



2017 Global Cyber Risk Transfer Comparison Report

Sponsored by Aon Risk Solutions

Independently conducted by Ponemon Institute LLC

Publication Date: April 2017



2017 Global Cyber Risk Transfer Comparison Report

Sponsored by Aon Risk Solutions
Independently Conducted by Ponemon Institute LLC
Publication Date: April 2017

Part 1. Introduction

The purpose of this research is to compare the relative insurance protection of certain tangible¹ versus intangible² assets. How do cyber asset values and potential losses compare to tangible asset values and potential losses from an organization's other perils, such as fires and weather?

The probability of any particular building burning down is significantly lower than one percent (1 percent). However, most organizations spend much more on fire-insurance premiums than on cyber insurance despite stating in their publicly disclosed documents that a majority of the organization's value is attributed to intangible assets.³ One recent concrete example is the sale of Yahoo!: Verizon recently reduced the purchase price by \$350 million because of the severity of cyber incidents in 2013 and 2014.

Acceleration in the scope, scale and economic impact of technology multiplied by the concomitant data revolution, which places unprecedented amounts of information in the hands of consumers and businesses alike, and the proliferation of technology-enabled business models,⁴ force organizations to examine the benefits and consequences of emerging technologies.⁵

This financial-statement quantification study demonstrates that organizations recognize the growing value of technology and data assets relative to historical tangible assets, yet a disconnect remains regarding cost-benefit analysis resource allocation. Particularly, a disproportionate amount is spent on tangible asset insurance protection compared to cyber asset protection⁶ based on their respective relative financial statement impact and potential expected losses.⁷

Quantitative models are being developed that evaluate the return on investment of various cyber risk management IT security and process solutions, which can incorporate cost-benefit analysis for different levels of insurance.⁸ As such, organizations are driven toward a holistic capital expenditure discussion spanning functional teams rather than being segmented in traditional siloes. The goal is to identify and protect critical assets by aligning macro-level risk tolerance in a more consistent manner.

¹ Property, Plant & Equipment ("PP&E")

² Computer systems and related digital assets. Most other cyber incident studies include damage estimates of subjective intangible assets that are difficult to quantify and almost impossible to insure, such as brand and reputation. Furthermore, the value of trade secrets and patent infringement are typically excluded from cyber insurance, although there are new models being developed to quantify intangible intellectual property values, which could eventually lead to viable insurance in the near future.

³ [More than 80% of a company's value is derived from intangible assets](#) according to some studies.

⁴ [No Ordinary Disruption: The Four Global Forces Breaking All the Trends](#). McKinsey Global Institute.

⁵ [World Economic Forum Global Risks Perception Survey](#)

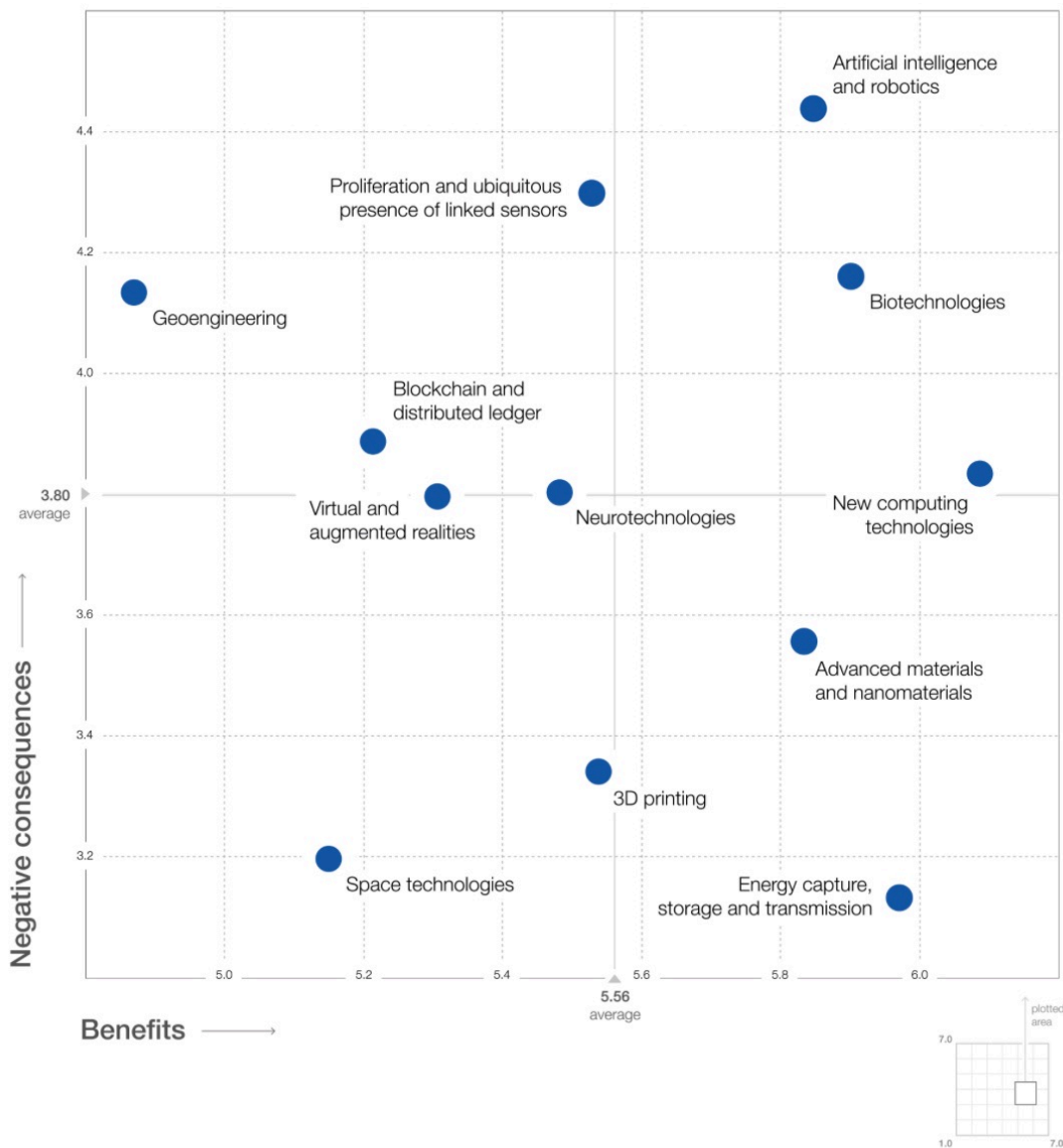
⁶ Aon has placed primary cyber insurance with 67 different insurance carriers, which means 67 different insurance applications, underwriting processes, policy form wording, servicing capabilities and claims payment aptitude.

