Ponemon INSTITUTE

The Second Annual Study on the Cybersecurity Risk to Knowledge Assets

Co-authored by Kilpatrick Townsend and Ponemon Institute

Independently conducted by Ponemon Institute LLC

Publication Date: April 2018

KILPATRICK TOWNSEND

The Second Annual Study on the Cybersecurity Risk to Knowledge Assets

Kilpatrick Townsend and Ponemon Institute, Aprll 2018

Part 1. Introduction

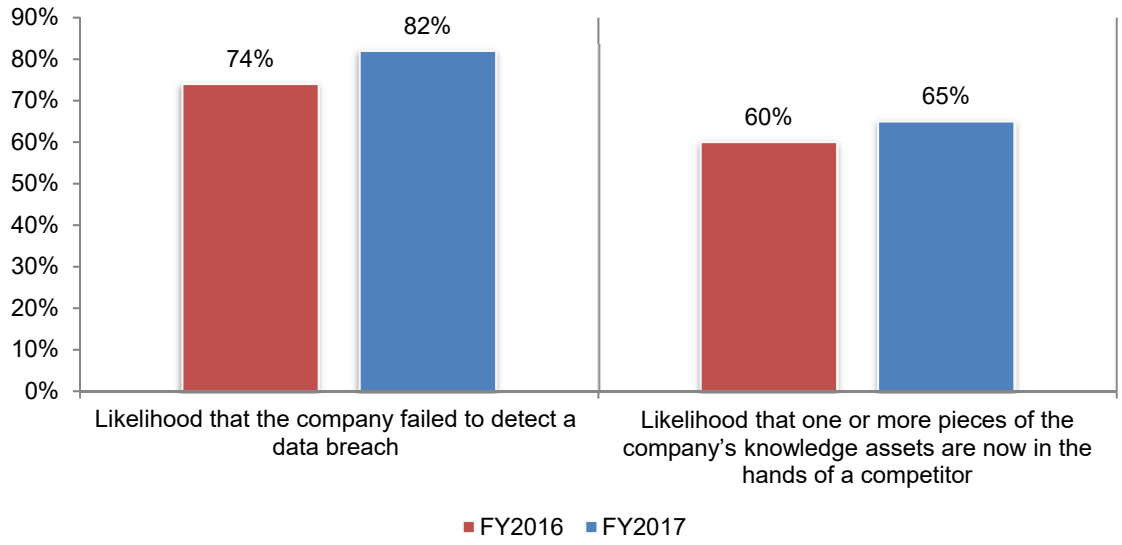
The Second Annual Study on the Cybersecurity Risk to Knowledge Assets[1], produced in collaboration between Kilpatrick Townsend and Ponemon Institute, was done to see whether and in what ways organizations are beginning to focus on how they are safeguarding confidential information critical to the development, performance and marketing of their core businesses in a period of targeted attacks on these assets.

Ponemon Institute surveyed 634 IT security practitioners who are familiar and involved with their organization's approach to managing knowledge assets. All organizations represented in this study have a program or set of activities for managing knowledge assets. The first study, *Cybersecurity Risk to Knowledge Assets,* was released in July 2016.

Awareness of the risk to knowledge assets increases. As shown in Figure 1, more respondents acknowledge that their companies very likely failed to detect a breach involving knowledge assets (an increase from 74 percent of respondents in 2016 to 82 percent of respondents in this year's research). Moreover, in this year's research, 65 percent of respondents are aware that one or more pieces of the company's knowledge assets are now in the hands of a competitor, an increase from 60 percent of respondents in the 2016 study.

Figure 1. The likelihood high value assets have been breached and possibly in the possession of a competitor

Very likely and Likely responses combined



The cost to recover from an attack against knowledge assets increases. The average total cost incurred by organizations represented in this research due to the loss, misuse or theft of knowledge assets over the past 12 months increased 26 percent from $5.4 million to $6.8 million.

[1] These knowledge assets do not include personal information that triggers notice requirements when a data breach occurs. Knowledge assets may include trade secrets and corporate confidential information such as profiles of high-value customers, product design, development and pricing, pre-release financial reports, strategic plans, confidential information about existing relationships or contemplated transactions, source code, or research and development secrets, any of which may reside within the company or with its partners or vendors.

Eighty-four percent of respondents state that the maximum loss their organizations could experience as a result of a material breach of knowledge assets is greater than $100 million as compared to 67 percent of respondents in 2016.

Actions taken that support the growing awareness of the risk to knowledge assets

Following are findings that illustrate how the growing awareness of the risk to knowledge assets is improving cybersecurity practices in many of the companies represented in this study.

- Companies are making the protection of knowledge assets an integral part of their IT security strategy (68 percent of respondents vs. 62 percent of respondents in 2016).
- Boards of directors are requiring assurances that knowledge assets are managed and safeguarded appropriately (58 percent of respondents vs. 50 percent of respondents in 2016).
- Companies are addressing the risk of employee carelessness in the handling of knowledge assets. Specifically, training and awareness programs are focused on decreasing employee errors in the handling of sensitive and confidential information (73 percent of respondents) and confirming employees' understanding and ability to apply what they learn to their work (68 percent of respondents).
- Companies are adopting specific technologies designed to protect knowledge assets. The ones for which use is increasing most rapidly include big data analytics, identity management and authentication and SIEM.
- There is a greater focus on assessing which knowledge assets are more difficult to secure and will require stricter safeguards for their protection. These are presentations, product/market information and private communications.
- There is greater recognition that third party access to a company's knowledge assets is a significant risk. As a result, more companies are requiring proof that the third party meets generally accepted security requirements (an increase from 31 percent of respondents in 2016 to 41 percent in this year's study) and proof that the third party adheres to compliance mandates (an increase from 25 percent of respondents in 2016 to 34 percent in this year's study).
- Companies are aware that nation-state attackers are targeting their company's knowledge assets (an increase from 50 percent to 61 percent in this year's study) and 79 percent of respondents believe their companies' trade secrets or knowledge assets are very valuable or valuable to a nation-state attacker.

Best practices and insights of organizations most effective in safeguarding knowledge assets

As part of the research, we did a special analysis of those respondents (89 respondents out of the total sample of 634 respondents) who rated their organizations' effectiveness in protecting their knowledge assets as very high (9+ on a scale of 1 = not effective to 10 = highly effective). In this study, effectiveness means mitigating the loss or theft of knowledge assets by insiders and external attackers.

Following are characteristics of high performing organizations:

- Senior management and boards of directors in high performing organizations are more concerned about the leakage of their organizations' knowledge assets and require assurances that knowledge assets are managed and safeguarded appropriately.

- High performing organizations are more likely to restrict employee access to knowledge assets based on need to know.

- High performing organizations are more likely to conduct audits to ensure adherence to their practices and policies that safeguard knowledge assets. They are significantly more likely to have independent audits by third parties.

- High performing organizations are more likely to conduct regular training and awareness programs and audits and assessments of areas most vulnerable to employee negligence.

- High performing organizations say a key characteristic of their training programs is the ability to result in a decrease of employee errors in the handling of sensitive and confidential information. Their training programs are more likely to be able to determine employees' understanding and ensure employees are able to apply what they learn to their work. The programs are also customized based on the role and handling of sensitive and confidential information.

- High-value knowledge assets are more secure in high performing organizations. Six knowledge assets that high performing organizations are more effective in safeguarding are source code, financial information, trade secrets, company-confidential information, private communications and analytics.

- High performing organizations are more likely to use certain technologies and processes specifically used to protect knowledge assets. More respondents in high performing organizations report they are using identity & access management, privileged user management, access governance and data loss prevention.

- High performing organizations are more likely than other organizations to detect and contain breaches of knowledge assets. More high performing organizations are restricting access to only those who have a need to know and a role in the prevention of breaches.

- More high performing organizations have achieved a mature level of digital transformation and have either deployed many digital transformation activities across the enterprise or have core digital transformation activities deployed. They are also more likely to say it is important to balance the security of their high value assets while enabling the free flow of information and an open business model.

- High performing organizations are faster at identifying a data breach involving knowledge assets caused by a malicious outsider or careless insider. High performing organizations on average reduce the (MTTI) to identify a data breach involving a knowledge asset caused by a malicious outsider by more than 90 days and the MTTI to identify a breach by a careless insider by 58 days.

- High performing organizations are faster at containing a data breach involving knowledge assets caused by a malicious outsider or careless insider. High performing organizations on average reduce the (MTTC) to identify a data breach involving a knowledge asset caused by a malicious outsider by more than 34 days and the MTTC to identify a breach by a careless insider by 32.54 days.

Part 2. Key findings

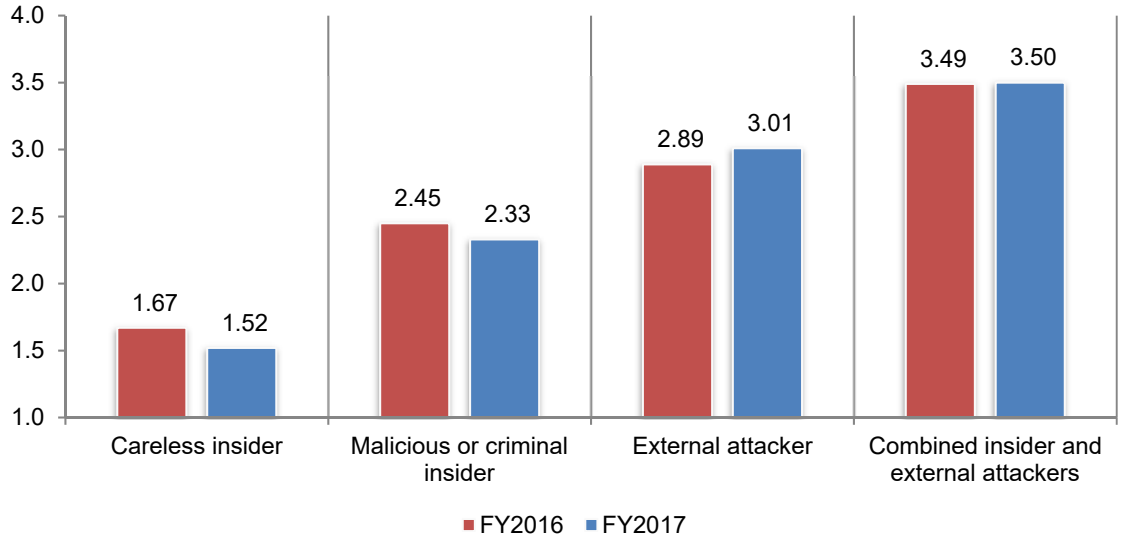
This section provides a more detailed analysis of the findings. The complete audited findings are presented in the Appendix of this report. The report is organized according to the following themes.

- Awareness grows about the vulnerability of knowledge assets to security exploits
- The insider threat to knowledge assets
- Trends in the risk to knowledge assets
- Governance practices for knowledge assets
- The cost of an insider or malicious outsider attack on knowledge assets
- The practices of organizations highly effective in safeguarding knowledge assets

Awareness grows about the vulnerability of knowledge assets to security exploits

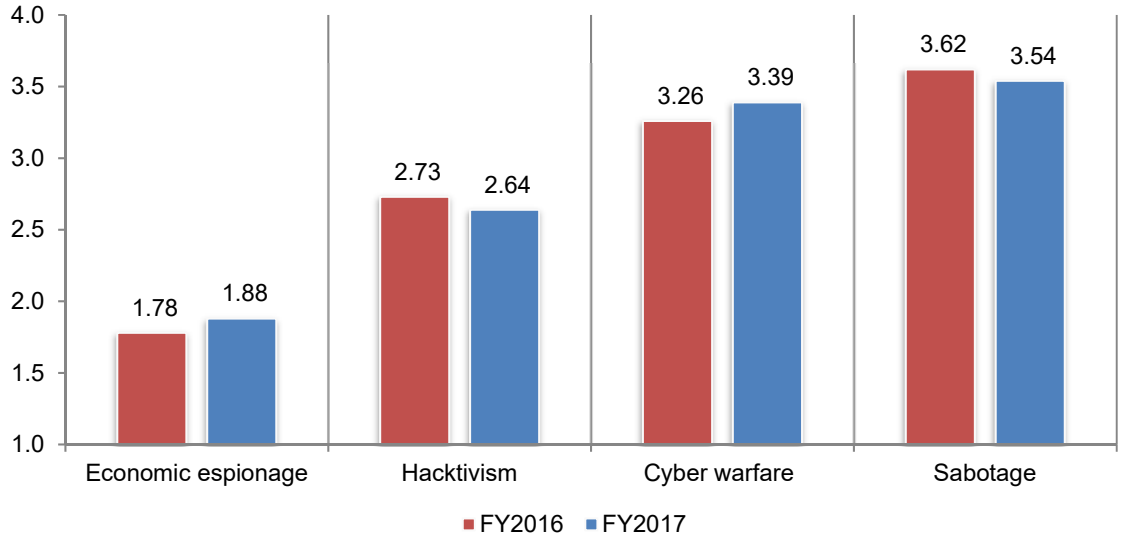
Insiders pose the greatest risk to knowledge assets. Respondents were asked to rank the most likely root causes involving the loss or theft of knowledge assets from 1 = most likely to 4 = least likely. As shown in Figure 2, the most likely causes are careless insiders and malicious or criminal insiders. These root causes have increased in likelihood since 2016.

Figure 2. What are the most likely root causes of data breaches involving your company's knowledge assets?
1 = most likely to 4 = least likely



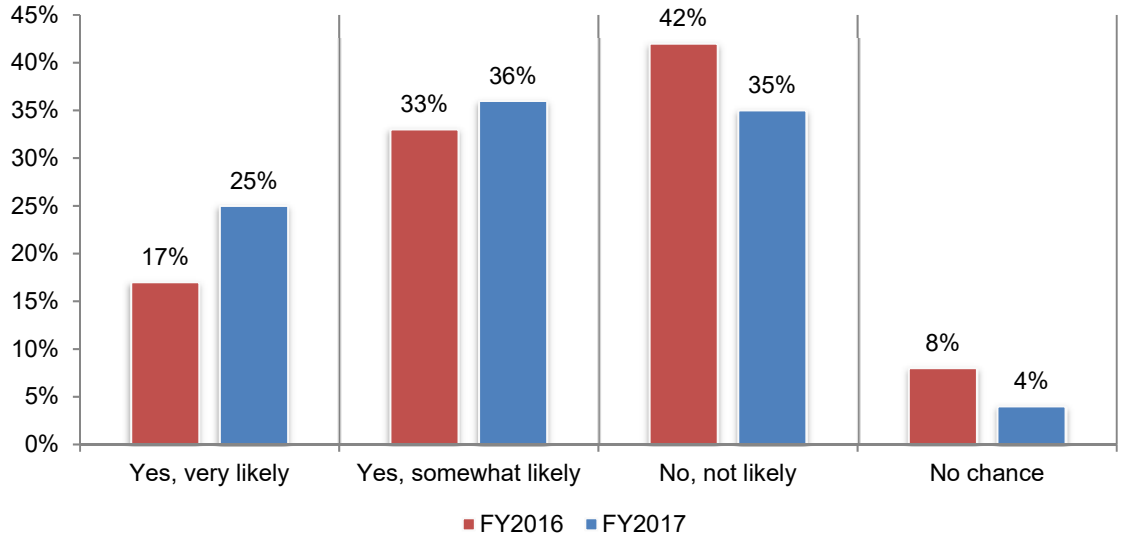
Economic espionage and hacktivism are the main motivations of attackers. Respondents were asked to rank the motivations of attackers from 1 = most likely to 4 = least likely. According to Figure 3, the most likely motivations are economic espionage and hacktivism. The third most likely motive is cyber warfare or nation-state attacks.

