	4%	3%
IT compliance and audit	5%	6%	7%	7%	6%
Application development	3%	4%	2%	3%	3%
Data center management	5%	6%	5%	4%	5%
Quality assurance	2%	4%	6%	3%	4%
Administration	0%	1%	0%	2%	1%
Total	100%	100%	100%	100%	100%

D3. What is the worldwide headcount of your organization?	US	UK	DE	FR	Combined
Fewer than 500 people	8%	11%	8%	12%	9%
500 to 1,000 people	11%	14%	16%	20%	15%
1,001 to 5,000 people	36%	41%	32%	39%	37%
5,001 to 25,000 people	25%	19%	26%	17%	22%
25,001 to 75,000 people	12%	10%	13%	9%	11%
More than 75,000 people	8%	5%	5%	3%	6%
Total	100%	100%	100%	100%	100%

D4. What industry best describes your organization's industry concentration or focus?	US	UK	DE	FR	[
Agriculture & food services	1%	1%	0%	3%	1%
Communications	3%	2%	3%	3%	3%
Consumer products	5%	6%	4%	5%	5%
Defense & aerospace	1%	0%	0%	0%	0%
Education & research	2%	3%	2%	1%	2%
Energy & utilities	5%	6%	6%	5%	5%
Entertainment & media	3%	2%	2%	1%	2%
Financial services	18%	16%	15%	17%	17%
Health & pharmaceutical	11%	9%	12%	10%	11%
Hospitality	2%	3%	2%	5%	3%
Industrial/manufacturing	10%	11%	13%	9%	11%
Public sector	11%	13%	11%	11%	11%
Retail	9%	9%	8%	10%	9%
Services	10%	9%	10%	11%	10%
Technology & software	7%	6%	8%	6%	7%
Transportation	2%	3%	2%	3%	2%
Other	0%	1%	2%	0%	1%
Total	100%	100%	100%	100%	100%

Employee end user respondents by geography	United States	United Kingdom	Germany	France	
Survey response End User GEO	US	UK	DE	FR	Combined
Total sampling frame	14,320	9,880	10,001	9,535	43,736
Total returns	561	326	309	298	1,494
Rejected or screened surveys	43	27	20	33	123
Final sample	518	299	289	265	1,371
Response rate	3.6%	3.0%	2.9%	2.8%	3.1%
Country weighting	0.38	0.22	0.21	0.19	1.00

Part 1. Attributions: % Strongly agree and Agree response combined	US	UK	DE	FR	Combined
Q1. I take all appropriate steps to protect company data accessed and used by me.	35%	39%	50%	37%	39%
Q2. My organization strictly enforces its policies against the misuse or unauthorized access to company data.	32%	35%	44%	29%	35%
Q3. My organization's IT function knows where my sensitive information is stored.	31%	30%	41%	29%	33%

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?	US	UK	DE	FR	Combined
Yes	88%	86%	91%	86%	88%
No (stop)	12%	14%	9%	14%	12%
Total	100%	100%	100%	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.	US	UK	DE	FR	Combined
Customer information including contact lists	55%	57%	49%	61%	55%
Email and attachments	97%	93%	90%	95%	94%
Employee records	28%	26%	23%	26%	26%
Student records	3%	2%	0%	1%	2%
Patient records	15%	11%	8%	9%	11%
Non-financial business information	78%	68%	73%	67%	73%
Financial information	33%	25%	30%	33%	31%
Source code	11%	8%	9%	10%	10%
Other intellectual properties	15%	10%	8%	13%	12%
Total	335%	300%	290%	315%	314%

Q6a. Is there company data you have access to that you think you probably should not see?	US	UK	DE	FR	Combined
Yes	64%	68%	55%	60%	62%
No	36%	32%	45%	40%	38%
Total	100%	100%	100%	100%	100%

Q6b. If yes, how often does this happen to you or your co-workers?	US	UK	DE	FR	Combined
Very frequently	18%	20%	9%	19%	17%
Frequently	32%	26%	31%	30%	30%
Not frequently	43%	45%	50%	43%	45%
Rarely	7%	9%	10%	8%	8%
Total	100%	100%	100%	100%	100%

Q6c. If yes, how much data would you or your co-workers likely see?	US	UK	DE	FR	Combined
A lot of data	44%	37%	27%	35%	37%
Some data	26%	28%	23%	24%	25%
A little data	23%	30%	46%	36%	32%
Unsure	7%	5%	4%	5%	6%
Total	100%	100%	100%	100%	100%