⁷ Unfortunately, it is not a binary discussion because property, general liability, crime, kidnap & ransom and other lines of insurance may intentionally or unintentionally include elements of cyber coverage.

⁸ [A 2016 Rand Study](#) found contrary results: "Cost of Cyber Incidents Not Large Compared with Other Business Losses; May Influence Responses by Businesses"

An interesting perspective on the perceived benefits and negative consequences of 12 emerging technologies is the *Global Risks Report* published by the World Economic Forum (WEF), as shown in Figure 1. This year, the WEF's Global Risks Perception Survey considered the impact of 12 emerging technologies.⁹ While the results suggest that the benefits of these technologies outweigh the negative consequences, there is a need for better governance of emerging technologies.

Figure 1. Examining the risk: Benefit analysis of intangible & intangible assets



⁹ [World Economic Forum Global Risks Perception Survey](http://reports.weforum.org/global-risks-2017/part-3-emerging-technologies/3-1-understanding-the-risk-landscape/)
<http://reports.weforum.org/global-risks-2017/part-3-emerging-technologies/3-1-understanding-the-risk-landscape/>

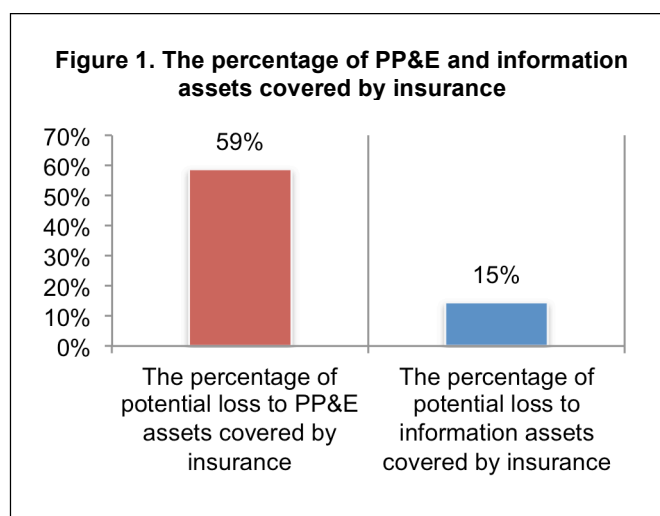
How do organizations qualify and quantify the corresponding impact of financial statement exposure? Our goal is to compare the financial statement impact of tangible property and network risk exposures. A better understanding of the relative financial statement impact will assist organizations in allocating resources and determining the appropriate amount of risk transfer (insurance) resources to allocate to the mitigation of the financial statement impact of network risk exposures.