Figure 3. Why are attackers motivated to steal knowledge assets?
1 = most likely to 4 = least likely



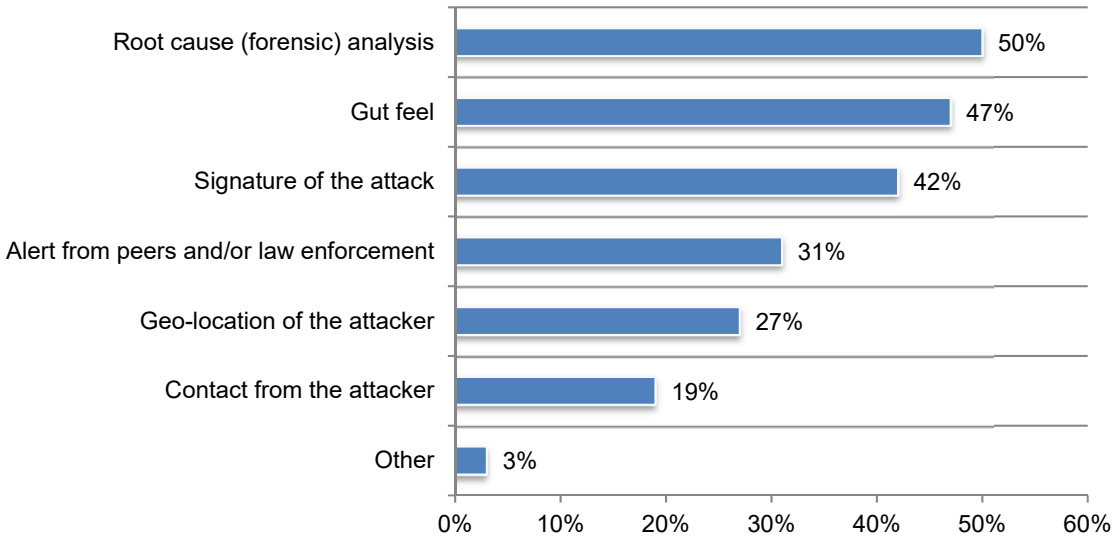
Awareness about the possibility of a nation-state attack against knowledge assets increases. As shown in Figure 4, the likelihood of a nation state attacker targeting a company's knowledge assets is increasing from 50 percent of respondents (17 percent + 33 percent) to 61 percent of respondents (25 percent + 36 percent).

Figure 4. Do you believe nation state attackers target your company's knowledge assets?



If respondents are aware of the possibility their companies' knowledge assets have been targeted, only half say it is because of root cause or forensic analysis, according to Figure 5. However, 47 percent of respondents say it was gut feel. Forty-two percent of respondents say it was the signature of the attack and 31 percent of respondents say it was an alert from peers and/or law enforcement.

Figure 5. If likely, how do you know if nation state attackers have targeted your company's knowledge assets?
More than one response allowed

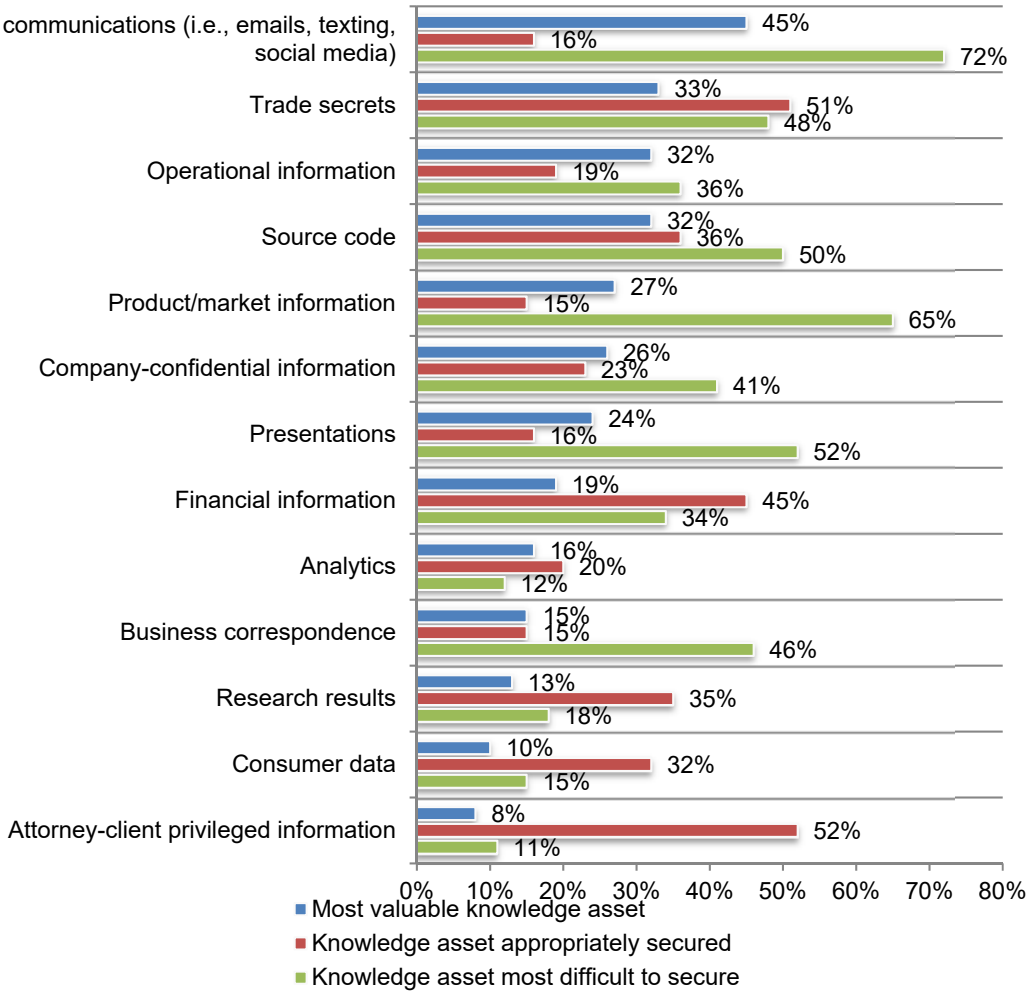


There is a gap in the ability to secure the most valuable knowledge assets. Figure 6 presents 13 types of knowledge assets and responses to the following questions: What knowledge assets are most valuable to a nation state attacker or competitor, what knowledge assets are most difficult to secure and what knowledge assets are appropriately secured?

As shown, private communications (i.e. emails, texting, social media) are considered most valuable to nation state attackers or competitors (45 percent of respondents). However, only 16 percent of respondents say these knowledge assets are appropriately secured. Seventy-two percent of respondents say these assets are difficult to secure.

Knowledge assets that are typically well-secured are attorney-client privileged information and knowledge assets recognized as trade secrets (52 percent and 51 percent of respondents, respectively). Also difficult to secure are product/market information and presentations (65 percent and 52 percent of respondents, respectively).

Figure 6. The knowledge asset security gap
Three responses allowed

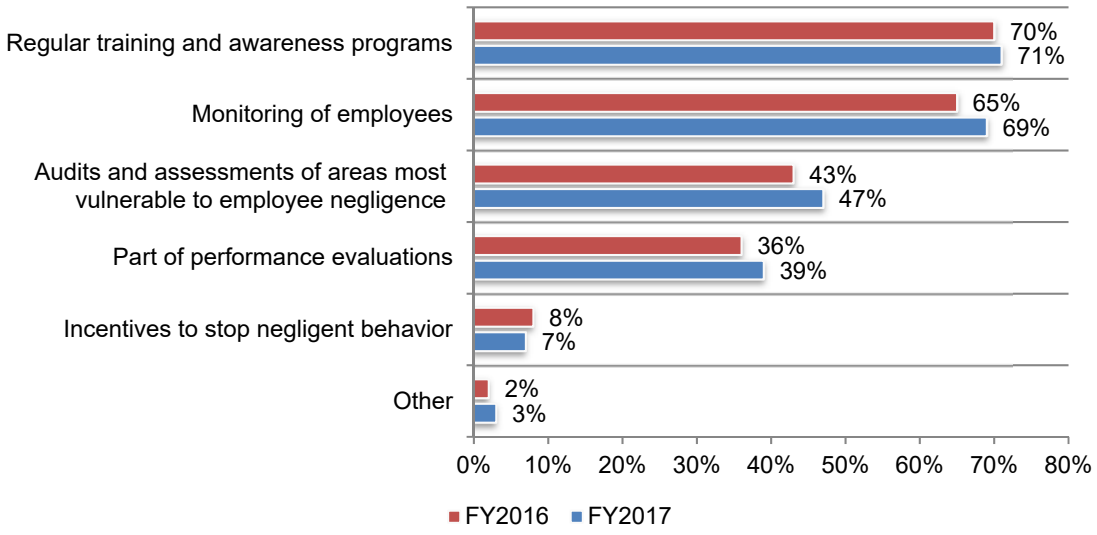


The insider threat to knowledge assets

More companies are taking steps to address the risk of employee carelessness in the handling of knowledge assets. Because the careless insider seems to pose the greatest threat to knowledge assets 67 percent of respondents say their organization takes steps to address the risk of employee carelessness in the handling of knowledge assets, an increase from 61 percent in the 2016 research.

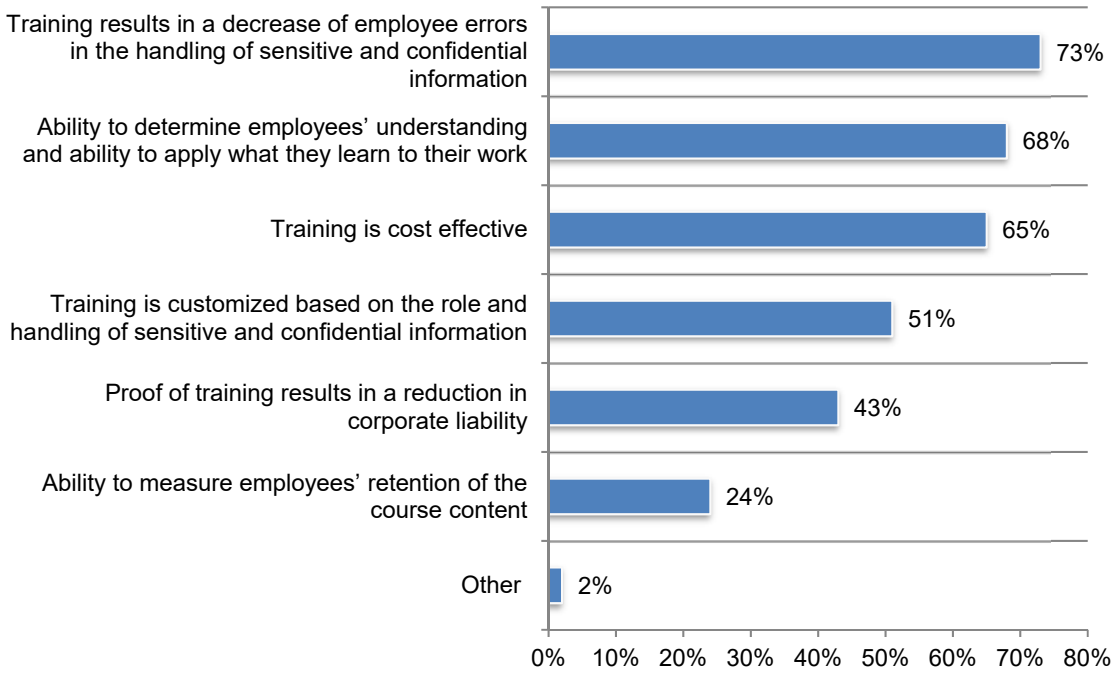
Of the 67 percent of respondents who say their organization takes steps, 71 percent of respondents say they conduct regular training and awareness programs and 69 percent of respondents say they are monitoring employees, as shown in Figure 7.

Figure 7. What steps does your organization take to reduce the careless insider risk?
More than one response allowed



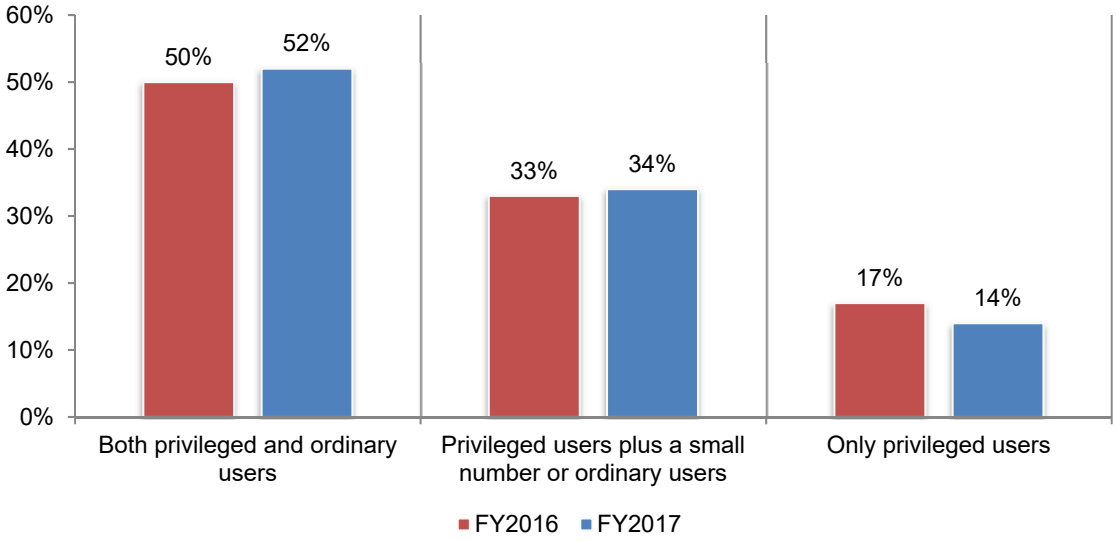
The goal of training programs is to reduce employees' errors in the handling of sensitive and confidential information. Figure 8 shows what respondents believe should be the most important goals for a training program. The number one component is a reduction in employee errors (73 percent of respondents) followed by the ability to determine if employees not only understand how to reduce the risk of carelessness but apply it to their work (68 percent of respondents). The cost-effectiveness of the program ranked third at 65 percent.

