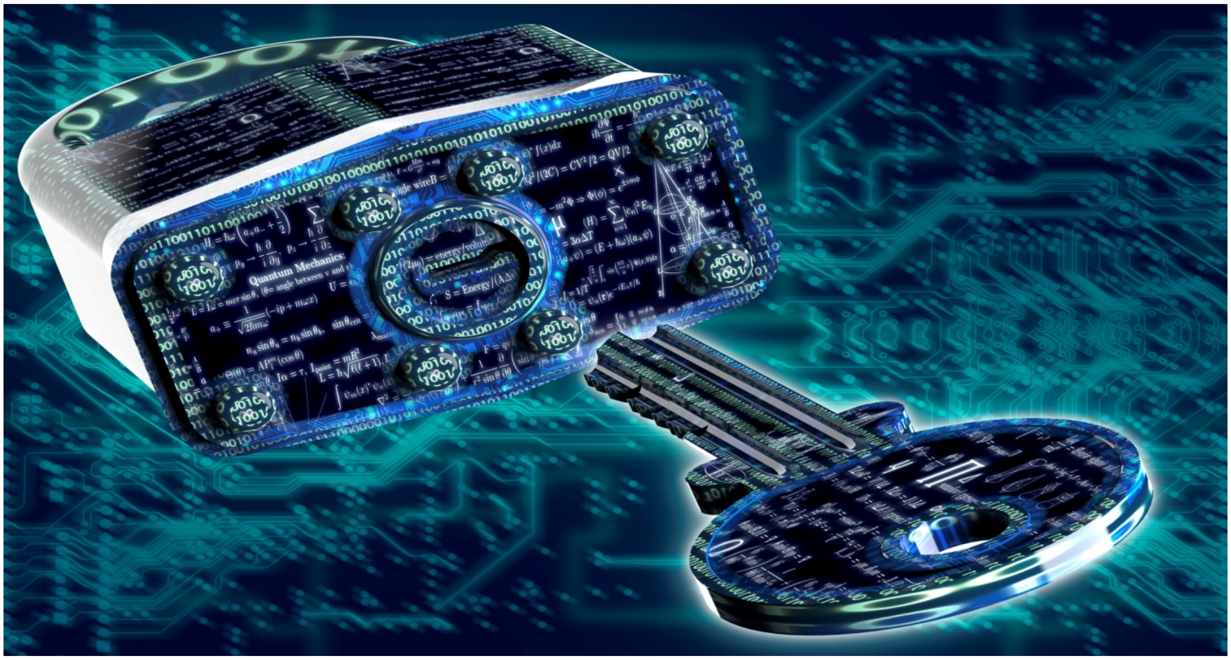


The Cybersecurity Risk to Knowledge Assets

Co-authored by Kilpatrick Townsend and Ponemon Institute

Independently conducted by Ponemon Institute LLC

Publication Date: July 2016

The Cybersecurity Risk to Knowledge Assets

Kilpatrick Townsend and Ponemon Institute, July 2016

Part 1. Executive Summary

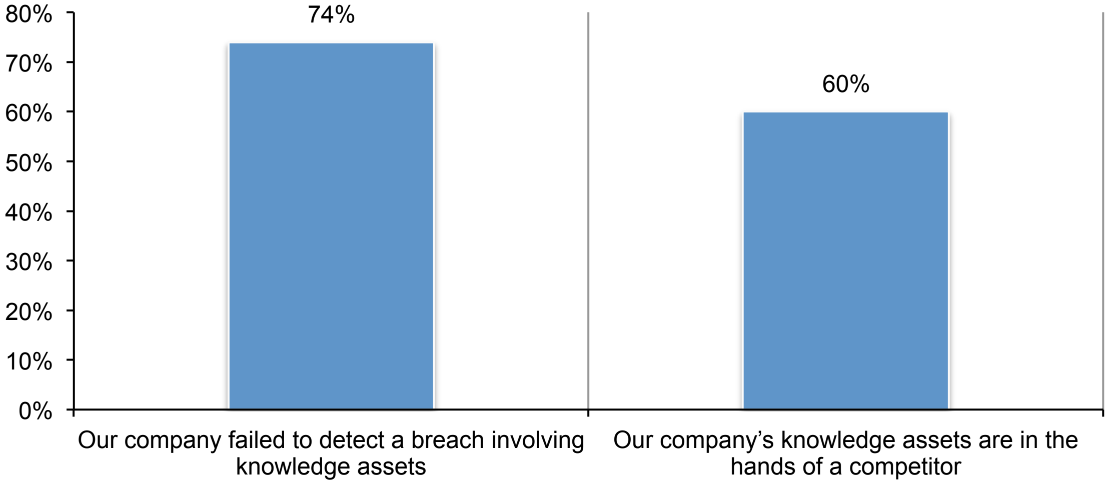
The Cybersecurity Risk to Knowledge Assets, produced in collaboration between Kilpatrick Townsend and Ponemon Institute was conducted to determine whether the publicity accorded data breaches subject to notification laws and related regulatory requirements has skewed the focus of organizations away from the theft or loss of their most critical information, and to provide helpful practices to reduce the risk. In the context of this research, knowledge assets are considered confidential information critical to the development, performance and marketing of a company's core businesses. [1]

Whether the result of a nation state attack, a careless or malicious insider or a third party, the loss of knowledge assets can affect a company's reputation and have significant financial consequences. In fact, the cost of attacks against companies' knowledge assets over the past 12 months averaged more than $5 million. Most of this cost involved dealing with the loss of reputation and brand damage. Companies with cyber insurance report on average that only 35 percent of losses involving knowledge assets are covered.

How serious is the threat? As shown in Figure 1, 74 percent of respondents say it is likely that their company failed to detect a data breach involving the loss or theft of knowledge assets and 60 percent of respondents say it is likely that one or more pieces of their company's knowledge assets are now in the hands of a competitor.

Figure 1. Why knowledge assets are at risk

Very likely and Somewhat likely response combined



[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.

More than 600 individuals in the United States familiar with and involved in their company's approach to managing knowledge assets were surveyed. All companies represented in this research have a program or set of activities for managing knowledge assets.

The research addressed the following topics and the most salient takeaways are discussed below.

- Understanding the risk to knowledge assets
- Data breaches involving knowledge assets
- How to protect knowledge assets

Understanding the risk to knowledge assets

The risk to knowledge assets is increasing. The protection of knowledge assets is difficult to achieve, according to 69 percent of respondents. Further, 50 percent of respondents say the theft of knowledge assets is increasing in their companies.

Employee negligence and third parties threaten the security of knowledge assets. While 59 percent of respondents say their organizations restrict employee access to knowledge assets based on a need-to-know basis, the biggest threat is employee negligence. This finding indicates that access control processes may not be working. Similarly, 67 percent of respondents say third-party access to their company's knowledge assets poses a serious risk.

Nation state attacks are also a serious threat. Fifty percent of respondents say such an attack is very likely (17 percent) or somewhat likely (33 percent). When respondents are asked to rank the main motivations of attackers, the top reasons given for stealing knowledge assets are economic espionage and hactivism.

IT security believes current approaches to protecting knowledge assets are ineffective. Only 28 percent of respondents rate the ability of their companies to mitigate the loss or theft of knowledge assets by insiders and external attackers as highly effective. Reasons they believe they are effective include: restriction of access to only those who need-to-know (64 percent of respondents) and creation of employee awareness about information risk (56 percent of respondents). The 72 percent of respondents who say current approaches are not effective cite such reasons as a lack of in-house expertise (67 percent), lack of clear leadership (59 percent) and a lack of collaboration with other functions (56 percent).

Data breaches involving knowledge assets

Executives worry more about data breaches that trigger a notification. A data breach involving high-value information assets would impact a company's ability to continue as a going concern, according to 59 percent of respondents. However, 53 percent of respondents say senior management is more concerned about a data breach involving credit card information or Social Security numbers (SSNs) than the leakage of knowledge assets.

The board of directors is often in the dark about security issues pertaining to knowledge assets. Fewer than half of respondents (48 percent) say their company's board of directors is made aware of the steps taken to secure knowledge assets. Only 23 percent of respondents say the board is made aware of all breaches involving the loss or theft of knowledge assets.

Data breaches involving knowledge assets have multi-million dollar consequences. The average cost to remediate attacks against knowledge assets in the past 12 months was $5.4 million. Respondents were asked to allocate 100 points to five possible consequences of the cost of attacks against knowledge assets. Most of the cost involved reputation loss and brand damage, followed by disruption to normal operations.

Is cyber insurance sufficient to reduce the financial consequences of data breaches involving knowledge assets? Sixty percent of companies represented either have cyber insurance (29 percent of respondents) or plan to obtain coverage in the next 12 months (31 percent of respondents). On average, respondents indicated that only 35 percent of a loss resulting from the theft is believed to be covered by their company's current insurance program.

Chief Risk Officers (CROs) are more likely to favor cyber insurance. Forty-nine percent of respondents who self-reported they are CROs say their organizations have cyber insurance in contrast to other respondents (27 percent). Organizations with CROs also report a higher level of coverage of theft or loss of knowledge assets than other organizations (an average of 48 percent vs. an average of 34 percent).

How to protect knowledge assets

Strong governance improves the protection of knowledge assets. Only 31 percent of respondents agree that senior management makes the protection of knowledge assets a priority. Similarly, only 32 percent of respondents say their company's senior management understands the risk caused by insecure knowledge assets. Moreover, board members keep their heads in the sand—only 37 percent of respondents say their company's board of directors requires assurances that knowledge assets are managed and safeguarded appropriately.

Sharing knowledge assets with third parties should require strict safeguards. Fifty-seven percent of respondents say third parties have access to their companies' knowledge assets. These companies rely upon purported contractual indemnification by the third party (50 percent of respondents), encryption of data in motion (44 percent of respondents) and encryption of data at rest (40 percent of respondents).

A formal approach aligned with the IT security strategy is needed. Sixty-two percent of respondents believe the protection of knowledge assets is an integral part of their company's IT security strategy. The approach for protecting knowledge assets in the companies represented in this study is most often informal or "ad hoc". Seventy-five percent of respondents say the plan or approach is not aligned (40 percent of respondents) or only partially aligned (35 percent of respondents) with the company's IT security strategy.

Most incident response plans and audits are informal. Only 21 percent of respondents say their companies have a formal incident response plan. More companies have an informal plan (40 percent of respondents). Similarly, only 26 percent of respondents say their companies conduct formal assessments or audits to determine the cyber and data breach risks posed by insecure knowledge assets. Informal assessments are conducted in the 39 percent of companies represented in this research.

More centralized control over the protection of knowledge assets is needed. The individuals most likely to determine the approach to securing knowledge assets are the chief information officer (56 percent of respondents) and the chief compliance officer (45 percent of respondents). However, responsibility for protecting knowledge assets is dispersed throughout the organization with 23 percent of respondents saying the chief information officer is primarily responsible and 15 percent of respondents saying no one person or department is responsible.

Training programs are not addressing employee negligence. The careless insider is the primary cause of a data breach involving knowledge assets, despite policies and training programs in place. Sixty-five percent of respondents say their companies have rules and policies for the protection of knowledge assets. In those companies with policies, 65 percent of respondents say employees are trained to follow these policies.

Access to knowledge assets is not managed properly. The most likely root cause of a data breach involving knowledge assets is the careless employee, but 50 percent of respondents say both privileged and ordinary users have access to the company's knowledge assets. This finding indicates employees' access to this information is not often controlled**.**

Preventing access to knowledge assets from remote locations and preventing the use of personally-owned mobile devices could reduce the risk. Sixty-six percent of respondents say their companies permit employees to access knowledge assets from remote locations and 53 percent of respondents say employees are allowed to use their mobile device to access such information.

Sixty-one percent of respondents say their organizations take steps to minimize the risk of employee carelessness. These steps mainly include regular training and awareness (70 percent of respondents), monitoring of employees (65 percent of respondents) and audits and assessments of areas most vulnerable to employee negligence (43 percent of respondents).