Q7. Which one statement best describes your access privileges to company data?	US	UK	DE	FR	Combined
My access privileges are too limited and at times prevent me from doing my job.	40%	43%	30%	42%	39%
My access privileges appropriately match what I need to do my job.	35%	32%	56%	35%	39%
My access privileges are broader than what is necessary to do my job.	20%	19%	11%	17%	17%
Unsure	5%	6%	3%	6%	5%
Total	100%	100%	100%	100%	100%

Q8. Typically, how long do you retain/store documents or files you have created or worked on?	US	UK	DE	FR	Combined
Hours	6%	5%	9%	4%	6%
Days	4%	5%	6%	5%	5%
Weeks	9%	10%	12%	8%	10%
Months	12%	13%	15%	6%	12%
One year	10%	8%	5%	11%	9%
More than one year	16%	19%	16%	15%	16%
Forever (no time limit or plan to delete)	43%	40%	37%	51%	43%
Total	100%	100%	100%	100%	100%

Q9. How often do you delete files?	US	UK	DE	FR	Combined
Daily, or as I finish with them	11%	9%	16%	8%	11%
Weekly	8%	10%	12%	9%	9%
Monthly	13%	14%	14%	6%	12%
Yearly	9%	8%	6%	13%	9%
Rarely, or less often than once a year	16%	18%	14%	14%	16%
Never	43%	41%	38%	50%	43%
Total	100%	100%	100%	100%	100%

Q10. What best defines the level of priority your organization places on the protection of company data?	US	UK	DE	FR	Combined
Very high priority	16%	15%	21%	15%	17%
High priority	21%	23%	20%	19%	21%
Moderate priority	33%	34%	35%	37%	34%
Low priority	15%	16%	17%	18%	16%
Not a priority	15%	12%	7%	11%	12%
Total	100%	100%	100%	100%	100%

Q11 In the past year, has access to company data tightened because of security requirements or concerns?	US	UK	DE	FR	Combined
Yes	45%	43%	44%	40%	43%
No	55%	57%	56%	60%	57%
Total	100%	100%	100%	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?	US	UK	DE	FR	Combined
My management would accept heightened security risk to maintain employee productivity	51%	48%	40%	50%	48%
My management would accept productivity decline to prevent security risk	21%	25%	30%	23%	24%
My management would be indifferent between security risks and productivity decline	20%	18%	25%	18%	20%
Cannot determine	8%	9%	5%	9%	8%
Total	100%	100%	100%	100%	100%

Q13. Has your organization experienced the loss or theft of company data over the past two years?	US	UK	DE	FR	Combined
Yes	63%	57%	53%	59%	59%
No	17%	24%	32%	20%	22%
Unsure	20%	19%	15%	21%	19%
Total	100%	100%	100%	100%	100%

Q14. In your opinion, when leakage of company data occurs, how often does it happen because of insider mistakes, negligence or malice?	US	UK	DE	FR	Combined
Very frequently	35%	33%	24%	37%	33%
Frequently	40%	41%	38%	39%	40%
Infrequently	18%	16%	27%	15%	19%
Rarely	7%	10%	11%	9%	9%
Total	100%	100%	100%	100%	100%

Q15. In your opinion, when leakage of company data occurs, how often does it happen because of external attackers or hackers?	US	UK	DE	FR	Combined
Very frequently	9%	7%	8%	11%	9%
Frequently	23%	24%	21%	30%	24%
Infrequently	33%	32%	29%	29%	31%
Rarely	35%	37%	42%	30%	36%
Total	100%	100%	100%	100%	100%

Q16. Who is most likely to put your organization's data at risk?	US	UK	DE	FR	Combined
Insiders who are negligent	60%	61%	53%	57%	58%
Insiders who have malice	17%	16%	16%	23%	18%
External attackers	21%	23%	28%	19%	23%
Other (please specify)	2%	0%	3%	1%	2%
Total	100%	100%	100%	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?	US	UK	DE	FR	Combined
Yes	50%	46%	35%	36%	43%
No	36%	40%	55%	51%	44%
Unsure	14%	14%	10%	13%	13%
Total	100%	100%	100%	100%	100%

Q17b. If yes, does knowing that make you less likely to take company data with you if you left your job?	US	UK	DE	FR	Combined
Yes	56%	54%	49%	58%	54%
No	34%	36%	43%	30%	36%
Unsure	10%	10%	8%	12%	10%
Total	100%	100%	100%	100%	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?	US	UK	DE	FR	Combined
Yes	12%	8%	6%	7%	9%
No	73%	79%	82%	80%	78%
Unsure	15%	13%	12%	13%	14%
Total	100%	100%	100%	100%	100%