Figure 8. The most important components of a training and awareness program
Three responses allowed



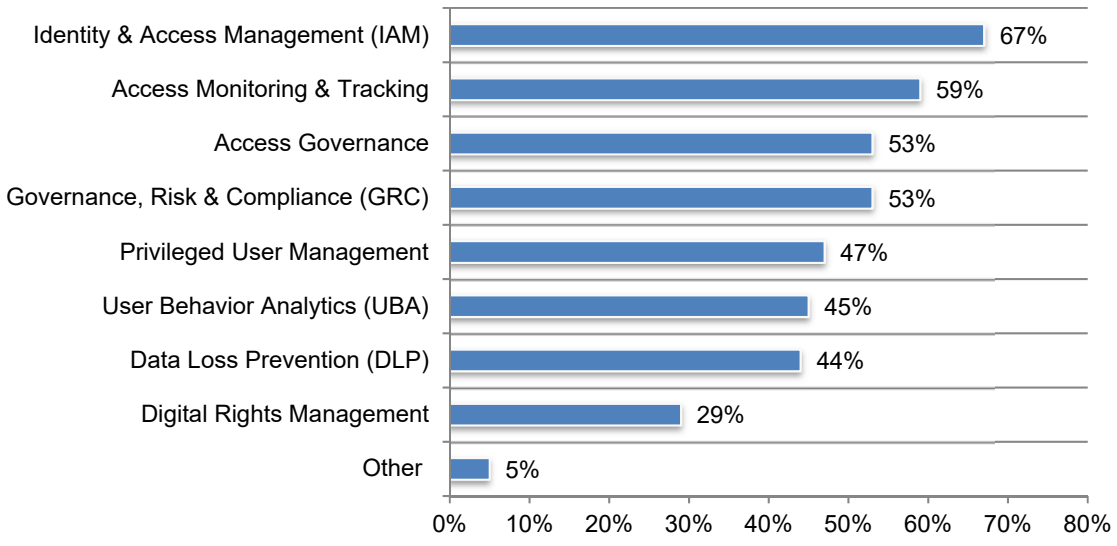
In most companies, ordinary users are not restricted from access to knowledge assets. Only 14 percent of respondents say their organizations only permit privileged users to access knowledge assets, as shown in Figure 9. In the context of this study, privileged users in this research are individuals who are assigned broad access rights to IT networks, enterprise systems, applications and knowledge assets based on their roles and responsibilities within the organization. Fifty-two percent of respondents say both privileged and ordinary users have access to knowledge assets.

Figure 9. In the normal course of business, who has access to your company's knowledge assets?



The top three technologies and processes used to ensure secure access are identity and access management (IAM) (67 percent of respondents), access monitoring and tracking (59 percent of respondents) and access governance (53 percent of respondents), as shown in Figure 10.

Figure 10. What technologies are used to ensure secure access to knowledge assets?
Three responses allowed

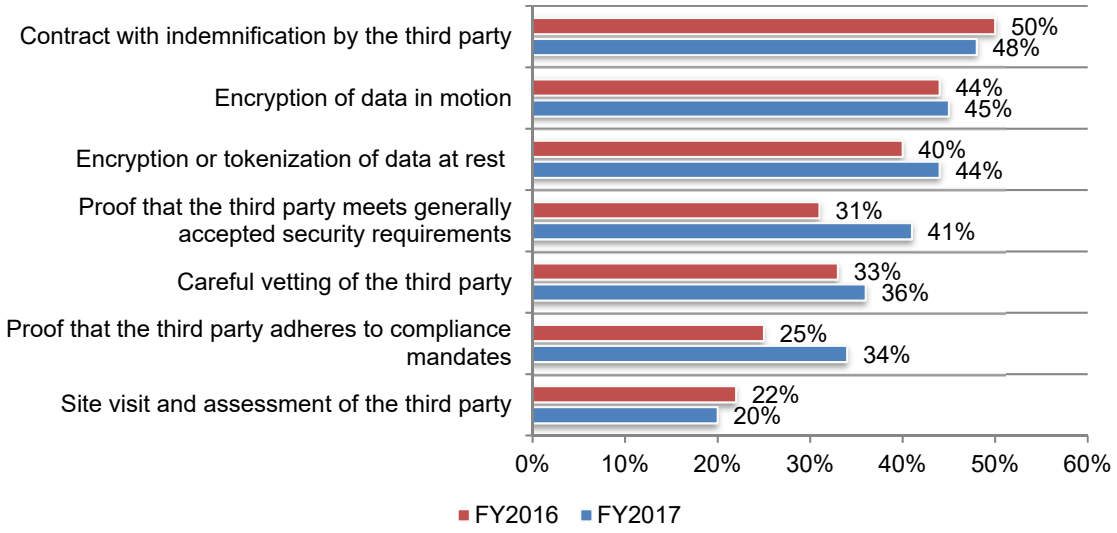


Trends in the risks to knowledge assets

Third party access to knowledge assets without appropriate security is a risk. Sixty-nine percent of respondents are concerned that third party access to knowledge assets is a serious risk to their organizations.

Sixty-one percent of respondents say third parties have access to their company's knowledge. Figure 13 reveals the steps organizations take to ensure the knowledge assets shared with third parties are protected. Most rely upon contracts with indemnification by the third party (48 percent of respondents). There are, however, interesting trends since 2016. More companies are requiring proof that the third party meets generally accepted security requirements (41 percent of respondents vs. 31 percent of respondents in 2016) and proof that the third party adheres to compliance mandates (25 percent of respondents vs. 34 percent of respondents in 2016).

Figure 11. How companies ensure third parties protect knowledge assets
More than one response allowed

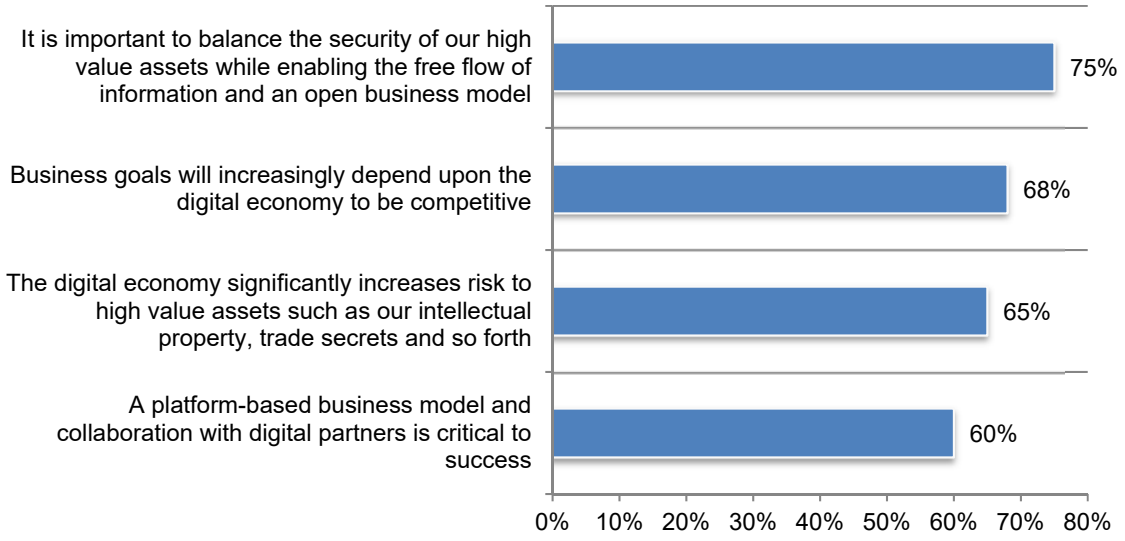


Businesses are embracing the digital economy, but it puts knowledge assets at risk. The digital economy has been described as the worldwide network of economic activities, commercial transactions and professional interactions that are enabled by information and communications technologies.[2]

According to Figure 12, 68 percent of respondents say their business goals will increasingly depend upon the digital economy to be competitive and 60 percent of respondents say a platform-based business model and collaboration with digital partners is critical to success.

However, 65 percent of respondents recognize that the digital economy will significantly increase the risk to high value assets such as intellectual property and trade secrets. The challenge for companies is being able to balance the security of high value assets while still enabling the free flow of information and an open business model.

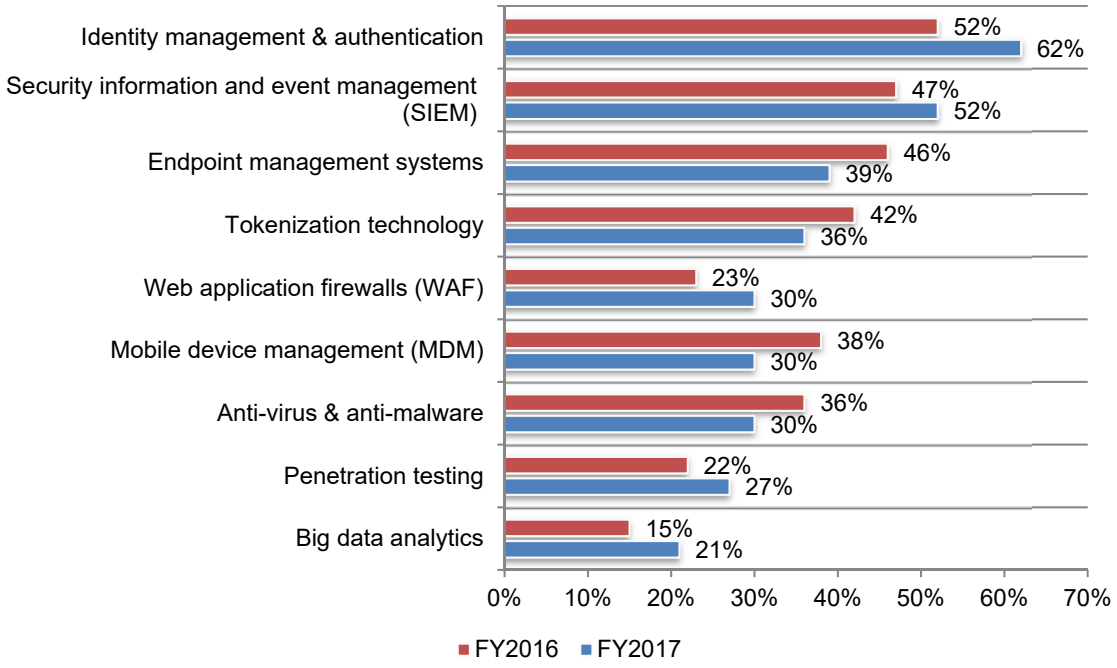
Figure 12. Perceptions about the risk to knowledge assets in the digital economy
Strongly agree and Agree responses combined



[2] The Digital Economy by Margaret Rouse, Search CIO.com, TechTarget, September 6, 2017

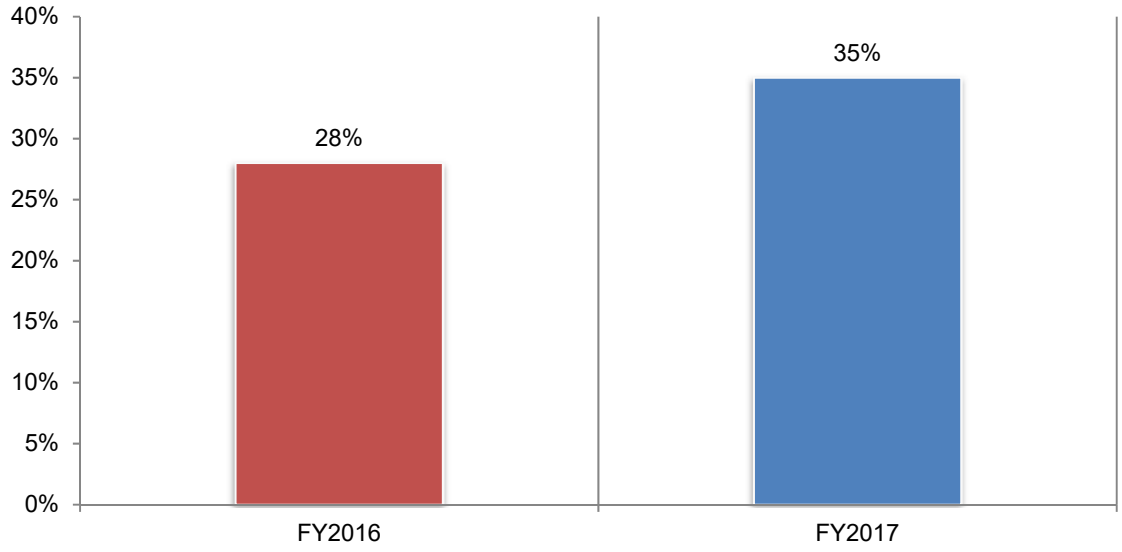
More companies are using identity management & authentication and SIEM to protect knowledge assets. Figure 13 presents trends in the technologies companies are deploying to protect knowledge assets. While the use of endpoint management systems, tokenization, mobile device management and anti-virus & anti-malware technologies have declined, Identity management and authentication, security information and event management (SIEM) and web application firewalls (WAF) have increased in use.

Figure 13. Trends in the use of enabling security technologies for protecting knowledge assets
Eight responses allowed



Companies' effectiveness in protecting knowledge assets remains low. Respondents were asked to rank their effectiveness in protecting knowledge assets on a scale of 1 = not effective to 10 = effective. As shown in Figure 14, those respondents ranking their organizations as highly effective in protecting knowledge assets (7+ respondents) increased from 28 percent in 2016 to 35 percent in this year's research.

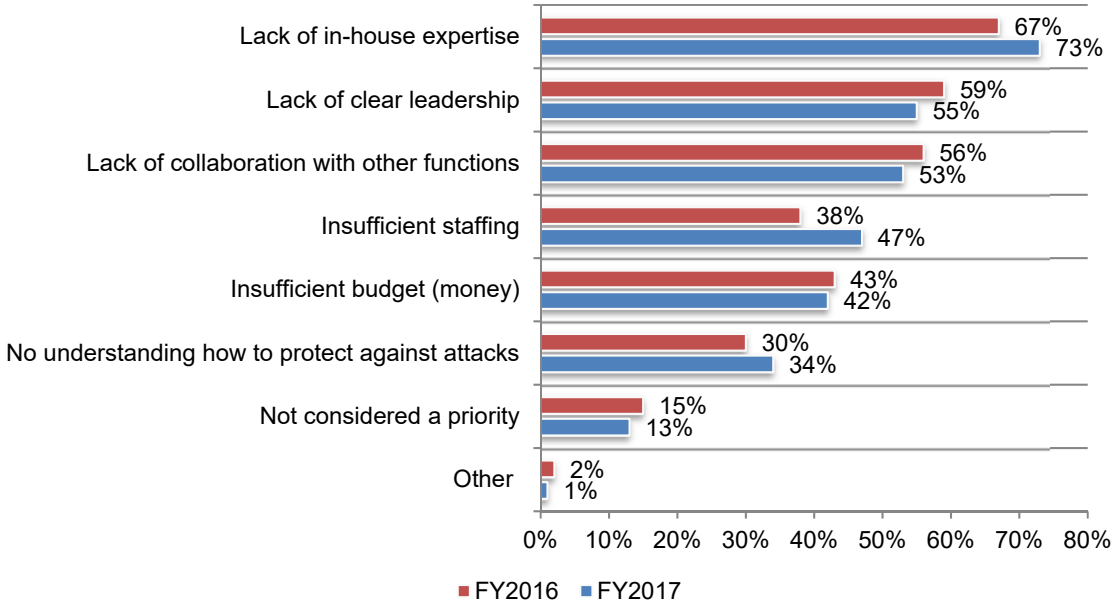
Figure 14. Effectiveness in protecting knowledge assets
1 = not effective to 10 = highly effective, 7 + responses reported



Reasons for not having an effective approach to the protection of knowledge assets are due to lack of in-house expertise and staffing. Those 65 percent of respondents who rate their organizations as not effective (a rating of 6 or lower) believe it is due to lack of in-house expertise (73 percent of respondents), lack of clear leadership (55 percent of respondents) and lack of collaboration with other functions (55 percent of respondents).