Companies are storing knowledge assets in the cloud without careful vetting of the provider. Sixty-three percent of respondents say their company stores knowledge assets in the cloud. The steps taken to secure knowledge assets in the cloud are: identity and access governance (56 percent of respondents), contracts with purported indemnification by the cloud provider (49 percent of respondents) and encryption of data in motion (45 percent of respondents).

Only 33 percent of respondents say their companies carefully vet the cloud provider. Similarly, only 30 percent of respondents say they require proof that the cloud provider meets generally accepted security requirements and only 23 percent of respondents say their organizations require proof that the cloud provider adheres to compliance mandates.

Encryption and identity management and authentication are most often deployed to safeguard knowledge assets. To secure knowledge assets, most companies rely upon encryption for data at rest (54 percent of respondents), identity management and authentication (52 percent of respondents) and encryption for data in motion (49 percent of respondents).

Companies need to have a process in place to understand what high-value information they must secure. Only 31 percent of respondents say their company has a classification system that segments information assets based on value or priority to the organization.

The most difficult knowledge assets to secure are not appropriately safeguarded. Sixty-seven percent of respondents say private communications such as emails, texting and social media and 60 percent of respondents say product/market information are the most difficult to secure. Only 16 percent and 19 percent of respondents, respectively, say these knowledge assets are adequately secured.

Part 2. Key Findings

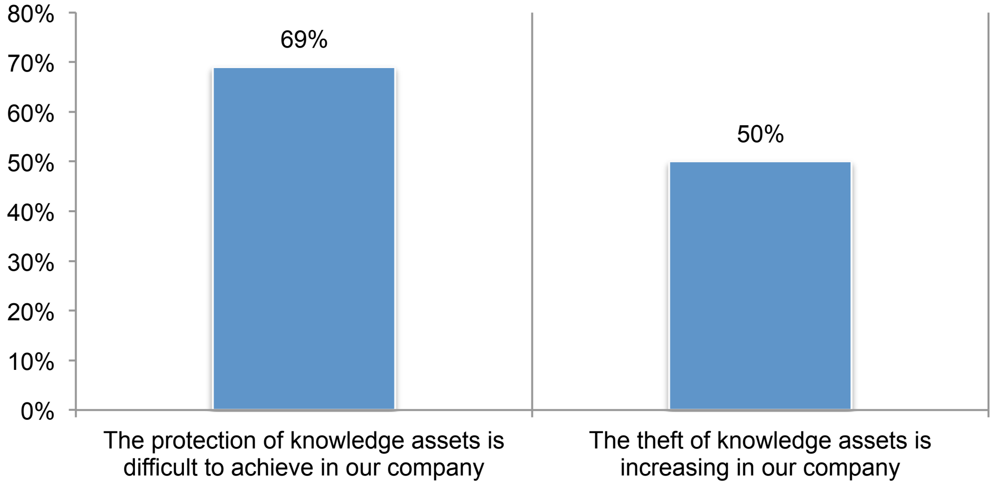
In this section, we provide a deeper analysis of the key findings. The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following topics.

- Understanding the risk to knowledge assets
- Data breaches involving knowledge assets
- How to protect knowledge assets

Understanding the risk to knowledge assets

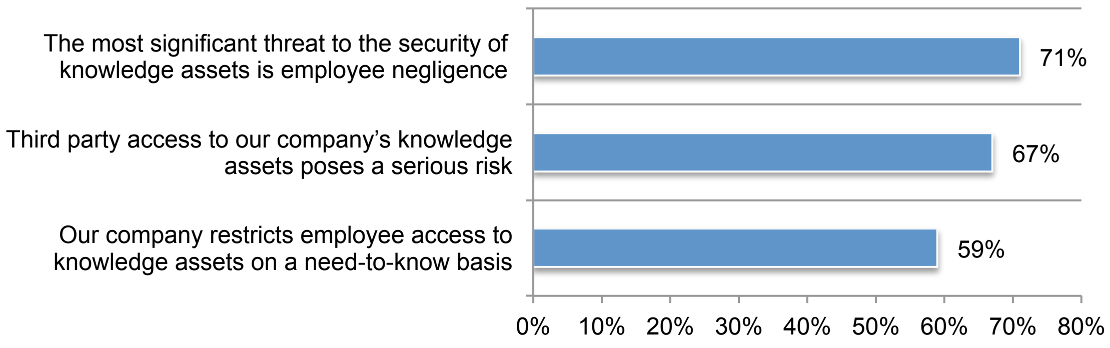
The risk to knowledge assets is increasing. The protection of knowledge assets is difficult to achieve, according to 69 percent of respondents. Further, 50 percent of respondents say the theft of knowledge assets is increasing in their companies, as shown in Figure 2.

Figure 2. What is the risk to knowledge assets?
Strongly agree and Agree responses combined



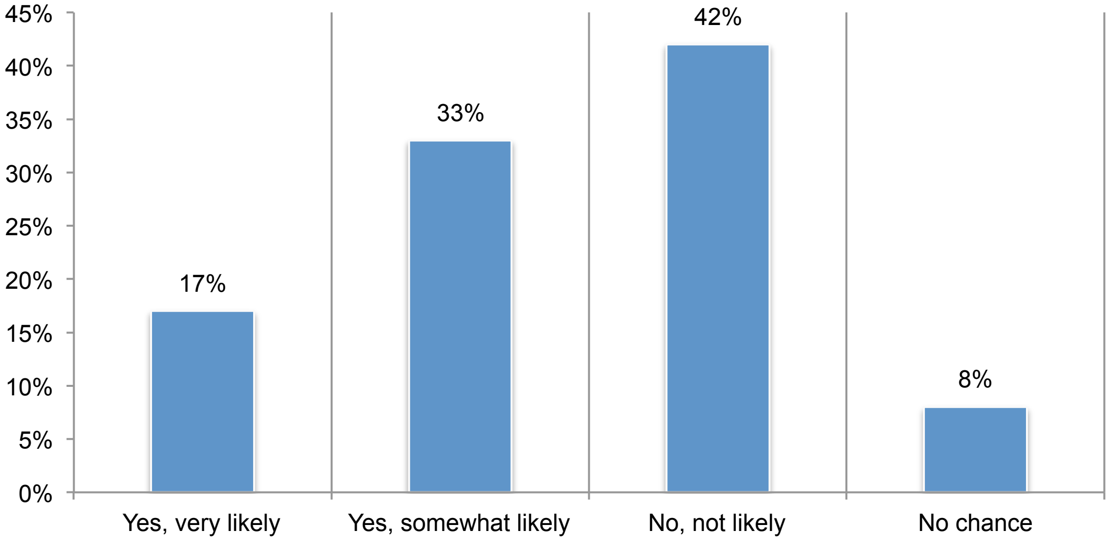
Employee negligence and third parties threaten the security of knowledge assets. While 59 percent of respondents say their organizations restrict employee access to knowledge assets based on a need-to-know basis, the biggest threat is employee negligence, as shown in Figure 3. This finding indicates that access control processes may not be working. Similarly, 67 percent of respondents say third-party access to their company's knowledge assets poses a serious risk.

Figure 3. Employee and third-party negligence puts knowledge assets at risk
Strongly agree and Agree responses combined



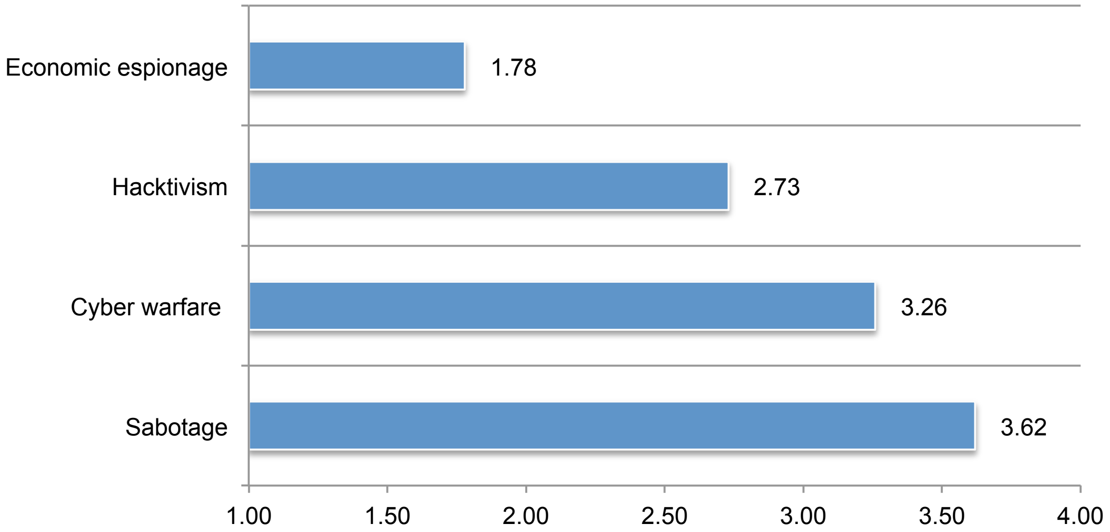
Nation state attacks are also a serious threat. As shown in Figure 4, 50 percent of respondents say it is very likely (17 percent) or somewhat likely (33 percent).

Figure 4. Do you believe your company's knowledge assets are targeted by nation state attacks?



When asked to rank the main motivations of attackers, the top two most likely reasons to steal knowledge assets are economic espionage and hacktivism, as shown in Figure 5.

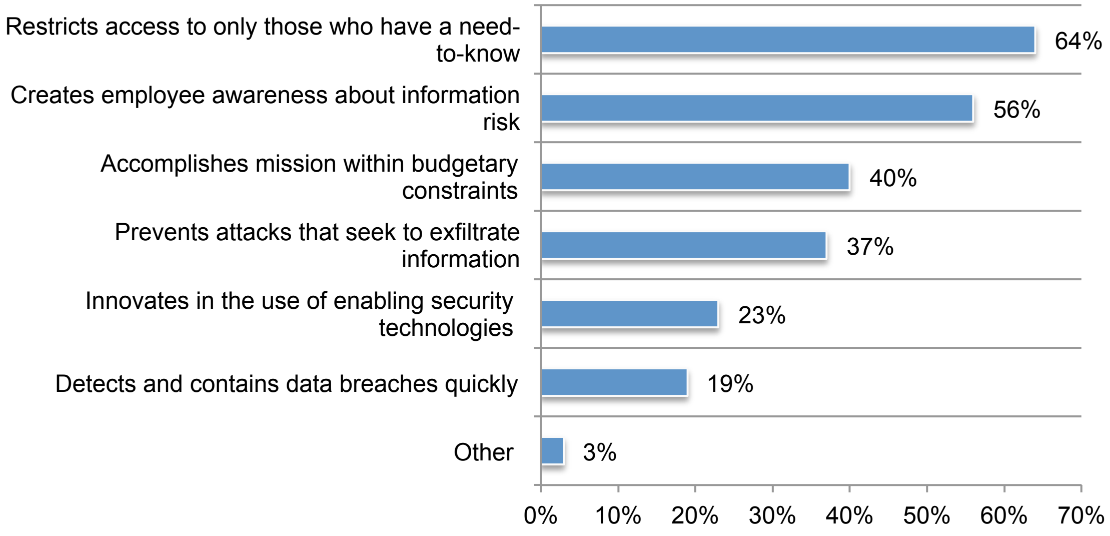
Figure 5. The main motivations of attackers who steal a company's knowledge assets
1 = most likely to 4 = least likely



IT security believes current approaches to protecting knowledge assets are ineffective. As discussed above, it is highly likely that one or more pieces of a company's knowledge assets are in the hands of a competitor. Accordingly, only 28 percent of respondents rate the ability of their companies to mitigate the loss or theft of knowledge assets by insiders and external attackers as highly effective.