Q18b. If yes, how was the infection detected?	US	UK	DE	FR	Combined
Ransomware notice prompting user to pay	20%	17%	15%	23%	19%
Detected by IT before it became a significant issue	70%	74%	75%	65%	71%
Unsure	10%	9%	10%	12%	10%
Total	100%	100%	100%	100%	100%

Q18c. If IT detected the ransomware, how successful was the recovery?	US	UK	DE	FR	Combined
Files were restored promptly with minimal disruption to productivity	13%	6%	21%	5%	12%
Files took days or weeks to recover	26%	23%	24%	28%	25%
We never got our files back	49%	52%	40%	47%	47%
Unsure	12%	19%	15%	20%	16%
Total	100%	100%	100%	100%	100%

Q18d. If a notice to pay was received, did your organization pay the ransom?	US	UK	DE	FR	Combined
Yes	12%	10%	15%	16%	13%
No	88%	90%	85%	84%	87%
Total	100%	100%	100%	100%	100%

Part 3: Organizational characteristics and demographics

D1. What organizational level best describes your present position?	US	UK	DE	FR	Combined
Senior Executive	3%	2%	3%	4%	3%
Vice President	2%	2%	2%	2%	2%
Director	16%	12%	13%	16%	14%
Manager	20%	16%	20%	18%	19%
Supervisor	15%	16%	14%	13%	15%
Associate/staff	28%	33%	26%	27%	28%
Technician	6%	7%	9%	7%	7%
Administrative	5%	6%	4%	6%	5%
Contractor/consultant	3%	5%	5%	7%	5%
Intern	2%	0%	1%	0%	1%
Other	0%	1%	3%	0%	1%
Total	100%	100%	100%	100%	100%

D2. Check the department or function that best defined your role.	US	UK	DE	FR	Combined
General management	14%	16%	14%	15%	15%
Finance & accounting	16%	15%	17%	14%	16%
Corporate IT	4%	5%	7%	5%	5%
Sales	15%	11%	10%	13%	13%
Marketing & communications	4%	5%	3%	6%	4%
Customer service	13%	15%	16%	16%	15%
Logistics & transportation	2%	4%	3%	2%	3%
Human resources	8%	9%	9%	8%	8%
Manufacturing	7%	4%	8%	5%	6%
Research & development	2%	3%	0%	3%	2%
Compliance & audit	6%	3%	6%	4%	5%
Administration	5%	4%	2%	4%	4%
Other	4%	6%	5%	5%	5%
Total	100%	100%	100%	100%	100%

D3. What is the worldwide headcount of your organization?	US	UK	DE	FR	Combined
Fewer than 500 people	9%	12%	8%	11%	10%
500 to 1,000 people	10%	13%	14%	21%	14%
1,001 to 5,000 people	35%	40%	33%	38%	36%
5,001 to 25,000 people	26%	20%	27%	18%	23%
25,001 to 75,000 people	13%	11%	12%	9%	12%
More than 75,000 people	7%	4%	6%	3%	5%
Total	100%	100%	100%	100%	100%

D4. What defines your age range?	US	UK	DE	FR	Combined
18 to 28	28%	26%	24%	25%	26%
29 to 39	36%	37%	36%	34%	36%
40 to 50	18%	20%	24%	26%	21%
51 to 60	12%	13%	13%	12%	12%
60+	6%	4%	3%	3%	4%
Total	100%	100%	100%	100%	100%

D5. What industry best describes your organization's industry concentration or focus?	US	UK	DE	FR	Combined
Agriculture & food services	1%	2%	0%	3%	1%
Communications	2%	3%	2%	4%	3%
Consumer products	5%	6%	4%	5%	5%
Defense & aerospace	1%	0%	0%	0%	0%
Education & research	1%	2%	3%	2%	2%
Energy & utilities	5%	6%	5%	6%	5%
Entertainment & media	2%	3%	3%	3%	3%
Financial services	19%	16%	15%	14%	17%
Health & pharmaceutical	11%	9%	11%	8%	10%
Hospitality	3%	2%	1%	5%	3%
Industrial/manufacturing	9%	8%	11%	10%	9%
Public sector	10%	13%	12%	11%	11%
Retail	9%	8%	7%	10%	9%
Services	9%	9%	11%	9%	9%
Technology & software	9%	7%	9%	8%	8%
Transportation	2%	2%	3%	1%	2%
Other	2%	4%	3%	1%	2%
Total	100%	100%	100%	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.