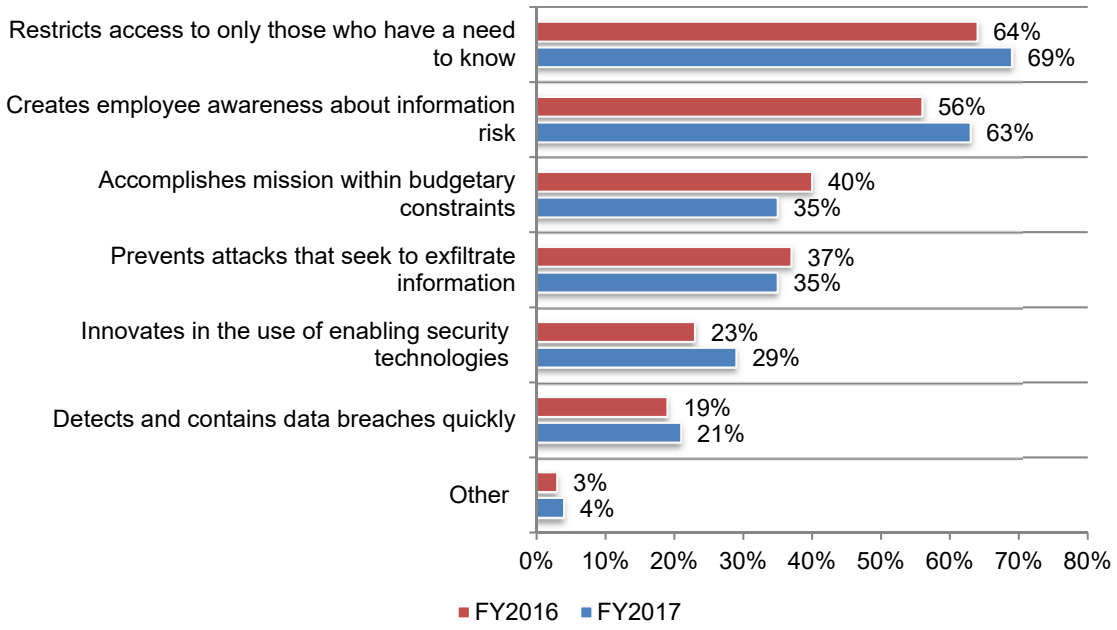
The most significant trends in barriers to effectiveness are the lack of in-house expertise (an increase from 67 percent of respondents in 2016 to 73 percent in this year's research) and insufficient staffing (an increase from 38 percent of respondents in 2016 to 47 percent of respondents in this year's research), as shown in Figure 15.

Figure 15. What prevents your company from being very effective?
More than one response allowed



Those 35 percent of respondents who rate their organizations as effective (7+ respondents) say it is because it restricts access to only those who have a need to know (69 percent of respondents) and creates employee awareness about information risk (63 percent of respondents), as shown in Figure 16.

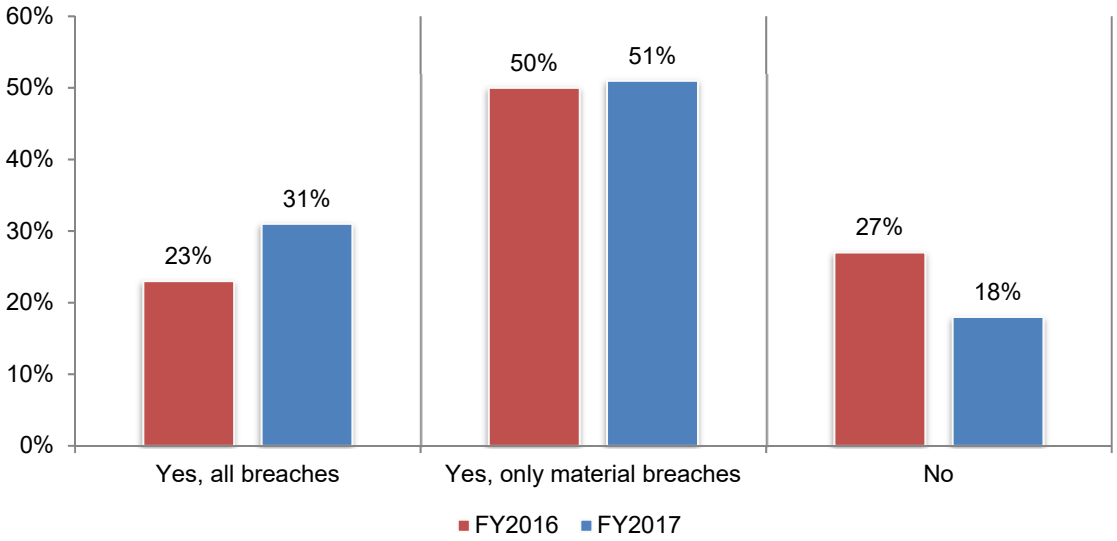
Figure 16. Why is your company effective?
More than one response allowed



Governance practices for knowledge assets

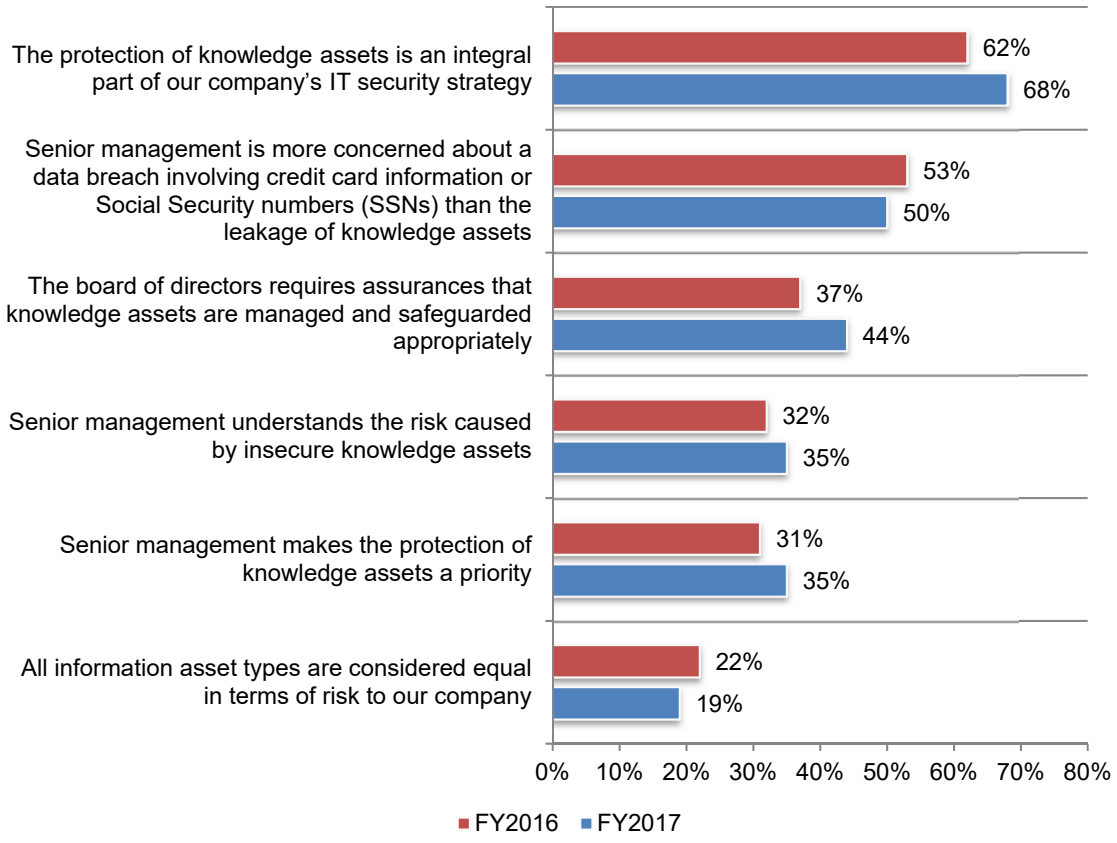
More boards of directors are informed about data breaches involving knowledge assets. According to Figure 17, the awareness of boards of directors about the loss or theft of knowledge assets increased from 23 percent of respondents to 31 percent of respondents.

Figure 17. Is your company's board of directors made aware of breaches involving the loss or theft of knowledge assets?



More boards of directors require assurances that knowledge assets are managed and safeguards appropriately. Since 2016, the requirement for assurance that knowledge assets are protected has increased from 37 percent of respondents to 44 percent of respondents, as shown in Figure 18.

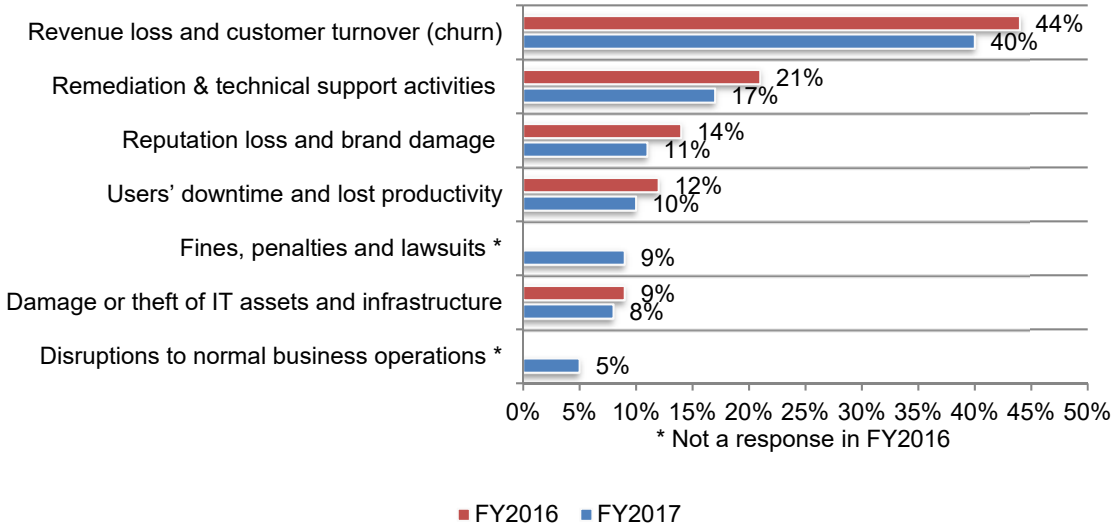
Figure 18. Perceptions about governance for knowledge assets
Strongly agree and Agree responses combined



The cost of an insider or malicious outsider attack on knowledge assets

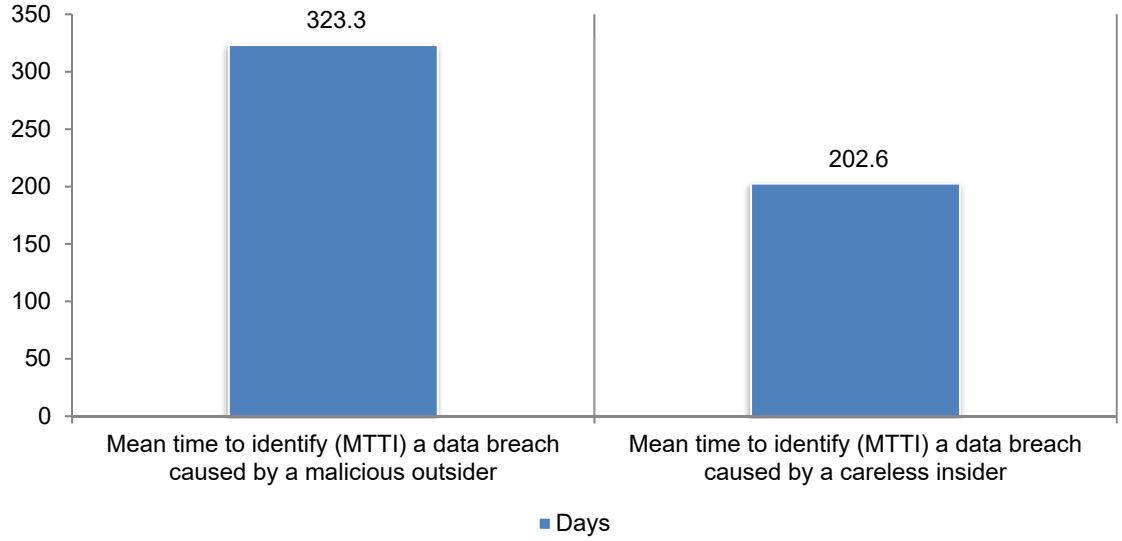
In the aftermath of an attack against knowledge assets, most costs are related to the restoration of reputation and brand. The average total cost incurred by organizations represented in this research due to the loss, misuse or theft of knowledge assets over the past 12 months increased 26 percent from $5.4 million to $6.8 million. As shown in Figure 19, 40 percent of this cost is spent on mitigating the consequences of reputation loss and brand damage.

Figure 19. The allocation of total costs for attacks against knowledge assets



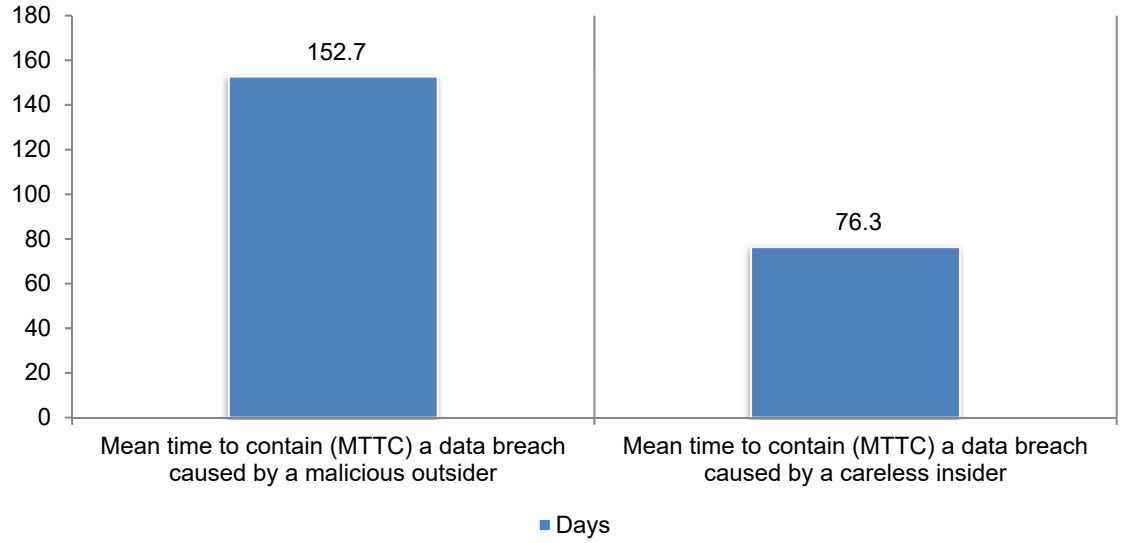
The time to identify and contain a data breach involving knowledge assets is greater for malicious outsiders than careless insiders. In this year's study, we asked respondents to estimate the mean time to identify (MTTI) and mean time to contain (MTTC) a data breach involving knowledge assets caused by a careless insider or a malicious outsider. According to the research, on average, it takes 203 days to identify a data breach caused by a careless insider but It takes 323 days to identify a data breach caused by a malicious outsider. Because it takes longer to respond to a malicious outsider, the costs and negative consequences can be greater than for the careless insider.