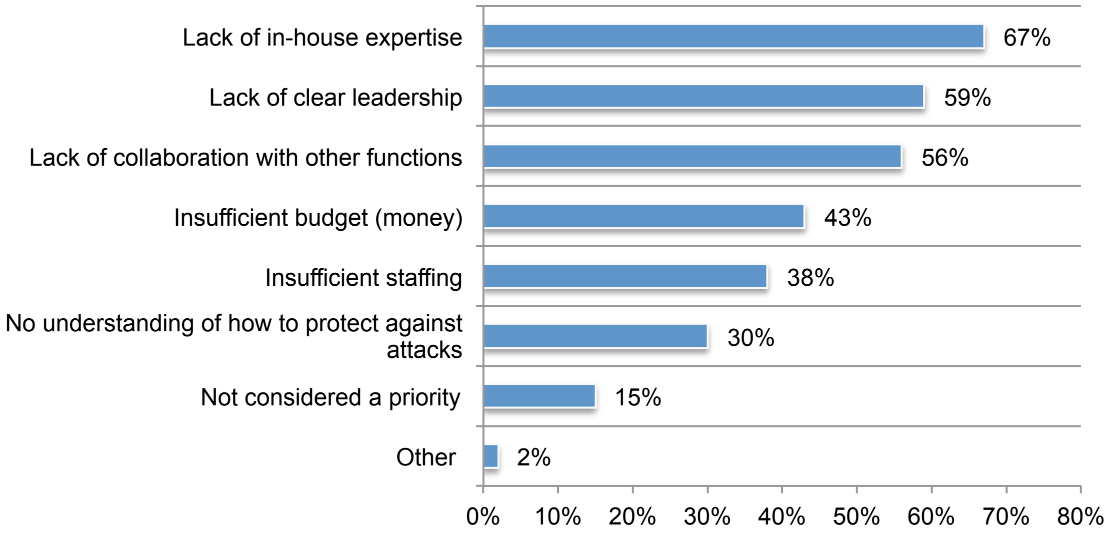
As presented in Figure 6, these respondents (28 percent) believe they are effective because they restrict access to only those who need-to-know (64 percent of respondents) and they create employee awareness about information risk (56 percent of respondents). However, only 19 percent of respondents say they are able to detect and contain data breaches quickly.

Figure 6. Why is your company effective in protecting knowledge assets?
More than one choice permitted



The 72 percent of respondents who say their companies are not effective cite such reasons as a lack of in-house expertise (67 percent), lack of clear leadership (59 percent) and a lack of collaboration with other functions (56 percent), as shown in Figure 7.

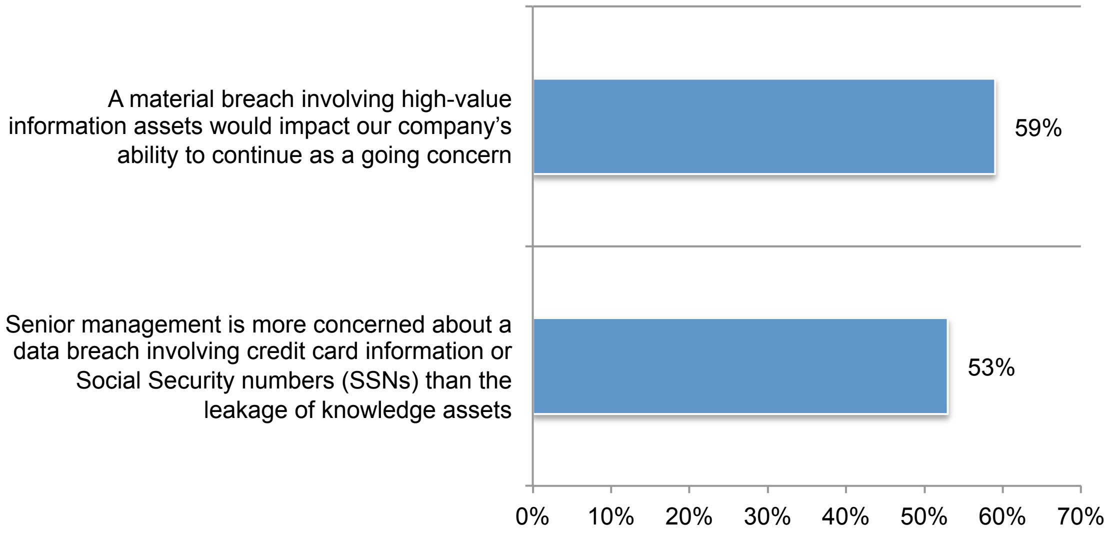
Figure 7. Why is your company not effective in protecting knowledge assets?
More than one choice permitted



Data breaches involving knowledge assets

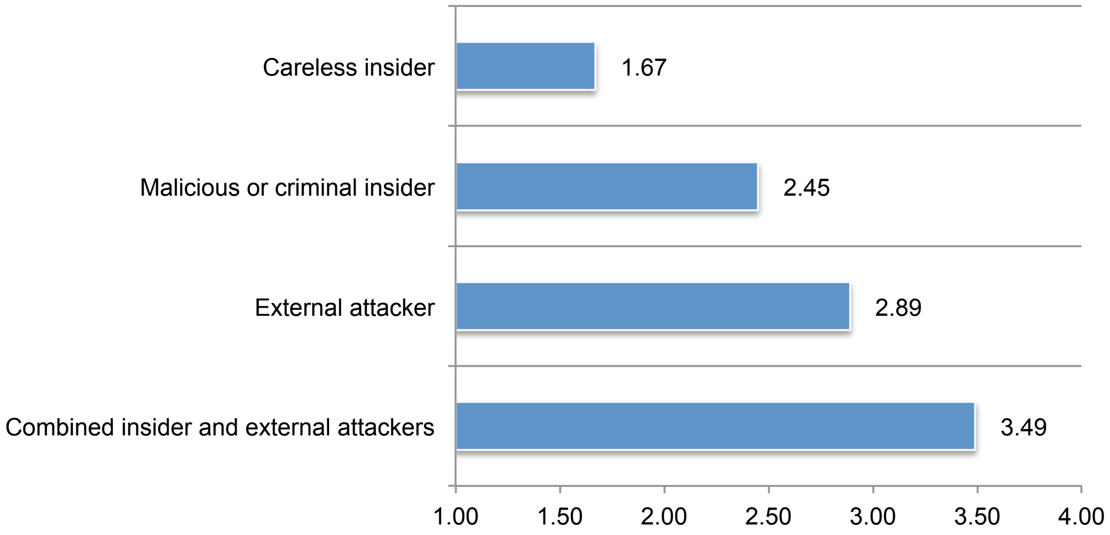
Executives worry more about data breaches that trigger a notification. According to Figure 8, a data breach involving high-value information assets would impact a company's ability to continue as a going concern, according to 59 percent of respondents. However, 53 percent of respondents say senior management is more concerned about a data breach involving credit card information or Social Security numbers (SSNs) than about the leakage of knowledge assets. The implication of this finding is that executives worry less about data breaches that are damaging to their company but do not trigger notification.

Figure 8. Perceptions about data breaches involving knowledge assets
Strongly agree and Agree responses combined



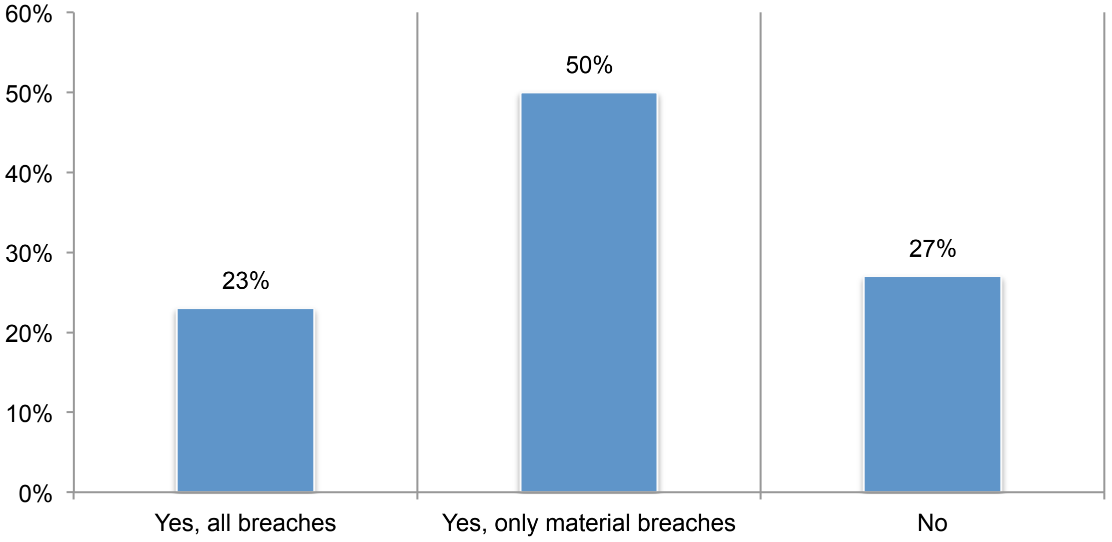
Insiders are most responsible for data breaches. Respondents were asked to rank four root causes of a data breach from most likely to least likely. Both careless and malicious insiders are most likely to cause the loss of knowledge assets, as presented in Figure 9.

Figure 9. The most likely root causes of data breaches
1 = most likely to 4 = least likely



The board of directors is often in the dark about security issues pertaining to knowledge assets. Fewer than half of respondents (48 percent) say their company's board of directors is made aware of the steps taken to secure knowledge assets. As shown in Figure 10, only 23 percent of respondents say the board is made aware of all breaches involving the loss or theft of knowledge assets.

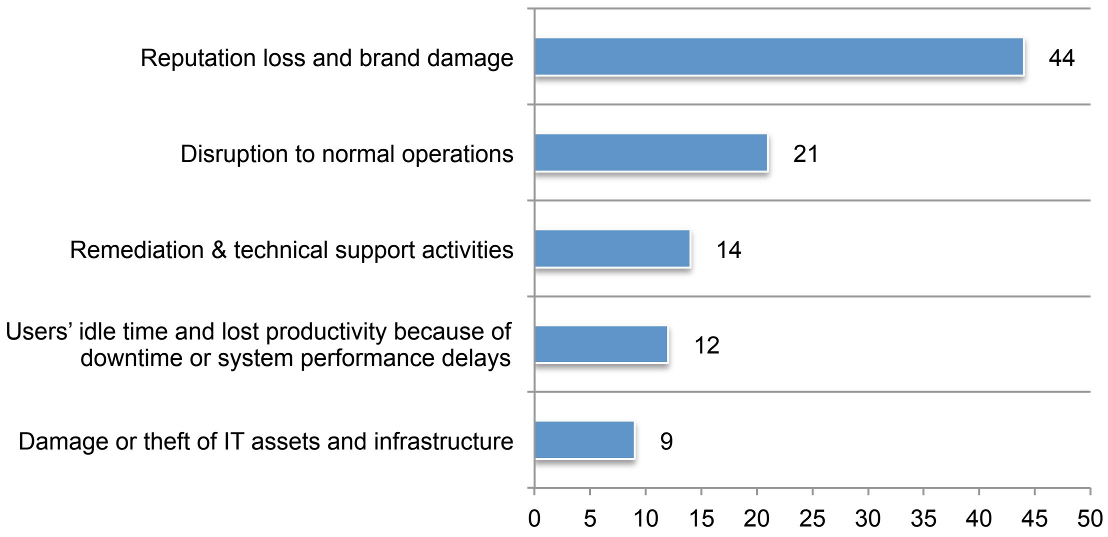
Figure 10. Is your company's board of directors made aware of breaches involving the loss or theft of knowledge assets?



Data breaches involving knowledge assets have multi-million dollar consequences. The average cost to remediate attacks against knowledge assets in the past 12 months was $5.4 million. Respondents were asked to allocate 100 points to five possible consequences of the cost of attacks against knowledge assets. As shown in Figure 11, most of the cost involved reputation loss and brand damage followed by disruption to normal operations, as shown in Figure 11.