Figure 20. The mean time to identify (MTTI) a data breach involving knowledge assets caused by a careless insider or malicious outsider
Extrapolated average reported



Similarly, it takes less time to contain a data breach caused by a careless insider (76 days vs. 153 days to contain a data breach.

Figure 21. The mean time to contain (MTTC) a data breach involving knowledge assets caused by a careless insider or malicious outsider

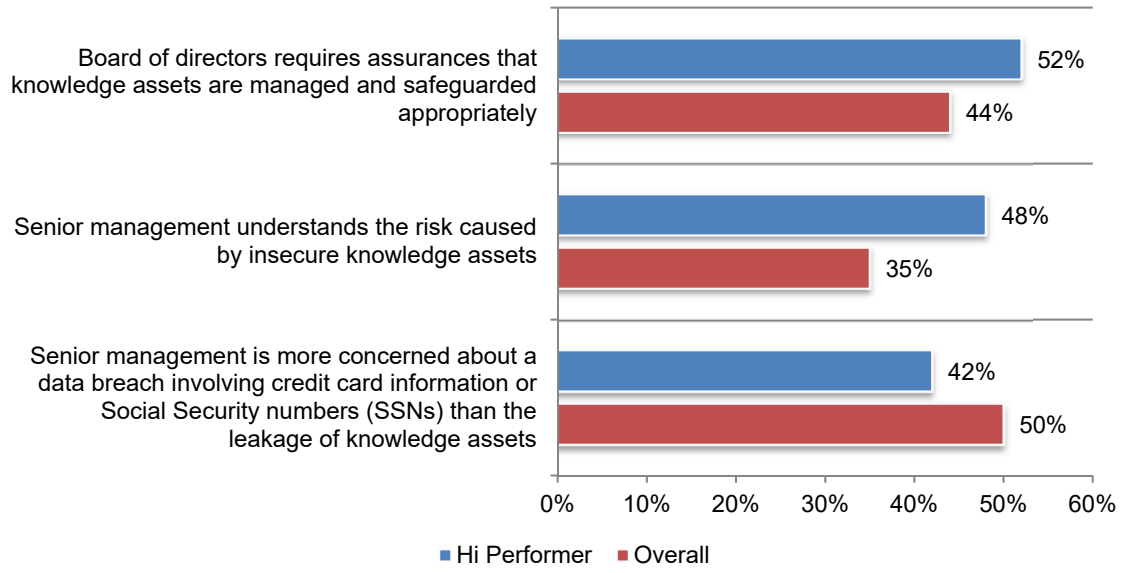


The practices of organizations highly effective in safeguarding knowledge assets

As part of the research, we did a special analysis of those respondents (89 respondents out of the total sample of 634 respondents) who rated their organizations' effectiveness in protecting their knowledge assets as very high (9+ on a scale of 1 = not effective to 10 = highly effective). In this study, effectiveness means mitigating the loss or theft of knowledge assets by insiders and external attackers.

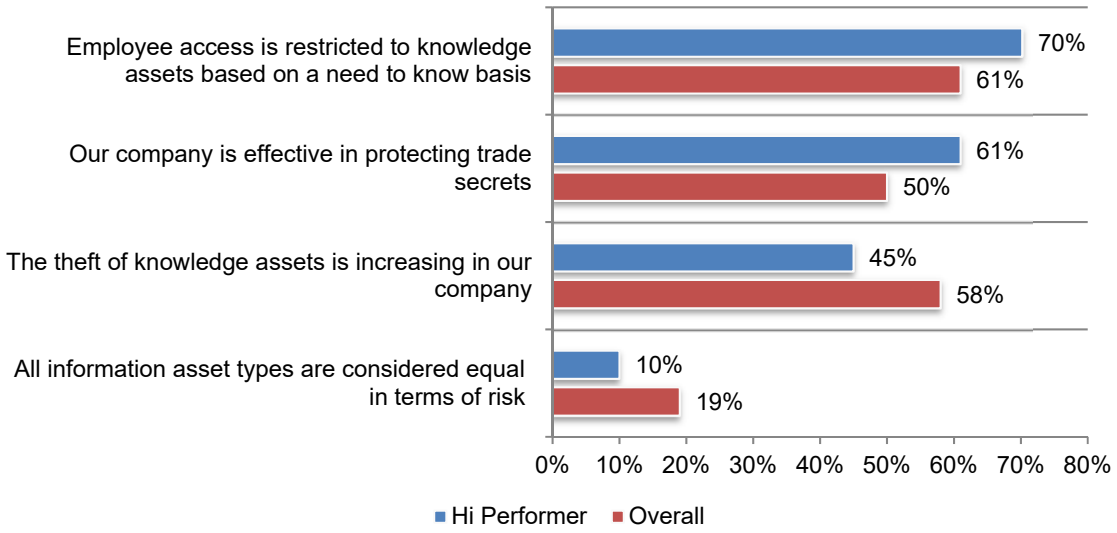
Senior management and boards of directors are more engaged in the protection of knowledge assets. As shown in Figure 22, senior management and boards of directors in high performing organizations are more likely to be concerned than the overall sample about the leakage of knowledge assets. They also understand the risk caused by insecure knowledge assets. In addition, boards of directors require assurances that knowledge assets are managed and safeguarded appropriately.

Figure 22. Perceptions about senior management and boards of directors
Strongly agree and Agree responses combined



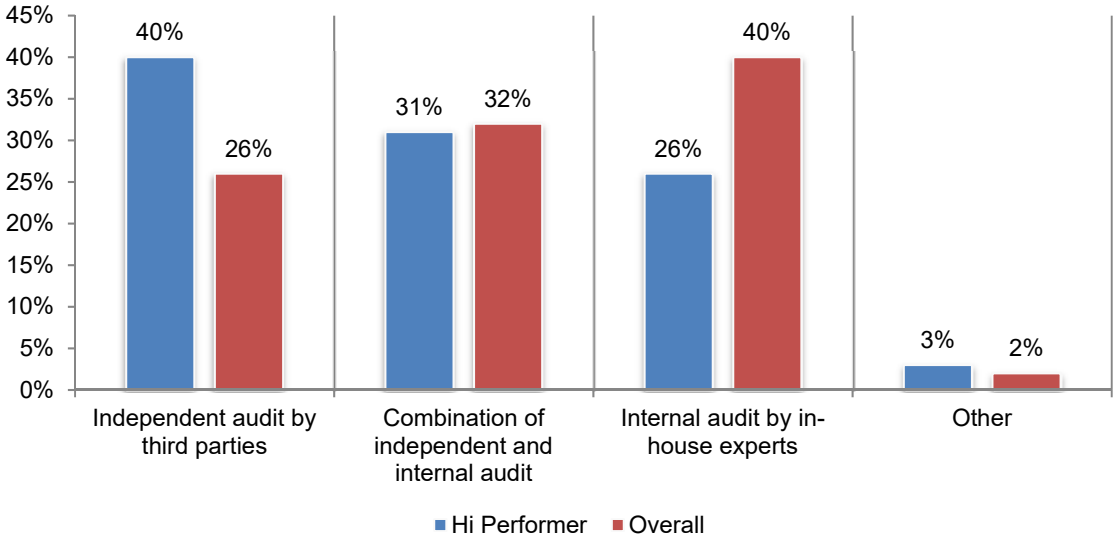
High performing organizations believe they are more effective in protecting trade secrets. Seventy percent of respondents in high performing organizations vs. 61 percent of respondents in the overall sample say their organizations restrict employee access to knowledge assets based on a need to know basis. As a consequence, high performing organizations believe they are more effective in protecting trade secrets and the theft of their knowledge assets is not increasing.

Figure 23. Differences in security practices
Strongly agree and Agree responses combined



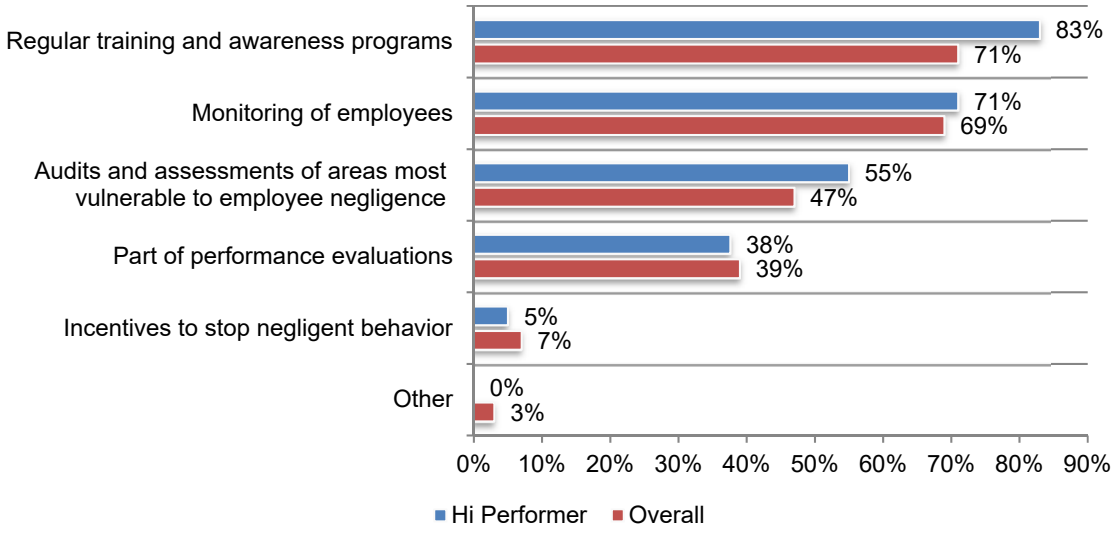
High performing organizations are more likely to conduct audits of practices and policies. Sixty-five percent of respondents in high performing organizations vs. 54 percent of respondents in the overall sample say their organizations conduct audits to ensure adherence to its practices and policies that safeguard knowledge assets. As shown in Figure 24, high performing organizations are more likely to have independent audits by third parties.

Figure 24. How are audits conducted to ensure adherence to practices and policies that safeguard knowledge assets?



High performing organizations are more likely to address the risk of employee carelessness in the handling of knowledge assets. Seventy-five percent of respondents in high performing organizations vs. 67 percent of respondents in the overall sample are proactive in trying to reduce the risk of employee carelessness. According to Figure 25, high performing organizations are more likely to conduct regular training and awareness programs and audits and assessments of areas most vulnerable to employee negligence.

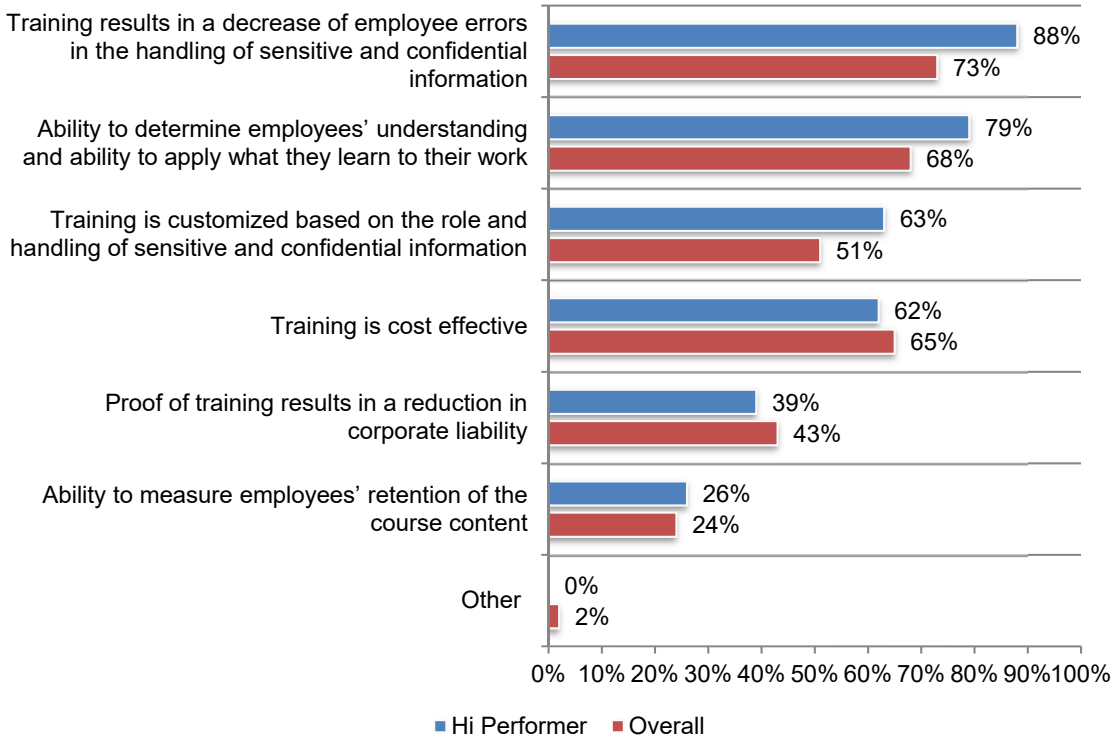
Figure 25. What steps does your organization take to minimize employee carelessness in the handling of knowledge assets?
More than one response permitted



Training in high performing organizations is not "one size fits all". As shown in Figure 26, 88 percent of high performing organizations say a key characteristic of their training programs is the ability to decrease of employee errors in the handling of sensitive and confidential information vs. 73 percent of respondents in the overall sample.