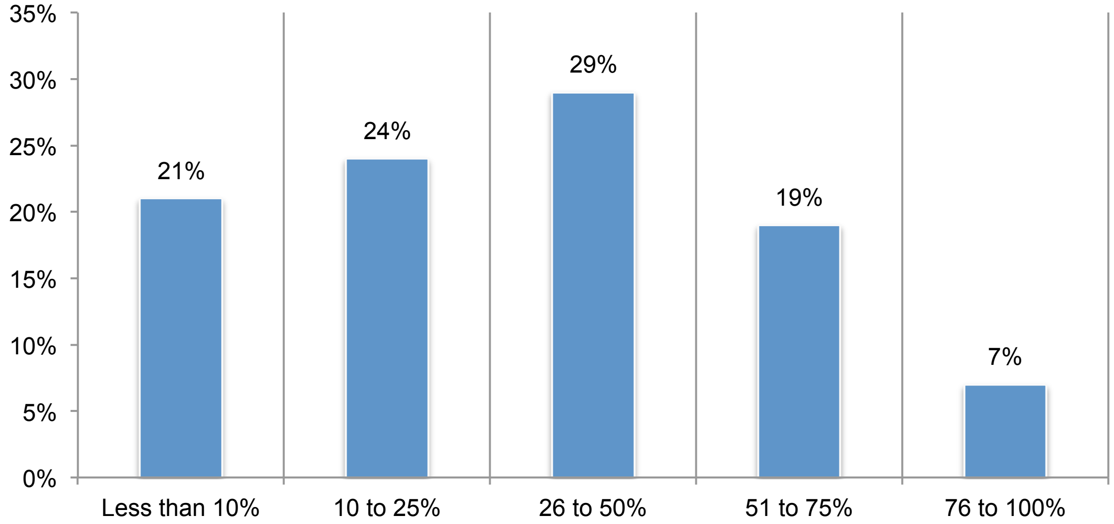
There is also a 15 percent likelihood of a material data breach involving knowledge assets in the next 12 months. The maximum loss that their organization could experience as a result of a material data breach of knowledge assets would be as much as $270 million.

Figure 11. Allocation of total cost of attacks against knowledge assets
Total of 100 points



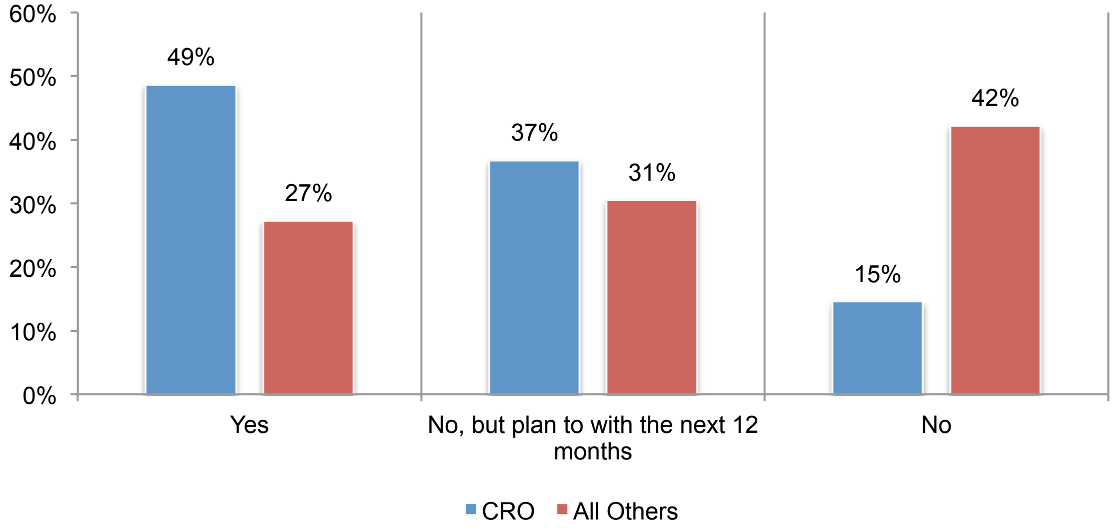
Is cyber insurance sufficient to reduce the financial consequences of data breaches involving knowledge assets? Sixty percent of companies represented either have cyber insurance (29 percent of respondents) or plan to obtain coverage in the next 12 months (31 percent of respondents). On average, according to Figure 13, only 35 percent of the loss resulting from the theft of knowledge assets is believed by respondents to be covered by their company's current insurance program.

Figure 13. How much of the loss resulting from the theft of knowledge assets is covered?
Extrapolated value = 35 percent



Chief Risk Officers (CROs) are more likely to favor cyber insurance. As shown in Figure 14, 49 percent of respondents who self-reported they are CROs say their organizations have cyber insurance in contrast to other respondents (27 percent of respondents). Organizations with CROs also report a higher level of coverage of knowledge assets than other organizations (an average of 47.7 percent vs. an average of 33.9 percent).

Figure 14. Does your company have cyber insurance?

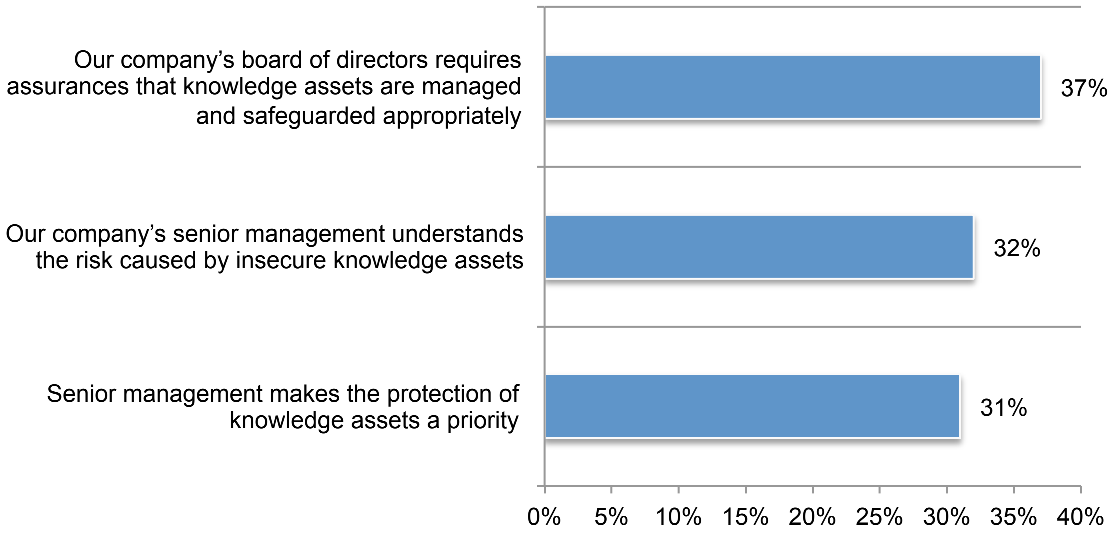


How to protect knowledge assets

Strong governance improves the protection of knowledge assets. As shown in Figure 15**,** a lack of senior-level and board of directors' support and understanding about the risk puts knowledge assets at risk. Only 31 percent of respondents agree that senior management makes the protection of knowledge assets a priority.

Similarly, only 32 percent of respondents say their company's senior management understands the risk caused by insecure knowledge assets. Moreover, board members keep their heads in the sand—only 37 percent of respondents say their company's board of directors requires assurances that knowledge assets are managed and safeguarded appropriately.

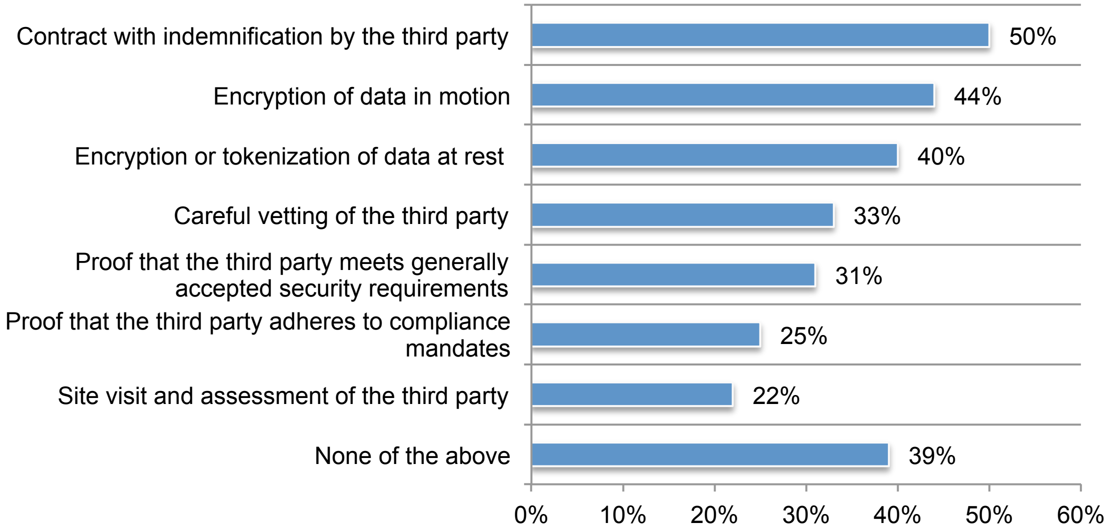
Figure 15. Perceptions about the role of senior management and board of directors in the security of knowledge assets
Strongly agree and Agree responses combined



Sharing knowledge assets with third parties should require strict safeguards. Fifty-seven percent of respondents say third parties have access to their company's knowledge assets.

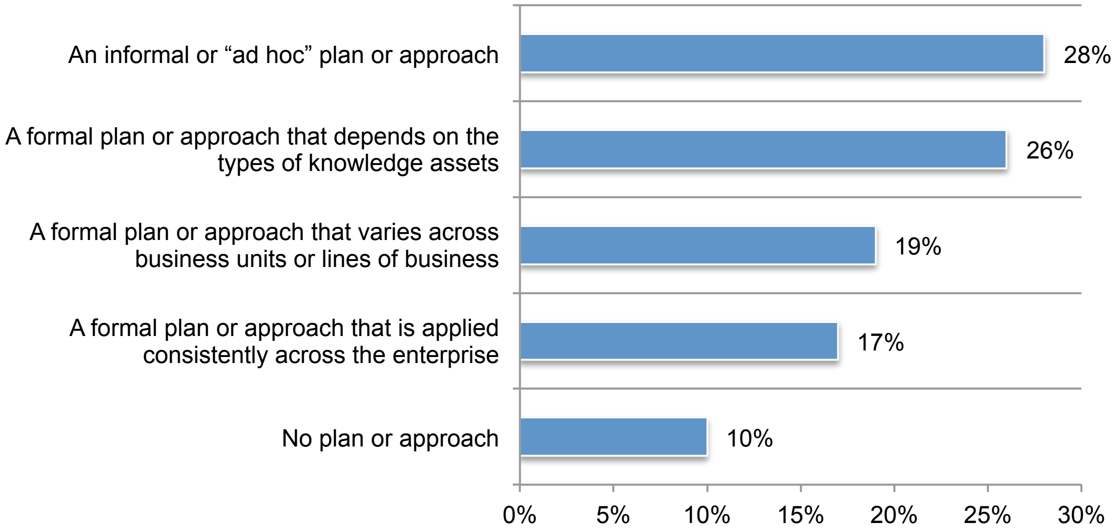
As shown in Figure 16, these companies rely upon purported contractual indemnification by the third party (50 percent of respondents), encryption of data in motion (44 percent of respondents) and encryption of data at rest (40 percent of respondents). Safeguarding high-value information in the hands of third parties requires a more proactive approach involving processes and technologies to protect knowledge assets.

Figure 16. Steps taken to protect knowledge assets shared with third parties
More than one choice permitted



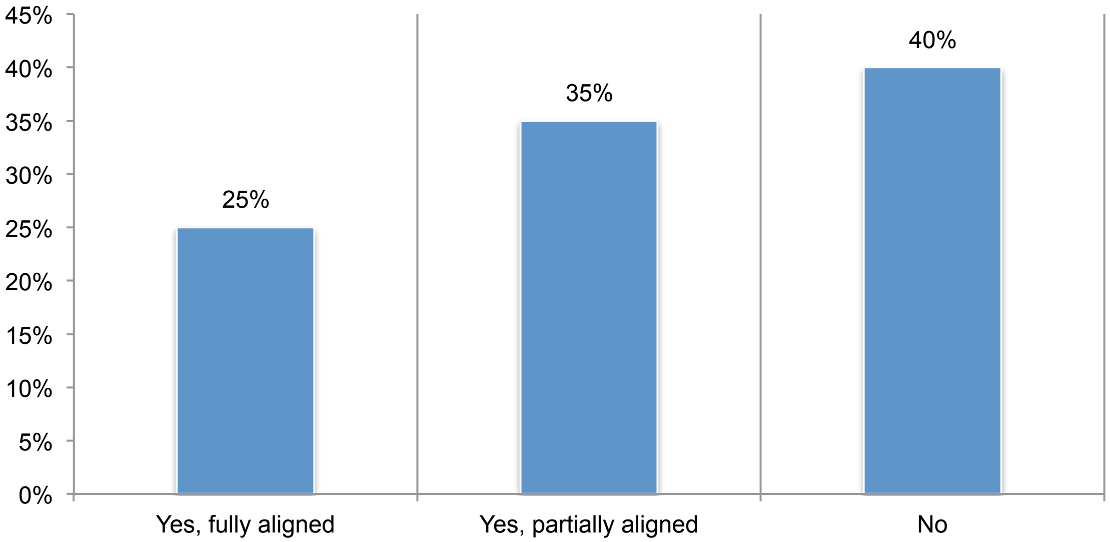
A formal approach aligned with the IT security strategy is needed. Sixty-two percent of respondents believe the protection of knowledge assets is an integral part of their company's IT security strategy. Figure 17 shows the approach for protecting knowledge assets in the companies represented in this study. Most often it is an informal or "ad hoc" approach.

Figure 17. What best describes your company's plan or approach for protecting knowledge assets?



Seventy-five percent of respondents say the plan or approach is not aligned (40 percent) or only partially aligned (35 percent) with the company's IT security strategy, according to Figure 18.

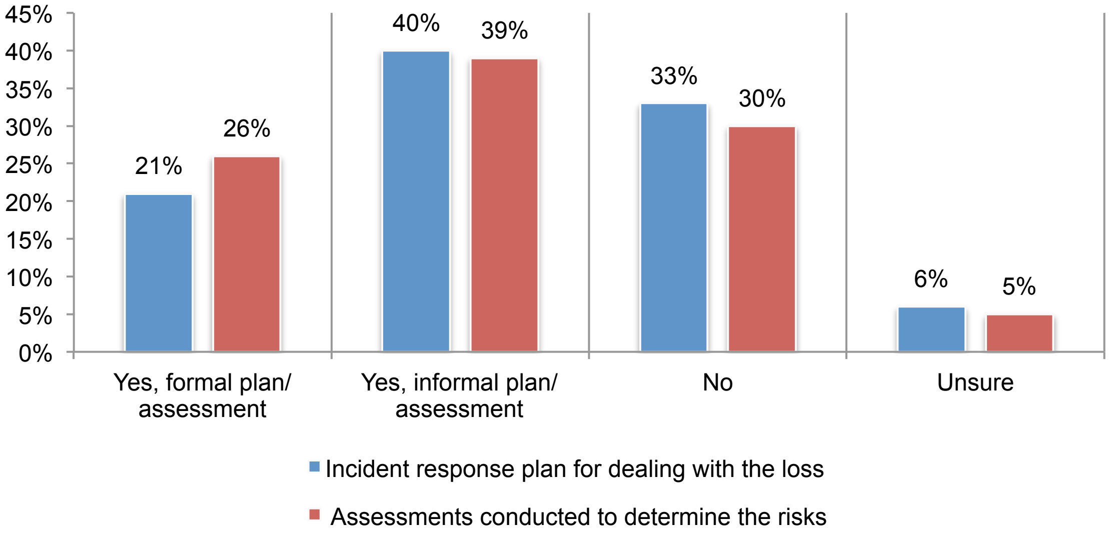
Figure 18. Is the plan or approach for protecting knowledge assets aligned with the company's IT security strategy?



Without a formalized strategy, knowledge assets are at risk. According to Figure 19, only 21 percent of companies represented in this study have a formal incident response plan. More companies (40 percent of respondents have an informal plan.

Similarly only 26 percent of respondents say they conduct formal assessments or audits to determine the cyber and data breach risks posed by insecure knowledge assets. Thirty-nine percent say audit and assessments are informal. Companies should create more formal plans in order to ensure that all processes and technologies are deployed to promptly respond to attacks against knowledge assets and to assess risks.

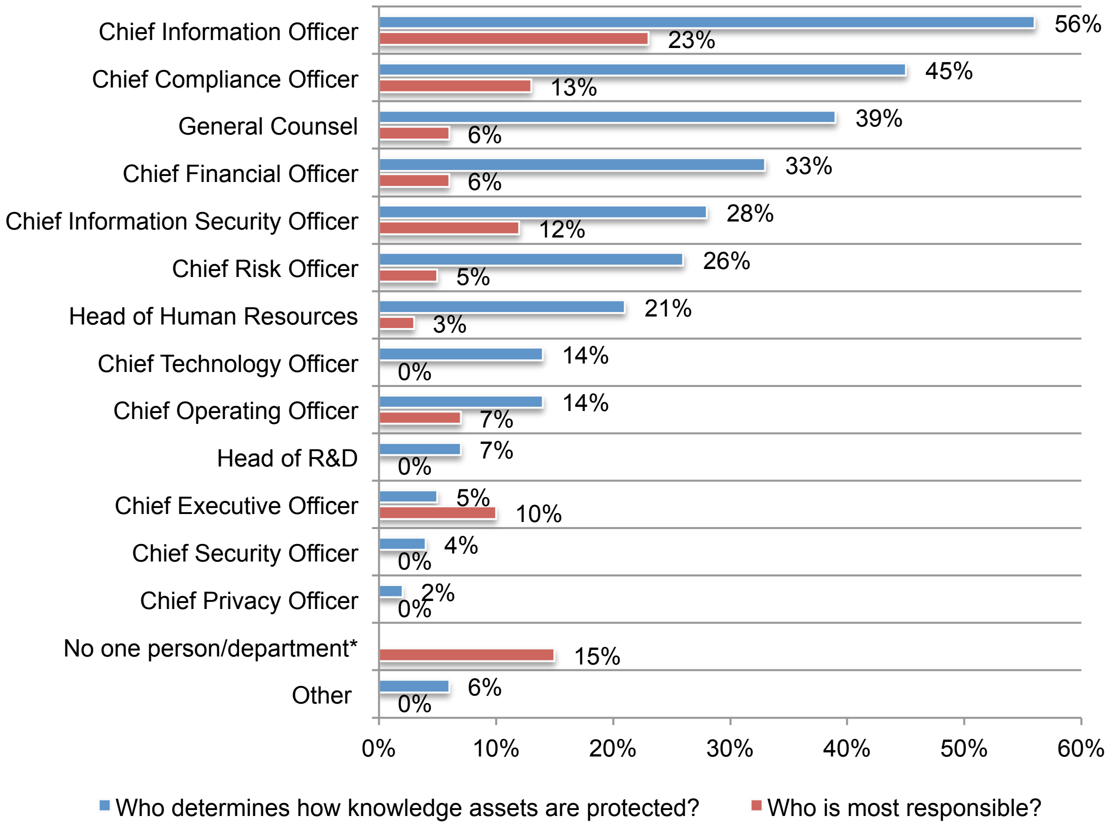
Figure 19. Steps taken to respond to data loss and determine risks



More centralized control over the protection of knowledge assets is needed. According to Figure 20 the individuals most likely to determine the approach to securing knowledge assets are the chief information officer (56 percent of respondents) and the chief compliance officer (45 percent of respondents).

However, responsibility for protecting knowledge assets is dispersed throughout the organization, with 23 percent of respondents saying the chief information officer is primarily responsible and 15 percent of respondents saying no one person or department is responsible.

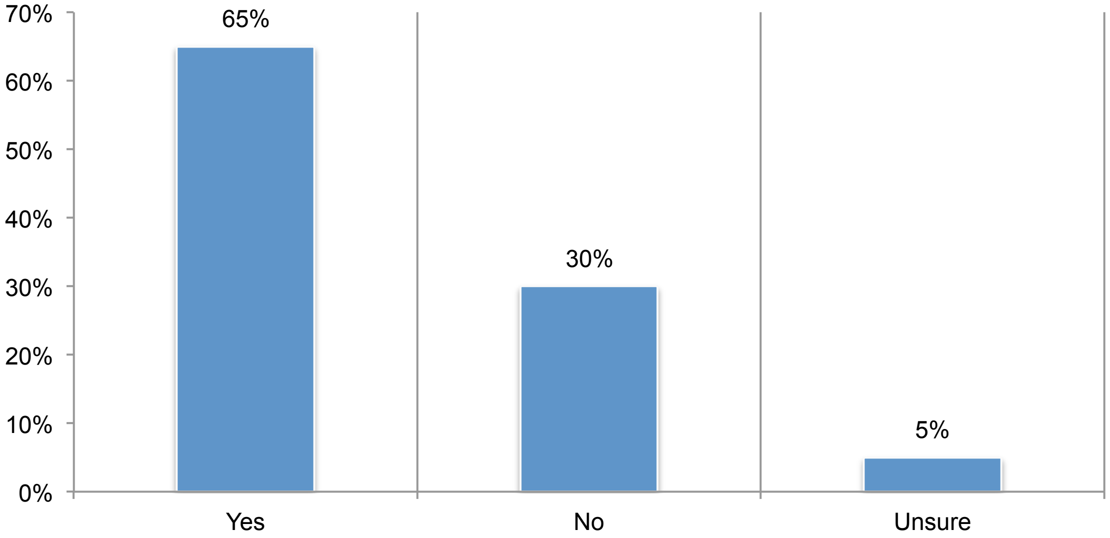
Figure 20. Who determines how knowledge assets are protected and who is most responsible?
More than one choice permitted



* Not a choice for this question

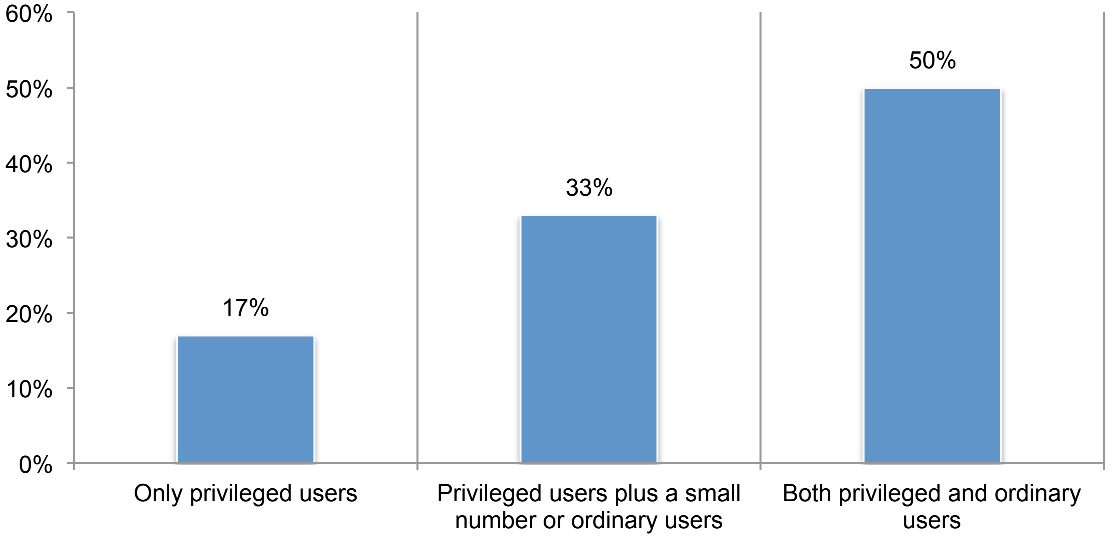
Training programs are not addressing employee negligence. The careless insider is the primary cause of a data breach involving knowledge assets despite policies and training programs in place. Sixty-five percent of respondents say their companies have rules and policies for the protection of knowledge assets. In those companies with policies, 65 percent of respondents say employees are trained to follow these policies, according to Figure 21.