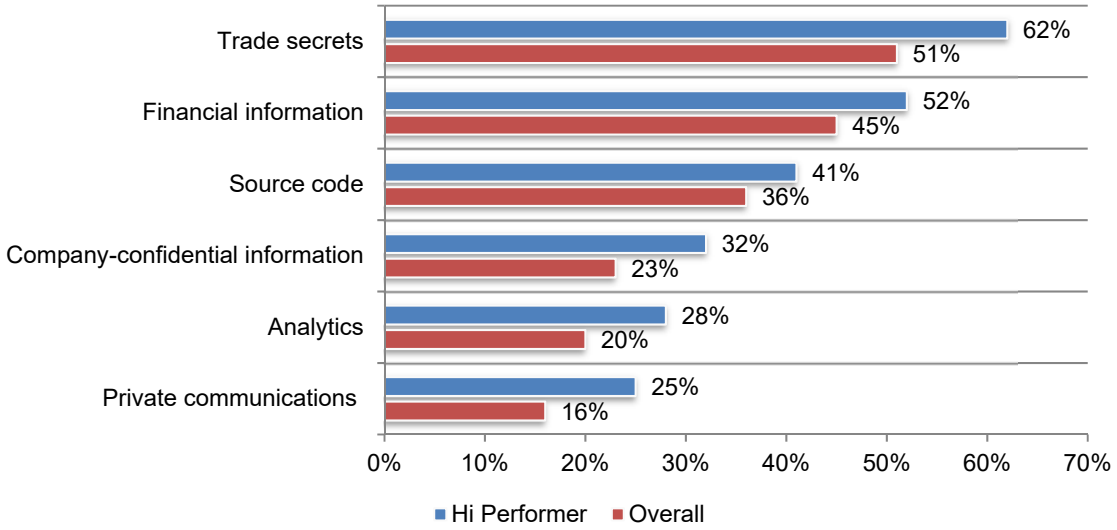
Seventy-nine percent of respondents in high performing organizations say their training programs are more likely to be able to determine employees' understanding and improve the ability to apply what they learn to their work. The programs are also customized based on the role and handling of sensitive and confidential information (63 percent vs. 51 percent of respondents). High performing organizations are also more likely to want to ensure the training results in a decrease of employee errors in the handling of sensitive and confidential information.

Figure 26. Characteristics of high performing training and awareness programs
More than one response permitted



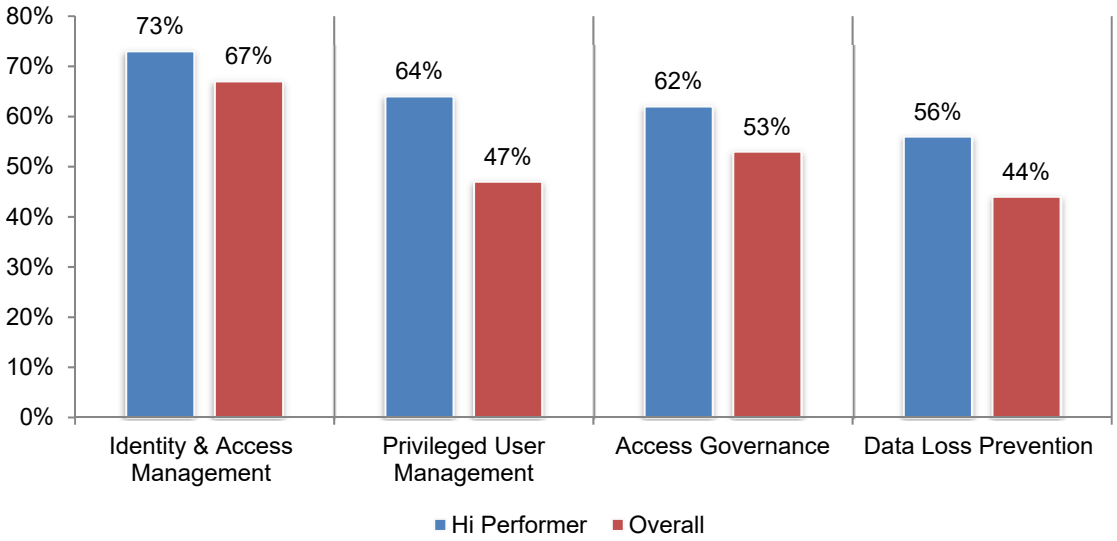
High value knowledge assets are more secure in high performing organizations. Figure 27 presents six knowledge assets that high performing organizations are more effective in safeguarding: source code, financial information, trade secrets, company-confidential information, private communications and analytics.

Figure 27. High performing organizations are more effective in securing certain knowledge assets
More than one response permitted



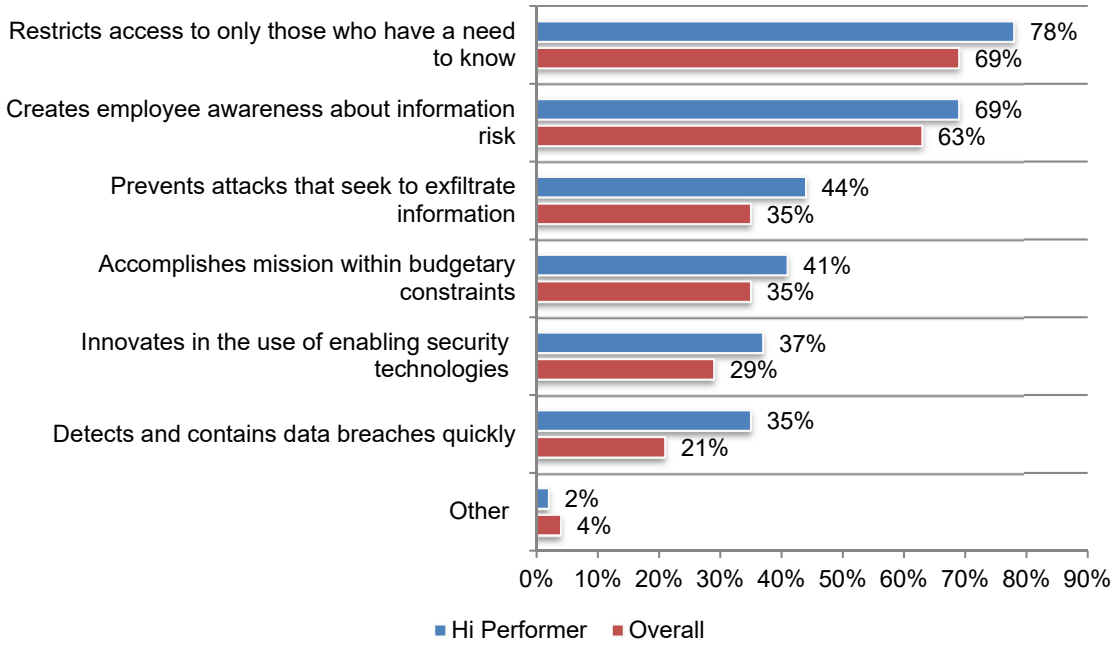
High performing organizations are more likely to use technologies and processes for the protection of knowledge assets. As shown in Figure 28, more respondents in high performing organizations report they are using identity & access management, privileged user management, access governance and data loss prevention.

Figure 28. Technologies or processes used by high performing organizations
More than one response permitted



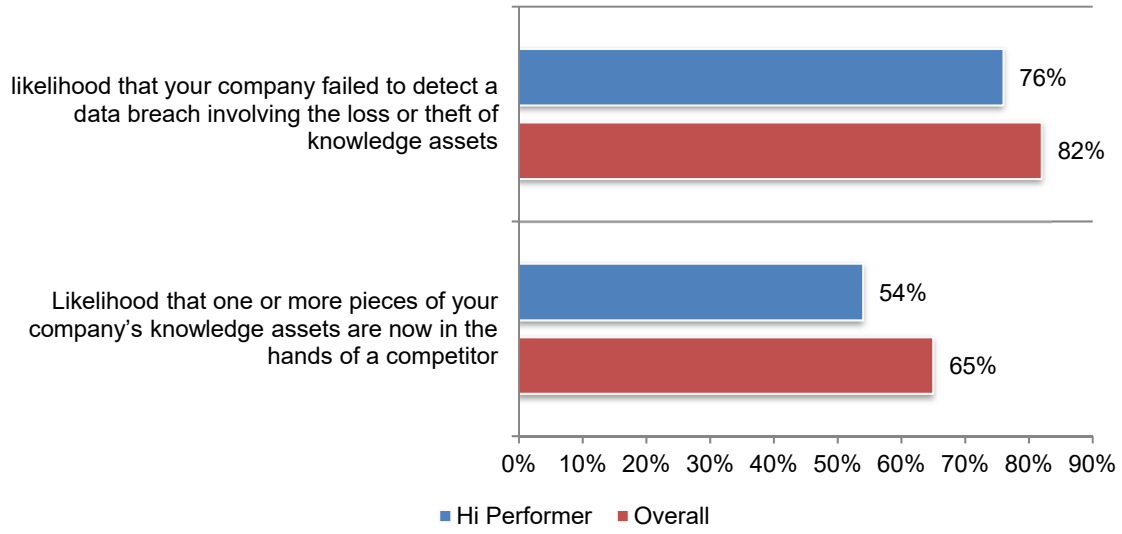
High performing organizations are more likely than other organizations to detect and contain data breaches. According to Figure 29, 35 percent of respondents in high performing organizations are more likely than the overall sample to detect and contain a data breach (35 percent vs. 21 percent of respondents). More high performing organizations are restricting access to only those who have a need to know and prevent attacks that seek to exfiltrate information (44 percent vs. 35 percent of respondents).

Figure 29. Why are high performing organizations more effective?
More than one response permitted



High performing organizations are more effective than other companies keeping knowledge assets out of the hands of competitors. According to Figure 30, 54 percent of respondents in high performing organizations vs. 65 percent of respondents in the overall sample to say it is very likely or somewhat likely that one or more of their knowledge assets has been stolen by a competitor. While all organizations in this research believe it is likely that they failed to detect a data breach involving the loss or theft of knowledge assets, high performing organizations are less likely to say they failed to detect such an incident.

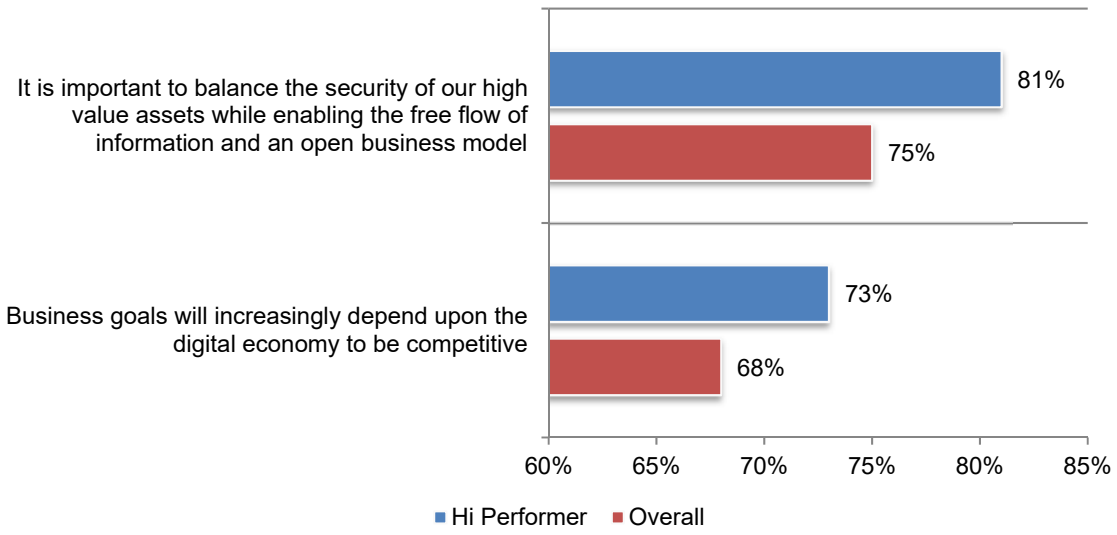
Figure 30. The likelihood that a data breach was not detected and a competitor has your organization's knowledge assets
Very likely and Somewhat likely responses combined



More high performing organizations have achieved a mature level of digital transformation. Sixty-four percent of respondents in high performing organizations say they have either deployed many digital transformation activities deployed across the enterprise or have core digital transformation activities deployed, maintained and/or refined across the enterprise. In contrast, only 45 percent of respondents in the overall sample have achieved such maturity.

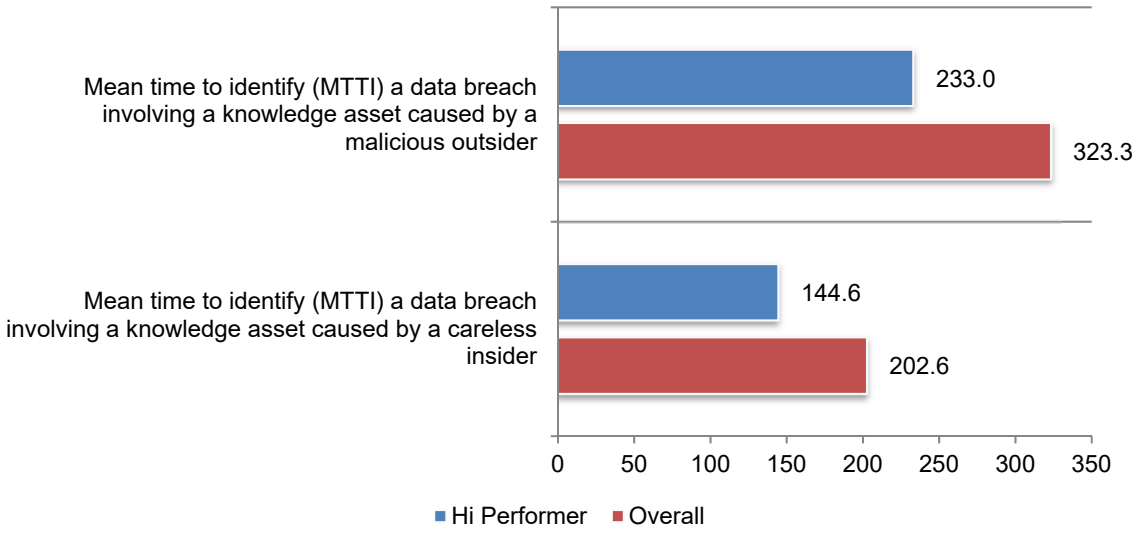
According to Figure 30, high performing organizations are more likely to say their business goals will increasingly depend upon the digital economy to be competitive. They are also more likely to say it is important to balance the security of their high value assets while enabling the free flow of information and an open business model.

Figure 31. Perceptions about knowledge assets in the digital economy
Strongly agree and Agree responses combined



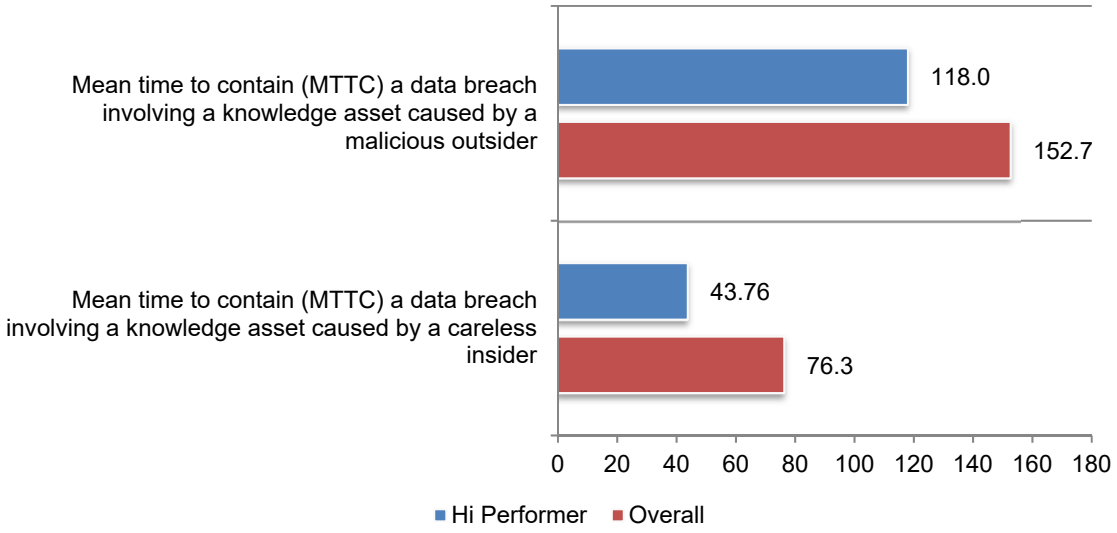
High performing organizations are faster at identifying a data breach involving knowledge assets caused by a malicious outsider or careless insider. According to Figure 32, high performing organizations on average reduce the (MTTI) to identify a data breach involving a knowledge asset caused by a malicious outsider by more than 90 days (323.3 – 233) and the MTTI to identify a breach by a careless insider by 58 days (202.6 – 144.6).