Figure 21. Do you train employees to adhere to these rules and policies?



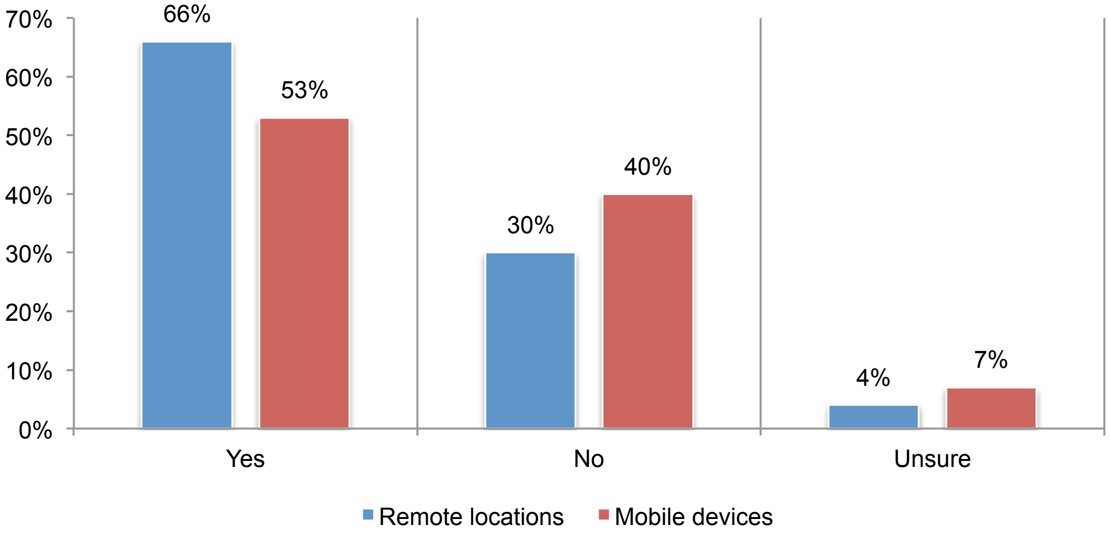
Access to knowledge assets is not managed properly. The most likely root cause of a data breach involving knowledge assets is the careless employee, but 50 percent of respondents say both privileged and ordinary users have access to the company's knowledge assets, as shown in Figure 22. This finding indicates employees' access to knowledge assets is not often controlled**.**

Figure 22. Who has access to your company's knowledge assets?



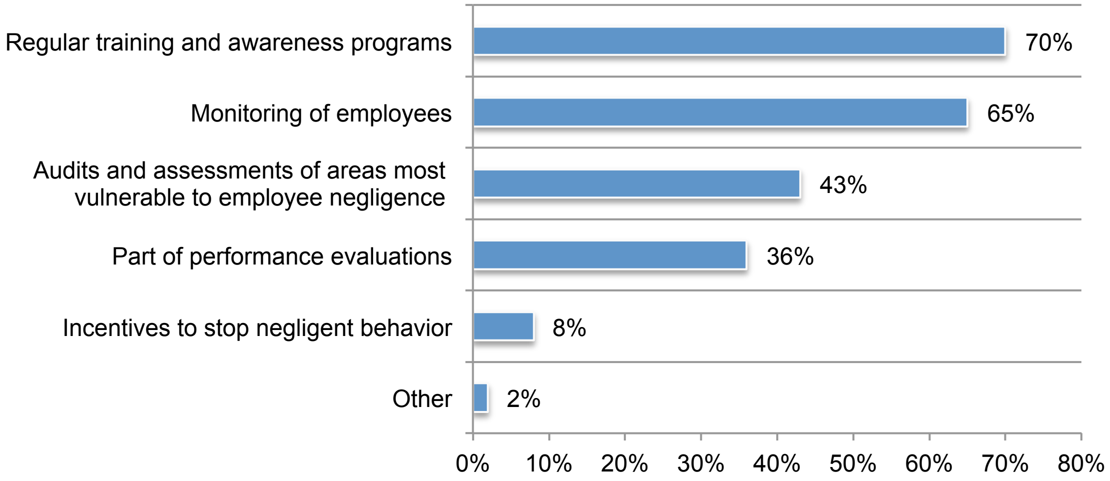
Preventing access to knowledge assets from remote locations and preventing the use of personally-owned mobile devices to access this information could reduce the risk. As presented in Figure 23, 66 percent of respondents say their companies permit employees to access knowledge assets from remote location and 53 percent of respondents say employees are allowed to use their mobile device to access such information.

Figure 23. Are employees allowed to access knowledge assets from remote locations and their mobile devices?



Sixty-one percent of respondents say their organizations take steps to minimize the risk of employee carelessness. According to Figure 24, these steps mainly include regular training and awareness (70 percent of respondents), monitoring of employees (65 percent of respondents) and audits and assessments of areas most vulnerable to employee negligence (43 percent of respondents).

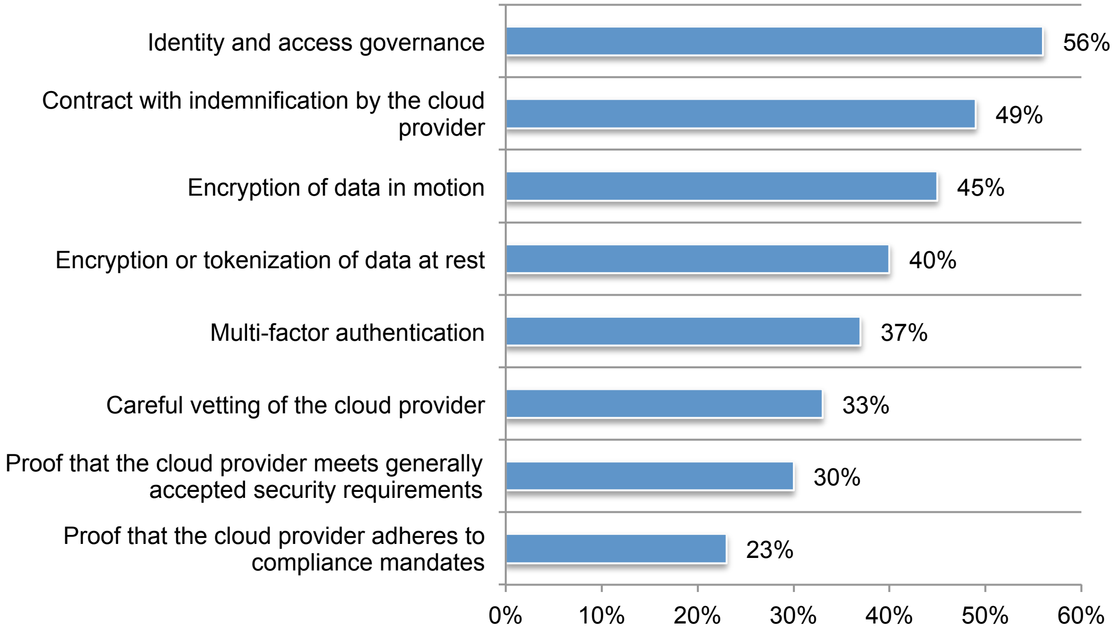
Figure 24. What steps are taken to address the risk of employee carelessness?
More than one choice permitted



Companies are storing knowledge assets in the cloud without careful vetting of the provider. Sixty-three percent of respondents say their company stores knowledge assets in the cloud. According to Figure 25, the steps taken to secure knowledge assets in the cloud are: identity and access governance (56 percent of respondents), contracts with purported indemnification by the cloud provider (49 percent of respondents) and encryption of data in motion (45 percent of respondents).

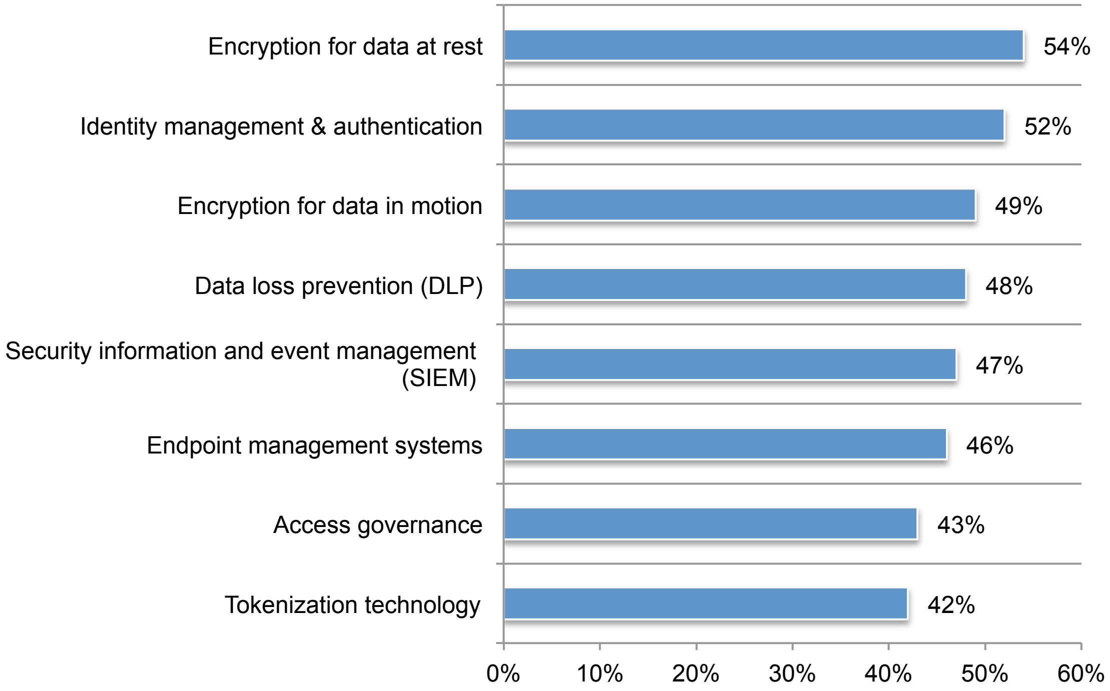
Only 33 percent of respondents say their companies carefully vet the cloud provider. Similarly, only 30 percent of respondents say they require proof that the cloud provider meets generally accepted security requirements, and only 23 percent of respondents say their organizations require proof that the cloud provider adheres to compliance mandates.

Figure 25. What steps are taken to secure knowledge assets in the cloud?
More than one choice permitted



Encryption and identity management and authentication are most often deployed to safeguard knowledge assets. As shown in Figure 26, to secure knowledge assets, most companies rely on encryption for data at rest (54 percent of respondents), identity management and authentication (52 percent of respondents) and encryption for data in motion (49 percent of respondents).

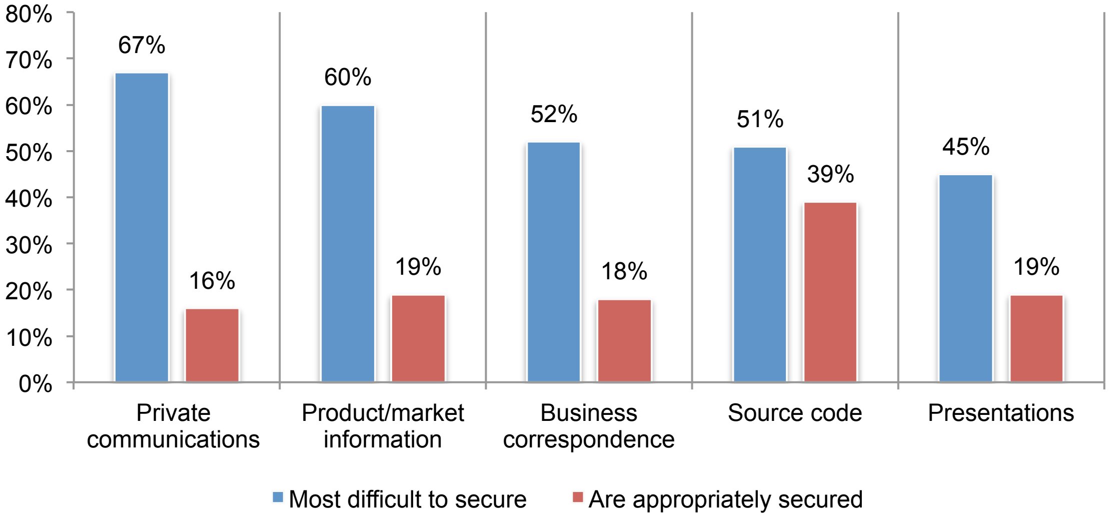
Figure 26. The most important security technologies for protecting knowledge assets
Eight choices permitted



Companies need to have a process in place to understand what high-value information they must secure. Only 31 percent of respondents say their company has a classification system that segments information assets based on value or priority to the organization.

The most difficult knowledge assets to secure are not appropriately safeguarded. Sixty-seven percent of respondents say private communications such as emails, texting and social media and 60 percent of respondents say product/market information are the most difficult to secure. According to Figure 27, only 16 percent and 19 percent of respondents, respectively, say these knowledge assets are adequately secured.

Figure 27. The top five knowledge asset categories most difficult to secure and appropriately secured
More than one choice permitted



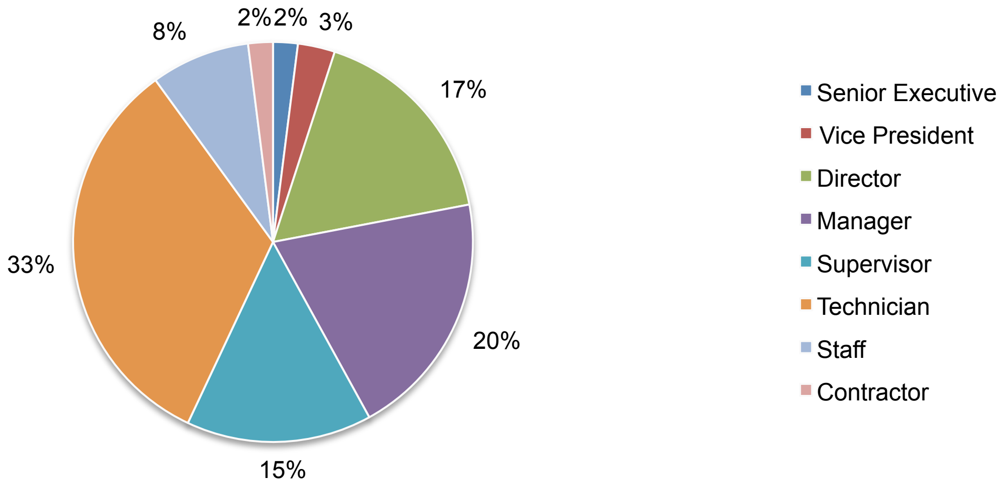
Part 3. Methods

A sampling frame of 17,540 individuals familiar with and involved in their company's approach to managing knowledge assets were selected as participants in the research. Table 1 shows 691 total returns. Screening and reliability checks required the removal of 88 surveys. Our final sample consisted of 603 surveys, or a 3.4 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	17,540	100.0%
Total returns	691	3.9%
Rejected or screened surveys	88	0.5%
Final sample	603	3.4%

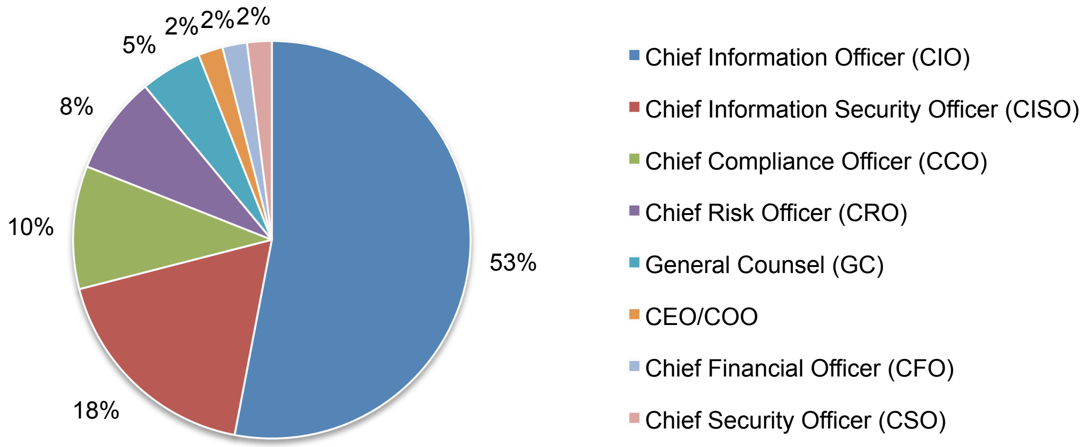
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half of the respondents (57 percent) are at or above the supervisory levels.

Pie Chart 1. Position level within the organization



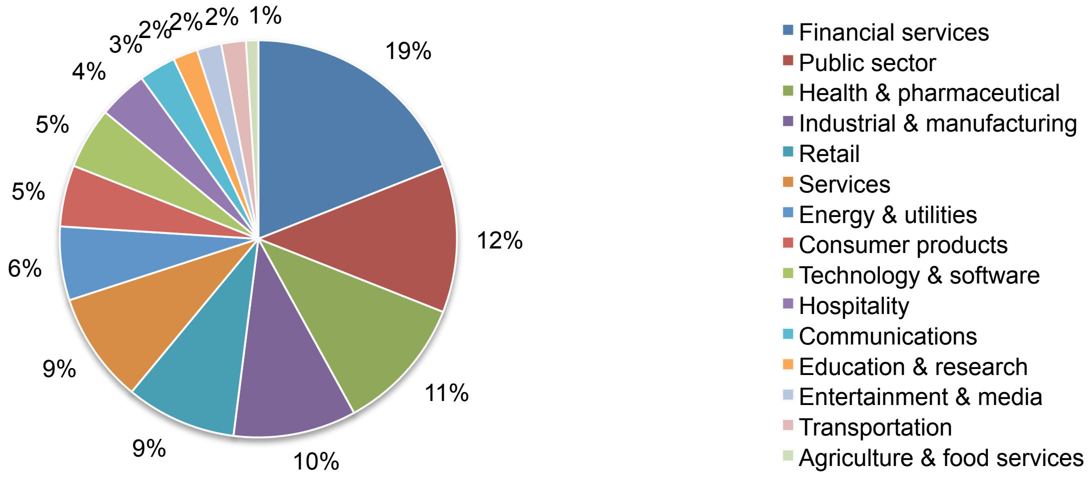
As shown in Pie Chart 2, 53 percent of respondents report directly to the CIO and 18 percent report to the CISO.

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



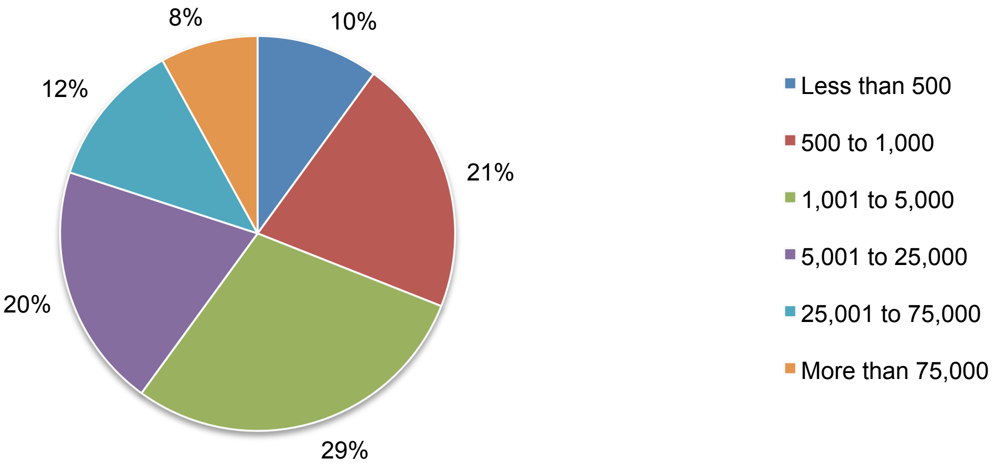
Pie Chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (19 percent of respondents) as the largest segment, followed by public sector (12 percent of respondents) and health and pharmaceutical (11 percent of respondents).

Pie Chart 3. Primary industry classification



According to Pie Chart 4, 69 percent of the IT respondents and end user respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 4. Worldwide headcount of the organization



In addition to the United States, 70 percent of respondents indicated their organization has employees located in Canada and 68 percent responded in Europe, as shown in Table 2.

Table 2. Global location of employees	
United States	100%
Canada	70%
Europe	68%
Asia-Pacific	61%
Latin America (including Mexico)	58%
Middle East & Africa	44%

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 in May 2016.

Survey response	**Freq**	**Pct%**
Total sampling frame	17,540	100.0%
Total returns	691	3.9%
Rejected or screened surveys	88	0.5%
Final sample	603	3.4%

Contextual response: please provide one example of a knowledge asset that is most valuable or important to your organization. Following is the **Top 10** list:	Freq	Pct%
Customer records	72	12%
Product design, development and pricing	55	9%
Early (pre-released) financial reports	41	7%
Board of director meeting minutes and correspondence	29	5%
Business process workflows	25	4%
Confidential information about mergers and acquisitions	19	3%
Source code	18	3%
Research and development	18	3%
Employee records	12	2%
Information about C-level executives	11	2%

Screening questions

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

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

S3. Do you have any involvement in managing knowledge assets?	Pct%
Yes, full involvement	23%
Yes, partial involvement	51%
Yes, minimal involvement	26%
No involvement (Stop)	0%
Total	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.	Pct%
Q1. Senior management makes the protection of knowledge assets a priority.	31%
Q2. Third-party access to our company's knowledge assets poses a serious risk.	67%
Q3. All information asset types are considered equal in terms of risk to our company.	22%
Q4. The protection of knowledge assets is an integral part of our company's IT security strategy.	62%
Q5. A material breach involving our high-value information assets would impact our company's ability to continue as a going concern.	59%
Q6. Our company's senior management understands the risk caused by insecure knowledge assets.	32%
Q7. 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.	53%
% Strongly Agree and Agree response combined.	Pct%
Q8. The most significant threat to the security of knowledge assets is employee negligence.	71%
Q9. Our company restricts employee access to knowledge assets based on a need-to-know basis.	59%
Q10. Our company's board of directors requires assurances that knowledge assets are managed and safeguarded appropriately.	37%
Q11. The theft of knowledge assets is increasing in our company.	50%
Q12. The protection of knowledge assets is difficult to achieve in our company.	69%

Part 3. Background

Q13. What best describes your company's plan or approach for protecting knowledge assets?	Pct%
A formal plan or approach that is applied consistently across the enterprise	17%
A formal plan or approach that varies across business units or lines of business	19%
A formal plan or approach that depends on the types of knowledge assets	26%
An informal or "ad hoc" plan or approach	28%
No plan or approach	10%
Total	100%