Figure 32. The mean time to identify (MTTI) a data breach involving knowledge assets caused by a careless insider or malicious outsider
Extrapolated values reported



High performing organizations are faster at containing a data breach involving knowledge assets caused by a malicious outsider or careless insider. According to Figure 33, high performing organizations on average reduce the (MTTC) to identify a data breach involving a knowledge asset caused by a malicious outsider by more than 34 days (152.7 - 118) and the MTTC to identify a breach by a careless insider by 32.54 days (76.3 – 43.76).

Figure 33. The mean time to contain (MTTC) a data breach involving knowledge assets caused by a careless insider or malicious outsider
Extrapolated values reported



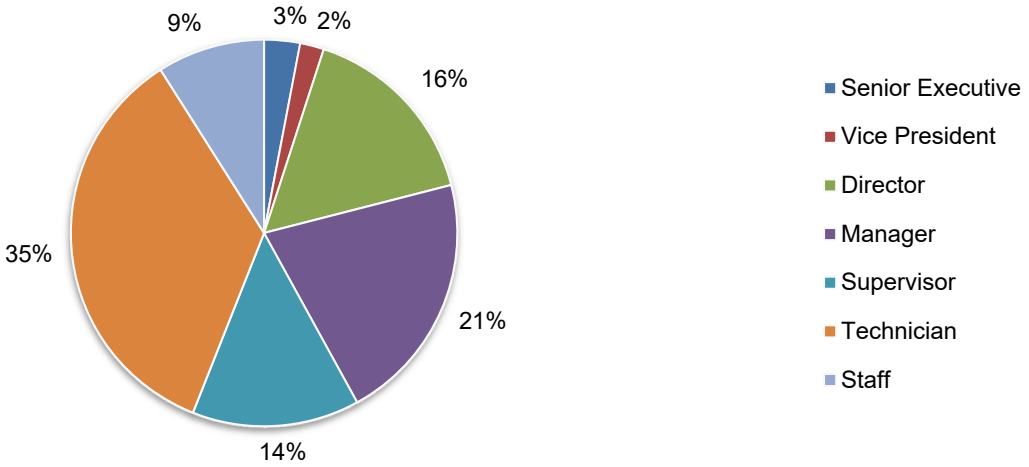
Part 3. Methods

A sampling frame of 17,991 individuals familiar with and involved in their company's approach to managing knowledge assets were selected as participants in the research. Table 1 shows 709 total returns. Screening and reliability checks required the removal of 75 surveys. Our final sample consisted of 634 surveys or a 3.5 percent response rate.

Table 1. Sample response	FY2017	FY2016
Sampling frame	17,991	17,540
Total returns	709	691
Rejected or screened surveys	75	88
Final sample	634	603
Response rate	3.5%	3.4%

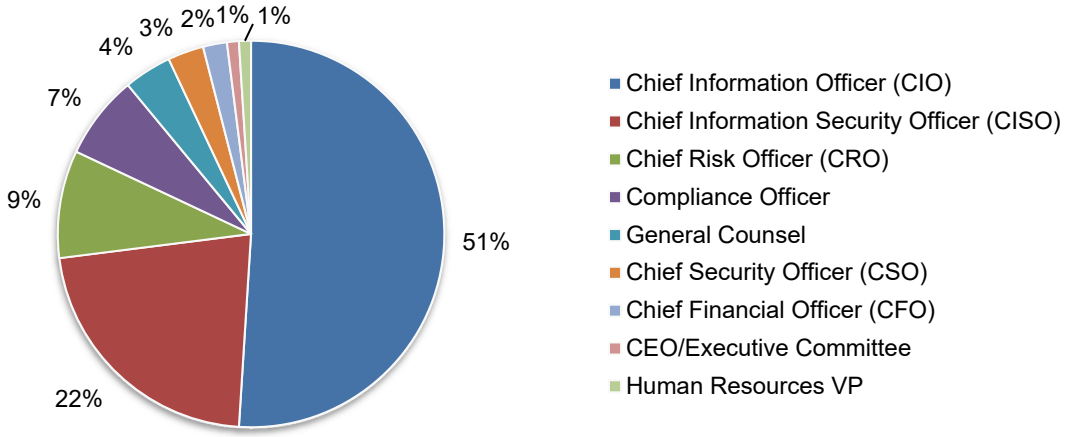
Pie Chart 1 reports the respondents' organizational levels within the participating organizations. By design, more than half of the respondents (56 percent) are at or above the supervisory levels.

Pie Chart 1. Current position within the organization



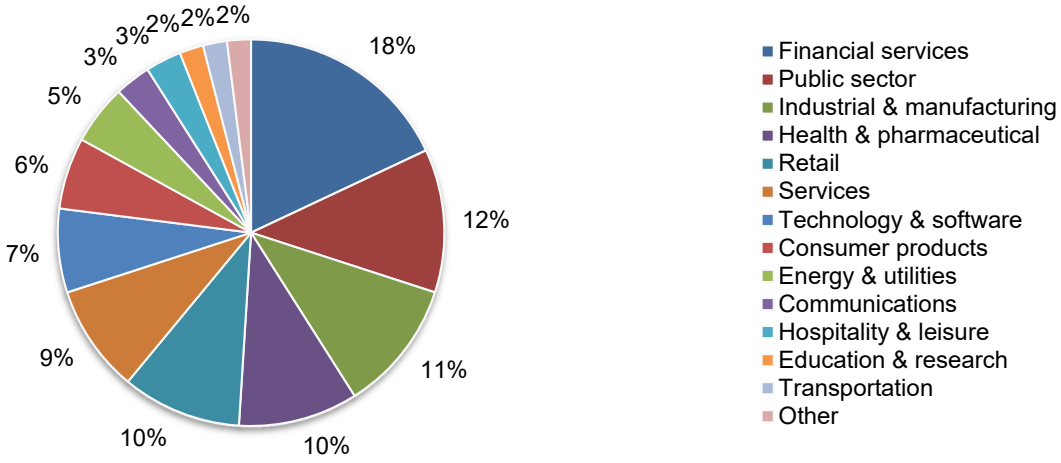
Pie Chart 2 shows that 51 percent of respondents report to the CIO, 22 percent report to the CISO and 9 percent indicated they report to the CRO.

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



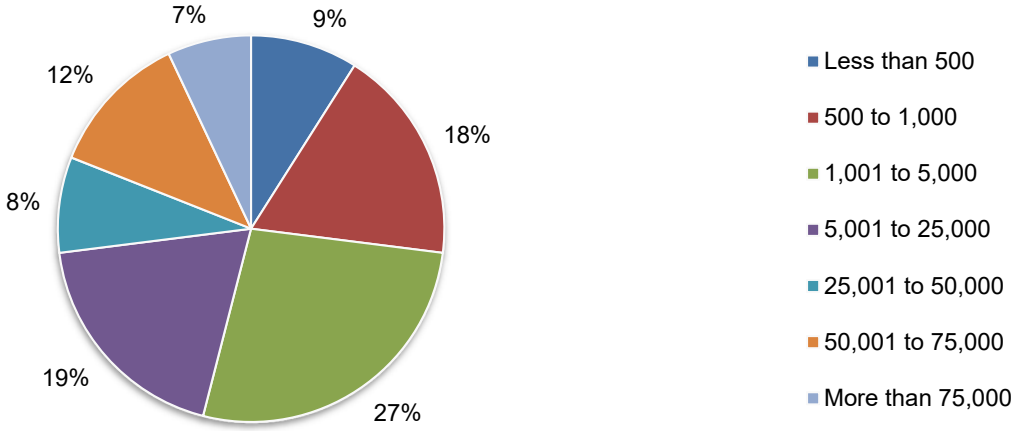
Pie Chart 3 reports the industry segments of respondents' organizations. This chart identifies financial services (18 percent) as the largest segment, followed by public sector (12 percent), industrial and manufacturing (11 percent), health and pharmaceutical (10 percent) and retail sector (10 percent).

Pie Chart 3. Primary industry classification of respondents' organizations



As shown in Pie Chart 4, 73 percent of respondents are from organizations with a global headcount of more than1,000 employees.

Pie Chart 4. Worldwide headcount of the organization



In addition to the United States, 71 percent of respondents indicated their organization has employees located in Canada, 70 percent responded their organization has employees in Europe, 63 percent have employees in Asia-Pacific, 57 percent have employees in Latin America and 46 percent have employees in the Middle East and Africa, as shown in Table 2.

Table 2. Global location of employees	
United States	100%
Canada	71%
Europe	70%
Asia-Pacific	63%
Latin America (including Mexico)	57%
Middle East & Africa	46%

Part 4. Caveats to this study

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

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

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are familiar with their companies' approach to managing knowledge assets and involved in the process and are located in the United States. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured between December 6, 2017 and December 20, 2017.

Survey response	FY2017	FY2016
Total sampling frame	17,991	17,540
Total returns	709	691
Rejected or screened surveys	75	88
Final sample	634	603
Response rate	3.5%	3.4%

Screening questions

S1. How familiar are you with your organization's approach to managing knowledge assets?	FY2017	FY2016
Very familiar	25%	23%
Familiar	46%	45%
Somewhat familiar	29%	32%
No knowledge (Stop)	0%	0%
Total	100%	100%

S2. Does your company have a program or set of activities for managing knowledge assets?	FY2017	FY2016
Yes	100%	100%
No (Stop)	0%	0%
Total	100%	100%

S3. Do you have any involvement in managing knowledge assets?	FY2017	FY2016
Yes, full involvement	26%	23%
Yes, partial involvement	49%	51%
Yes, minimal involvement	25%	26%
No involvement (Stop)	0%	0%
Total	100%	100%

Part 2. Attributions: Please rate each of the following statements using the five-point agreement scale provided below each item. % Strongly Agree and Agree response combined.	FY2017	FY2016
Q1. Senior management makes the protection of knowledge assets a priority.	35%	31%
Q2. Third party access to our company's knowledge assets poses a serious risk.	69%	67%
Q3. All information asset types are considered equal in terms of risk to our company.	19%	22%
Q4. The protection of knowledge assets is an integral part of our company's IT security strategy.	68%	62%
Q5. Our company's senior management understands the risk caused by insecure knowledge assets.	35%	32%
Q6. Our company's senior management is more concerned about a data breach involving credit card information or Social Security numbers (SSNs) than the leakage of knowledge assets.	50%	53%
Q7. The most significant threat to the security of knowledge assets is employee negligence.	75%	71%
Q8. Our company restricts employee access to knowledge assets based on a need to know basis.	61%	59%
Q9. Our company's board of directors requires assurances that knowledge assets are managed and safeguarded appropriately.	44%	37%
Q10. The theft of knowledge assets is increasing in our company.	58%	50%
Q11. The protection of knowledge assets is difficult to achieve in our company.	68%	69%
Q12. Our company is effective in protecting trade secrets.	50%	

Part 3. Governance & IT security practices

Q13. Who is involved in determining your company's approach for protecting knowledge assets? Please select your top 3 choices.	FY2017	FY2016
General Counsel	42%	39%
Chief Executive Officer	4%	5%
Chief Operating Officer	12%	14%
Chief Compliance Officer	39%	45%
Chief Financial Officer (CFO)	35%	33%
Chief Technology Officer (CTO)	13%	14%
Chief Information Officer (CIO)	53%	56%
Chief Information Security Officer (CISO)	32%	28%
Chief Security Officer (CSO)	3%	4%
Chief Privacy Officer (CPO)	3%	2%
Head of Human Resources	19%	21%
Head of R&D	6%	7%
Chief Risk Officer (CRO)	30%	26%
No one person/department	9%	6%
Total	300%	300%

Q14. Who is **most responsible** for protecting your company's knowledge assets?	FY2017	FY2016
General Counsel	5%	6%
Chief Executive Officer	8%	10%
Chief Operating Officer	7%	7%
Chief Compliance Officer	12%	13%
Chief Financial Officer (CFO)	5%	6%
Chief Technology Officer (CTO)	2%	0%
Chief Information Officer (CIO)	20%	23%
Chief Information Security Officer (CISO)	15%	12%
Chief Security Officer (CSO)	0%	0%
Chief Privacy Officer (CPO)	0%	0%
Head of human resources	4%	3%
Head of R&D	0%	0%
Chief Risk Officer (CRO)	6%	5%
No one person/department	16%	15%
Total	100%	100%

Q15a. Does your company conduct audits to ensure adherence to its practices and policies that safeguard knowledge assets?	FY2017
Yes	54%
No	41%
Unsure	5%
Total	100%

Q15b. If yes, how are these audits conducted? Please select all that apply.	FY2017
Independent audit by third parties	26%
Internal audit by in-house experts	40%
Combination of independent and internal audit	32%
Other (please specify)	2%
Total	100%

Q16a. Does your organization take steps to address the risk of employee carelessness in the handling of knowledge assets?	FY2017	FY2016
Yes	67%	61%
No	26%	30%
Unsure	7%	9%
Total	100%	100%

Q16b. If yes, what steps does it take? Please select all that apply.	FY2017	FY2016
Regular training and awareness programs	71%	70%
Monitoring of employees	69%	65%
Audits and assessments of areas most vulnerable to employee negligence	47%	43%
Incentives to stop negligent behavior	7%	8%
Part of performance evaluations	39%	36%
Other	3%	2%
Total	236%	224%

Q17. If your organization has a training and awareness program, what should its most important components be? Please select your top 3 responses.	FY2017
Ability to determine employees' understanding and ability to apply what they learn to their work	68%
Ability to measure employees' retention of the course content	24%
Training is cost effective	65%
Training is customized based on the role and handling of sensitive and confidential information	51%
Training results in a decrease of employee errors in the handling of sensitive and confidential information	73%
Proof of training results in a reduction in corporate liability	43%
Other (please specify)	2%
Total	326%