Q14. Who is involved in determining your company's approach for protecting knowledge assets? Top 3 choices.	Pct%
Chief Information Officer	56%
Chief Compliance Officer	45%
General Counsel	39%
Chief Financial Officer	33%
Chief Information Security Officer	28%
Chief Risk Officer	26%
Head of Human Resources	21%
Chief Operating Officer	14%
Chief Technology Officer	14%
Head of R&D	7%
Chief Executive Officer	5%
Chief Security Officer	4%
Chief Privacy Officer	2%
Other (please specify)	6%
Total	300%

Q15. Who is **most responsible** for protecting your company's knowledge assets?	Pct%
Chief Information Officer	23%
No one person/department	15%
Chief Compliance Officer	13%
Chief Information Security Officer	12%
Chief Executive Officer	10%
Chief Operating Officer	7%
Chief Financial Officer	6%
General Counsel	6%
Chief Risk Officer	5%
Head of Human Resources	3%
Chief Technology Officer	0%
Chief Security Officer	0%
Chief Privacy Officer	0%
Head of R&D	0%
Other (please specify)	0%
Total	100%

Q16. 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.	Pct%
1 or 2	11%
3 or 4	25%
5 or 6	36%
7 or 8	18%
9 or 10	10%
Total	100%
Extrapolated value	5.32

Q17.**For those who rate 6 and below**: What prevents your company from being very effective?	Pct%
Lack of in-house expertise	67%
Lack of clear leadership	59%
Lack of collaboration with other functions	56%
Insufficient budget (money)	43%
Insufficient staffing	38%
No understanding how to protect against attacks	30%
Not considered a priority	15%
Other (please specify)	2%
Total	310%

Q18**. For those who rate 7 and above**: Why is your company effective?	Pct%
Restricts access to only those who have a need-to-know	64%
Creates employee awareness about information risk	56%
Accomplishes mission within budgetary constraints	40%
Prevents attacks that seek to exfiltrate information	37%
Innovates in the use of enabling security technologies	23%
Detects and contains data breaches quickly	19%
Other (please specify)	3%
Total	242%

Q19. Is the plan or approach for protecting knowledge assets **aligned** with the company's IT security strategy?	Pct%
Yes, fully aligned	25%
Yes, partially aligned	35%
No	40%
Total	100%

Q20. Does your company have an incident response plan for dealing with the loss or theft of knowledge assets?	Pct%
Yes, formal plan	21%
Yes, informal plan	40%
No	33%
Unsure	6%
Total	100%

Q21. Does your company conduct assessments to determine the risks posed by insecure knowledge assets?	Pct%
Yes, formal assessment or audit	26%
Yes, informal assessment	39%
No	30%
Unsure	5%
Total	100%

Q22. 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?	Pct%
Very likely	24%
Somewhat likely	36%
Not likely	30%
No chance	10%
Total	100%

Q23. In your opinion, what is the likelihood that your company **failed to detect** a data breach involving the loss or theft of knowledge assets?	Pct%
Very likely	34%
Somewhat likely	40%
Not likely	21%
No chance	5%
Total	100%

Q24. 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.	Average rank	Rank Order
Careless insider	1.67	1
Malicious or criminal insider	2.45	2
External attacker	2.89	3
Combined insider and external attackers	3.49	4
Average	2.63	

Q25. 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.	Average rank	Rank Order
Economic espionage	1.78	1
Sabotage	3.62	4
Hacktivism	2.73	2
Cyber warfare (nation-state attacks)	3.26	3
Total	2.85	

Q26a. Does your organization take steps to address the risk of employee carelessness in the handling of knowledge assets?	Pct%
Yes	61%
No	30%
Unsure	9%
Total	100%

Q26b. If yes, what steps does it take?	Pct%
Regular training and awareness programs	70%
Monitoring of employees	65%
Audits and assessments of areas most vulnerable to employee negligence	43%
Part of performance evaluations	36%
Incentives to stop negligent behavior	8%
Other	2%
Total	224%

Q27a. Does your company have rules and policies for the protection of knowledge assets?	Pct%
Yes	65%
No	26%
Unsure	9%
Total	100%

Q27b. If yes, do you train employees to adhere to these rules and policies?	Pct%
Yes	65%
No	30%
Unsure	5%
Total	100%

Q28. Are employees allowed to access knowledge assets from remote locations?	Pct%
Yes	66%
No	30%
Unsure	4%
Total	100%

Q29. Are employees allowed to access knowledge assets from their mobile device (including BYOD)?	Pct%
Yes	53%
No	40%
Unsure	7%
Total	100%

Q30. Over the last two years, has the threat against knowledge assets increased, decreased or stayed the same?	Pct%
Increased	43%
Stayed the same	49%
Decreased	8%
Total	100%

Q31a. Does your company store knowledge assets in the cloud?	Pct%
Yes	63%
No	26%
Unsure	11%
Total	100%

Q31b. What steps does your company take to secure knowledge assets in the cloud?	Pct%
Identity and access governance	56%
Contract with indemnification by the cloud provider	49%
Encryption of data in motion	45%
Encryption or tokenization of data at rest	40%
Multi-factor authentication	37%
Careful vetting of the cloud provider	33%
Proof that the cloud provider meets generally accepted security requirements	30%
Proof that the cloud provider adheres to compliance mandates	23%
Other (please specify)	0%
Total	313%

Q32. Is funding adequate to safeguard knowledge assets within our company?	Pct%
Yes, more than adequate (generous)	11%
Yes, adequate	54%
No, inadequate	26%
Unsure	9%
Total	100%

Q33. Does your organization have a specific budget for safeguarding knowledge assets?	Pct%
Yes	37%
No	55%
Unsure	8%
Total	100%

Q34. Following are 25 enabling security solutions. What are the most important enabling security technologies for protecting knowledge assets? Please select 8 top choices.	Pct%
Encryption for data at rest	54%
Identity management & authentication	52%
Encryption for data in motion	49%
Data loss prevention (DLP)	48%
Security information and event management (SIEM)	47%
Endpoint management systems	46%
Access governance	43%
Tokenization technology	42%
Traditional firewalls	40%
Hardware security modules (HSM)	39%
Mobile device management (MDM)	38%
Anti-virus & anti-malware	36%
Network and traffic intelligence systems	35%
Virtual private networks (VPN)	33%
Web application firewalls (WAF)	23%
Intrusion prevention systems (IPS)	22%
Penetration testing	22%
Intrusion detection systems (IDS)	21%
Governance, risk and compliance systems (eGRC)	21%
Next generation firewalls	19%
Secure USB flash device or mobile media	19%
Test data anonymization solution	17%
Big data analytics	15%
Code vulnerability scanning and debugging systems	14%
Other (please specify)	5%
Total	800%

Q35. Do you believe your company's knowledge assets are targeted by nation state attackers?	Pct%
Yes, very likely	17%
Yes, somewhat likely	33%
No, not likely	42%
No chance	8%
Total	100%

Q36. Is your company's board of directors made aware of the steps taken to secure knowledge assets?	Pct%
Yes	48%
No	43%
Unsure	9%
Total	100%

Q37. In your opinion, is your company's board of directors made aware of breaches involving the loss or theft of knowledge assets?	Pct%
Yes, all breaches	23%
Yes, only material breaches	50%
No	27%
Total	100%

Q38. Does your company have a classification system that segments information asset based on **value** or priority to the organization?	Pct%
Yes	31%
No	69%
Total	100%

Q39. Following are 13 categories of knowledge assets. Please select the five (5) knowledge asset categories that in your experience are most difficult to secure.	Pct%
Private communications (i.e., emails, texting, social media)	67%
Product/market information	60%
Business correspondence	52%
Source code	51%
Presentations	45%
Trade secrets	44%
Company-confidential information	40%
Operational information	40%
Financial information	37%
Research results	25%
Consumer data	18%
Analytics	11%
Attorney-client privileged information	10%
Total	500%

Q40. 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.	Pct%
Attorney-client privileged information	50%
Financial information	49%
Trade secrets	45%
Research results	41%
Source code	39%
Consumer data	28%
Company-confidential information	24%
Analytics	24%
Operational information	21%
Presentations	19%
Product/market information	19%
Business correspondence	18%
Private communications (i.e., emails, texting, social media)	16%

Q41. In the normal course of business, who has access to your company's knowledge assets?	Pct%
Only privileged users	17%
Privileged users plus a small number or ordinary users	33%
Both privileged and ordinary users	50%
Total	100%

Q42a. Do third parties have access to your company's knowledge assets?	Pct%
Yes	57%
No	29%
Unsure	14%
Total	100%

Q42b. If yes, how does your company ensure knowledge assets shared with third parties are appropriately protected?	Pct%
Contract with indemnification by the third party	50%
Encryption of data in motion	44%
Encryption or tokenization of data at rest	40%
Careful vetting of the third party	33%
Proof that the third party meets generally accepted security requirements	31%
Proof that the third party adheres to compliance mandates	25%
Site visit and assessment of the third party	22%
None of the above	39%
Total	284%

Q43. Approximately, how much was the total cost due to attacks against knowledge assets over the past 12 months?	Pct%
Zero	5%
Less than $50,000	2%
50,001 to $100,000	5%
100,001 to $250,000	7%
250,001 to $500,000	15%
500,001 to $1,000,000	15%
1,000,001 to $5,000,000	20%
5,000,001 to $10,000,000	14%
10,000,001 to $25,000,000	12%
More than $25,000,000	5%
Total	100%
Extrapolated value	$5,435,650

Q44. To understand the relationship of each of the five categories to the total cost of attacks against knowledge assets, please allocate points to each category for a total of 100 points.	Points
Remediation & technical support activities	14
Users' idle time and lost productivity because of downtime or system performance delays	12
Disruption to normal operations	21
Damage or theft of IT assets and infrastructure	9
Reputation loss and brand damage	44
Total points	100

Q45. What is the likelihood of a material data breach involving your company's knowledge assets sometime in the next 12 months?	Pct%
Less than 1%	4%
1 to 5%	14%
6 to 10%	17%
11 to 15%	18%
16 to 20%	25%
21 to 25%	14%
26 to 50%	7%
More than 50%	1%
Total	100%
Extrapolated value	15.1%

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

Q47a. Does your company have data breach (cyber) insurance?	Pct%
Yes	29%
No, but plan to with the next 12 months	31%
No	40%
Total	100%

Q47b. If yes, in percentage terms, how much of the loss resulting from the theft of knowledge assets is covered?	Pct%
Zero	0%
Less than 10%	21%
10 to 25%	24%
26 to 50%	29%
51 to 75%	19%
76 to 100%	7%
Total	100%
Extrapolated value	35.0%

Part 4. Organizational Characteristics & Demographics

D1. What organizational level best describes your current position?	Pct%
Senior Executive	2%
Vice President	3%
Director	17%
Manager	20%
Supervisor	15%
Technician	33%
Staff	8%
Contractor	2%
Total	100%

D2. Check the **Primary Person** you or your leader reports to within the organization.	Pct%
CEO/COO	2%
Chief Financial Officer (CFO)	2%
General Counsel (GC)	5%
Chief Information Officer (CIO)	53%
Chief Information Security Officer (CISO)	18%
Chief Compliance Officer (CCO)	10%
Head of Human Resources	0%
Chief Security Officer (CSO)	2%
Chief Risk Officer (CRO)	8%
Total	100%

D3. What industry best describes your organization’s **primary** industry classification?	Pct%
Agriculture & food services	1%
Communications	3%
Consumer products	5%
Education & research	2%
Energy & utilities	6%
Entertainment & media	2%
Financial services	19%
Health & pharmaceutical	11%
Hospitality	4%
Industrial & manufacturing	10%
Public sector	12%
Retail	9%
Services	9%
Technology & software	5%
Transportation	2%
Total	100%

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

D5. What is the worldwide headcount of your organization?	Pct%
Less than 500	10%
500 to 1,000	21%
1,001 to 5,000	29%
5,001 to 25,000	20%
25,001 to 75,000	12%
More than 75,000	8%
Total	100%

Please contact research@ponemon.org or call us at 800.877.3118 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.