Q18. What are the most important enabling security technologies for protecting knowledge assets? Please select 8 top choices.	FY2017	FY2016
Access governance	42%	43%
Anti-virus & anti-malware	30%	36%
Big data analytics	21%	15%
Blockchain	6%	
Can't determine	0%	
Code vulnerability scanning and debugging systems	15%	14%
Data loss prevention (DLP)	45%	48%
Encryption for data at rest	53%	54%
Encryption for data in motion	45%	49%
Endpoint management systems	39%	46%
Governance, risk and compliance systems (eGRC)	19%	21%
Hardware security modules (HSM)	40%	39%
Identity management & authentication	62%	52%
Intrusion detection systems (IDS)	25%	21%
Intrusion prevention systems (IPS)	22%	22%
Mobile device management (MDM)	30%	38%
Network and traffic intelligence systems	34%	35%
Next generation firewalls	22%	19%
Penetration testing	27%	22%
Secure USB flash device or mobile media	15%	19%
Security information and event management (SIEM)	52%	47%
Test data anonymization solution	13%	17%
Tokenization technology	36%	42%
Traditional firewalls	42%	40%
Virtual private networks (VPN)	35%	33%
Web application firewalls (WAF)	30%	23%
Other (please specify)	0%	5%
Total	800%	800%

Q19. Following are 13 categories of knowledge assets. Please select the three knowledge assets categories that in your experience are most difficult to secure.*	FY2017	FY2016
Source code	50%	51%
Business correspondence	46%	52%
Financial information	34%	37%
Operational information	36%	40%
Research results	18%	25%
Attorney-client privileged information	11%	10%
Presentations	52%	45%
Product/market information	65%	60%
Trade secrets	48%	44%
Company-confidential information	41%	40%
Private communications (i.e., emails, texting, social media)	72%	67%
Consumer data	15%	18%
Analytics	12%	11%
Total	500%	500%

*FY2016 Allowed 5 responses

Q20. How confident are you that the above 13 knowledge asset categories are appropriately secured within your company? Please rate each information asset category using the following five-point confidence scale: % High confidence response.	FY2017	FY2016
Source code	36%	39%
Business correspondence	15%	18%
Financial information	45%	49%
Operational information	19%	21%
Research results	35%	41%
Attorney-client privileged information	52%	50%
Presentations	16%	19%
Product/market information	15%	19%
Trade secrets	51%	45%
Company-confidential information	23%	24%
Private communications (i.e., emails, texting, social media)	16%	16%
Consumer data	32%	28%
Analytics	20%	24%
Total	375%	393%

Q21. In the normal course of business, who has access to your company's knowledge assets?	FY2017	FY2016
Only privileged users	14%	17%
Privileged users plus a small number or ordinary users	34%	33%
Both privileged and ordinary users	52%	50%
Total	100%	100%

Q22. What technologies or processes are used to ensure secure access to your company's knowledge assets?	FY2017
User Behavior Analytics (UBA)	45%
Governance, Risk & Compliance (GRC)	53%
Digital Rights Management	29%
Access Governance	53%
Privileged User Management	47%
Data Loss Prevention (DLP)	44%
Identity & Access Management (IAM)	67%
Access Monitoring & Tracking	59%
Other (please specify)	5%
Total	402%

Q23a. Do third parties have access to your company's knowledge assets?	FY2017	FY2016
Yes	61%	57%
No	27%	29%
Unsure	12%	14%
Total	100%	100%

Q23b. If yes, how does your company ensure knowledge assets shared with third parties are appropriately protected?	FY2017	FY2016
Encryption or tokenization of data at rest	44%	40%
Encryption of data in motion	45%	44%
Contract with indemnification by the third party	48%	50%
Proof that the third party meets generally accepted security requirements	41%	31%
Proof that the third party adheres to compliance mandates	34%	25%
Careful vetting of the third party	36%	33%
Site visit and assessment of the third party	20%	22%
Other (please specify)	0%	0%
Total	268%	284%

Part 4. The threat to knowledge assets

Q24. Using the following 10-point scale, please rate your company's effectiveness in protecting its knowledge assets. In the context of this study, effectiveness means mitigating the loss or theft of knowledge assets by insiders and external attackers. 1 = not effective to 10 = very effective.	FY2017	FY2016
1 or 2	8%	11%
3 or 4	24%	25%
5 or 6	33%	36%
7 or 8	21%	18%
9 or 10	14%	10%
Total	100%	100%
Extrapolated value	5.68	5.32

Q25. **For those who rate 6 and below**: What prevents your company from being very effective?	FY2017	FY2016
Insufficient budget (money)	42%	43%
Insufficient staffing	47%	38%
Lack of in-house expertise	73%	67%
Lack of clear leadership	55%	59%
No understanding how to protect against attacks	34%	30%
Lack of collaboration with other functions	53%	56%
Not considered a priority	13%	15%
Other (please specify)	1%	2%
Total	318%	310%

Q26**. For those who rate 7 and above**: Why is your company effective?	FY2017	FY2016
Restricts access to only those who have a need to know	69%	64%
Prevents attacks that seek to exfiltrate information	35%	37%
Creates employee awareness about information risk	63%	56%
Accomplishes mission within budgetary constraints	35%	40%
Innovates in the use of enabling security technologies	29%	23%
Detects and contains data breaches quickly	21%	19%
Other (please specify)	4%	3%
Total	256%	242%

Q27. In your opinion, is your company's board of directors made aware of breaches involving the loss or theft of knowledge assets?	FY2017	FY2016
Yes, all breaches	31%	23%
Yes, only material breaches	51%	50%
No	18%	27%
Total	100%	100%

Q28. In your opinion, what is the likelihood that one or more pieces of your company's knowledge assets are now in the hands of a competitor?	FY2017	FY2016
Very likely	30%	24%
Somewhat likely	35%	36%
Not likely	27%	30%
No chance	8%	10%
Total	100%	100%

Q29. In your opinion, what is the likelihood that your company **failed to detect** a data breach involving the loss or theft of knowledge assets?	FY2017	FY2016
Very likely	39%	34%
Somewhat likely	43%	40%
Not likely	16%	21%
No chance	2%	5%
Total	100%	100%

Q30. What are the most likely root causes of data breaches involving your company's knowledge assets? Please rank the following list from 1 = most likely to 4 = least likely.	FY2017	FY2016
Careless insider	1.52	1.67
Malicious or criminal insider	2.33	2.45
External attacker	3.01	2.89
Combined insider and external attackers	3.50	3.49
Average	2.59	2.63

Q31. What are the main motivations of attackers that seek to steal your company's knowledge assets? Please rank the following list from 1 = most likely to 4 = least likely.	FY2017	FY2016
Economic espionage	1.88	1.78
Sabotage	3.54	3.62
Hacktivism	2.64	2.73
Cyber warfare (nation-state attacks)	3.39	3.26
Average	2.86	2.85

Q32. What best describes the maturity level of your organization's digital transformation today?	FY2017
Has not been launched (Skip to Q34a)	5%
Early stage – many digital transformation activities have not as yet been planned or deployed	19%
Middle stage – digital transformation activities are planned and defined but only partially deployed	31%
Late-middle stage – many digital transformation activities are deployed across the enterprise	25%
Mature stage – Core digital transformation activities are deployed, maintained and/or refined across the enterprise	20%
Total	100%

Please express your opinion about each one of the following statements using the five-point agreement scale provided below each item. % Strongly Agree and Agree response combined.	FY2017
Q33a. My organization's business goals will increasingly depend upon the digital economy to be competitive.	68%
Q33b. In my organization, it is important to balance the security of our high value assets while enabling the free flow of information and an open business model.	75%
Q33c. In my organization, the digital economy significantly increases risk to high value assets such as our intellectual property, trade secrets and so forth.	65%
Q33d. In my organization, a platform-based business model and collaboration with digital partners is critical to success.	60%

Q34a. Do you believe nation state attackers target your company's knowledge assets?	FY2017	FY2016
Yes, very likely	25%	17%
Yes, somewhat likely	36%	33%
No, not likely	35%	42%
No chance	4%	8%
Total	100%	100%

Q34b. If likely, how do you know if nation state attackers have targeted your company's knowledge assets? Please select all that apply.	FY2017
Root cause (forensic) analysis	50%
Signature of the attack	42%
Geo-location of the attacker	27%
Contact from the attacker	19%
Alert from peers and/or law enforcement	31%
Gut feel	47%
Other (please specify)	3%
Total	219%

Q35. How valuable do you believe your trade secrets or knowledge assets are to a nation state attacker?	FY2017
Very valuable	45%
Valuable	34%
Not valuable	21%
Total	100%

Q36. Please select the three knowledge assets categories that in your experience would be most valuable to a nation state attacker or competitor?	FY2017
Source code	32%
Business correspondence	15%
Financial information	19%
Operational information	32%
Research results	13%
Attorney-client privileged information	8%
Presentations	24%
Product/market information	27%
Trade secrets	33%
Company-confidential information	26%
Private communications (i.e., emails, texting, social media)	45%
Consumer data	10%
Analytics	16%
Total	300%

Part 5. Budget and cost

Q37. Approximately, how much was the total cost incurred by your organization due to the loss, misuse or theft of knowledge assets over the past 12 months? Approximately, how much was the total cost due to attacks against knowledge assets over the past 12 months?	FY2017	FY2016
Zero	0%	5%
Less than $50,000	0%	0%
50,001 to $100,000	3%	7%
100,001 to $250,000	5%	7%
250,001 to $500,000	11%	15%
500,001 to $1,000,000	18%	15%
1,000,001 to $5,000,000	26%	20%
5,000,001 to $10,000,000	16%	14%
10,000,001 to $25,000,000	13%	12%
More than $25,000,000	8%	5%
Total	100%	100%
Extrapolated value	$6,842,250	$5,435,650

Q38. To understand the relationship of each of the seven (7) categories to the total cost of attacks against knowledge assets, please allocate points to each category for a total of 100 points.	FY2017	FY2016*
Remediation & technical support activities	11	14
Users' downtime and lost productivity	10	12
Disruptions to normal business operations	17	21
Damage or theft of IT assets and infrastructure	8	9
Revenue loss and customer turnover (churn)	9	
Reputation loss and brand damage	40	44
Fines, penalties and lawsuits	5	
Total points	100	100

*Five categories in FY2016

Q39. What is the likelihood of a data breach involving knowledge assets over the next 12 months?	FY2017	FY2016
Less than 1%	0%	4%
1% to 5%	6%	0%
6% to 10%	6%	14%
11% to 15%	9%	17%
16% to 20%	18%	18%
21% to 25%	24%	25%
26% to 50%	30%	22%
More than 50%	7%	0%
Total	100%	100%
Extrapolated value	25.7%	20.6%

Q40. What is the mean time to identify (MTTI) a data breach involving a knowledge asset caused by a careless insider?	FY2017
Less than 1 day	0%
1 to 10 days	5%
11 to 50 days	7%
51 to 100 days	14%
101 to 150 days	21%
151 to 200 days	18%
201 to 300 days	18%
301 to 600 days	12%
More than 600 days	5%
Total	100%
Extrapolated value (days)	202.6

Q41. What is the mean time to contain (MTTC) a data breach involving a knowledge asset caused by a careless insider?	FY2017
Less than 1 day	5%
1 to 10 days	13%
11 to 50 days	38%
51 to 100 days	23%
101 to 150 days	9%
151 to 200 days	6%
201 to 300 days	3%
301 to 600 days	1%
More than 600 days	2%
Total	100%
Extrapolated value (days)	76.3

Q42. What is the mean time to identify (MTTI) a data breach involving a knowledge asset caused by a malicious outsider?	FY2017
Less than 1 day	0%
1 to 10 days	1%
11 to 50 days	6%
51 to 100 days	5%
101 to 150 days	12%
151 to 200 days	15%
201 to 300 days	19%
301 to 600 days	23%
More than 600 days	19%
Total	100%
Extrapolated value (days)	323.3

Q43. What is the mean time to contain (MTTC) a data breach involving a knowledge asset caused by a malicious outsider?	FY2017
Less than 1 day	1%
1 to 10 days	2%
11 to 50 days	12%
51 to 100 days	30%
101 to 150 days	18%
151 to 200 days	17%
201 to 300 days	10%
301 to 600 days	8%
More than 600 days	2%
Total	100%
Extrapolated value (days)	152.7

Q44. Approximately, what percentage of the total cost is due to careless insiders?	FY2017
Zero	0%
Less than 10%	11%
10% to 25%	23%
26% to 50%	19%
51% to 75%	32%
76% to 100%	15%
Total	100%
Extrapolated value (days)	45%

Q45. Approximately, what percentage of the total cost is due to malicious outsiders?	FY2017
Zero	0%
Less than 10%	9%
10% to 25%	15%
26% to 50%	18%
51% to 75%	30%
76% to 100%	28%
Total	100%
Extrapolated value (days)	53%

Q46. What is the **maximum loss** that your organization could experience as a result of a material data breach of knowledge assets?	FY2017	FY2016
Less than $500,000	0%	0%
500,000 to $1,000,000	0%	1%
1,000,001 to $5,000,000	2%	3%
5,000,001 to $10,000,000	1%	5%
10,000,001 to $25,000,000	2%	7%
25,000,001 to $50,000,000	4%	7%
50,000,000 to $100,000,000	7%	10%
100,000,000 to $250,000,000	25%	18%
250,000,000 to $500,000,000	36%	30%
More than $500,000,000	23%	19%
Total	100%	100%
Extrapolated value	$323,985,000	$269,822,500

Part 6. Organizational Characteristics & Demographics

D1. What organizational level best describes your current position?	FY2017	FY2016
Senior Executive	3%	2%
Vice President	2%	3%
Director	16%	17%
Manager	21%	20%
Supervisor	14%	15%
Technician	35%	33%
Staff	9%	8%
Contractor	0%	2%
Total	100%	100%

D2. Check the **Primary Person** you or your leader reports to within the organization.	FY2017	FY2016
CEO/Executive Committee	1%	2%
Chief Financial Officer (CFO)	2%	2%
General Counsel	4%	5%
Chief Information Officer (CIO)	51%	53%
Chief Information Security Officer (CISO)	22%	18%
Compliance Officer	7%	10%
Human Resources VP	1%	0%
Chief Security Officer (CSO)	3%	2%
Chief Risk Officer (CRO)	9%	8%
Total	100%	100%

D3. What industry best describes your organization's **primary** industry classification?	FY2017	FY2016
Agriculture & food services	0%	1%
Communications	3%	3%
Consumer products	6%	5%
Defense & aerospace	1%	0%
Education & research	2%	2%
Energy & utilities	5%	6%
Financial services	18%	19%
Health & pharmaceutical	10%	11%
Hospitality & leisure	3%	4%
Industrial & manufacturing	11%	10%
Media & entertainment	1%	2%
Public sector	12%	12%
Retail	10%	9%
Services	9%	9%
Technology & software	7%	5%
Transportation	2%	2%
Other	0%	0%
Total	100%	100%

D4. Where are your employees located? Check all that apply.	FY2017	FY2016
United States	100%	100%
Canada	71%	70%
Europe	70%	68%
Middle East & Africa	46%	44%
Asia-Pacific	63%	61%
Latin America (including Mexico)	57%	58%

D5. What is the worldwide headcount of your organization?	FY2017	FY2016
Less than 500	9%	10%
500 to 1,000	18%	21%
1,001 to 5,000	27%	29%
5,001 to 25,000	19%	20%
25,001 to 50,000	8%	0%
50,001 to 75,000	12%	12%
More than 75,000	7%	8%
Total	100%	100%

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

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

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