Network risk exposures can broadly include breach of privacy and security of personally identifiable information, stealing an organization's intellectual property, confiscating online bank accounts, creating and distributing viruses on computers, posting confidential business information on the Internet, robotic malfunctions and disrupting a country's critical national infrastructure.¹⁰

We surveyed 2,168 individuals in North America, Europe, the Middle East, Africa, Asia Pacific, Japan and Latin America¹¹ who are involved in their company's cyber risk management as well as enterprise risk management activities. Most respondents are either in finance, treasury and accounting (32 percent of respondents) or risk management (26 percent of respondents). Other respondents are in corporate compliance/audit (14 percent of respondents) and general management (12 percent of respondents).

All respondents are familiar with the cyber risks facing their company. In the context of this research, cyber risk means any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems.¹²

As shown in Figure 1, despite the greater average potential loss to information assets (\$979 million) compared to property, plant & equipment ("PP&E") (\$770 million), the latter has much higher insurance coverage (59 percent vs. 15 percent).



Following are some of the key takeaways from this research:

- Information assets are underinsured against theft or destruction based on the value, probable maximum loss (PML) and likelihood of an incident.
- Disclosure of a material loss of PP&E and disclosure of information assets differ. Forty-three percent of respondents say their company would disclose the loss of PP&E in its financial statements as a footnote disclosure. However, 36 percent of respondents say a material loss to information assets does not require disclosure.

¹⁰ Even though some network risks, also known as cyber risks, are not yet fully insurable via traditional insurance markets (e.g. the **value** of trade secrets) and other cyber risks may be insurable under legacy policies (e.g. property, general liability, crime, etc.), it is useful to understand the relative risks in terms of enterprise management financial statement impact.

¹¹ Countries included in this report are Canada and the United States

¹² Source: Institute of Risk Management

- Despite the risk, companies are reluctant to purchase cyber insurance coverage. Sixty-four percent of respondents believe their company's exposure to cyber risk will increase over the next 24 months. However, only 24 percent of respondents say their company has cyber insurance coverage.
- Most companies in this study experienced a material or significantly disruptive security exploit or data breach one or more times during the past two years, and the average economic impact was \$3.6 million.
- Eighty-seven percent of respondents believe cyber liability is in the top 10 business risks for their company.

Part 2. Key findings

The complete audited findings are presented in the appendix of this report. We have organized the report according to the following topics:

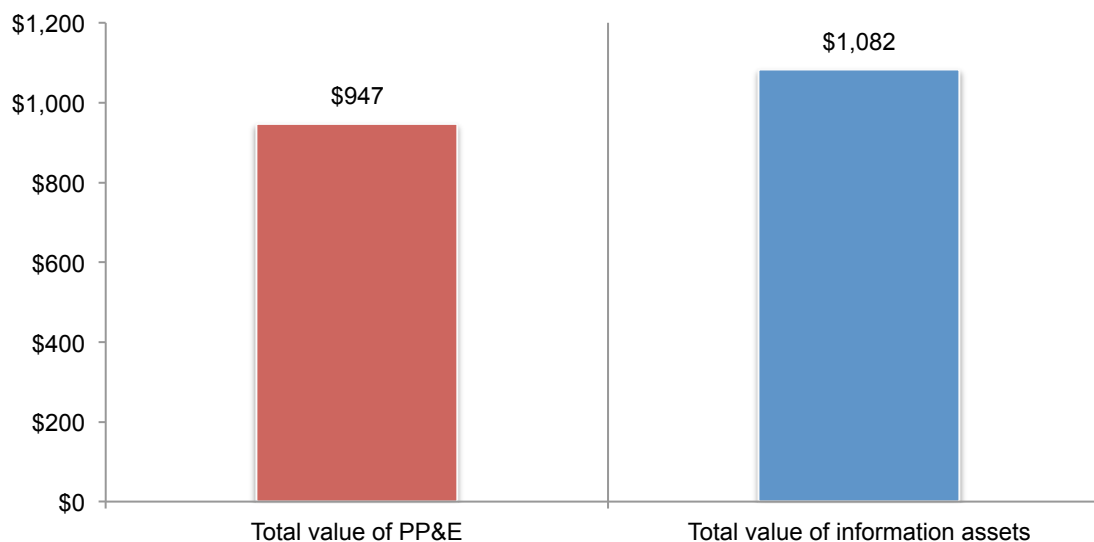
- Differences between the valuation and PML of PP&E and information assets
- The cyber risk experience of companies
- Perceptions about the financial impact of cyber exposures

Differences between the valuation and PML of PP&E and information assets

Companies value information assets slightly higher than they do PP&E¹³. According to Figure 2, on average, the total value of PP&E, including all fixed assets plus SCADA and industrial control systems is approximately \$947 million for the companies represented in this research. The average total value of information assets, which includes customer records, employee records, financial reports, analytical data, source code, models methods and other intellectual properties, is slightly more than PP&E at \$1,082 million.

Figure 2. The total value of PP&E and information assets

Extrapolated value (\$ millions)



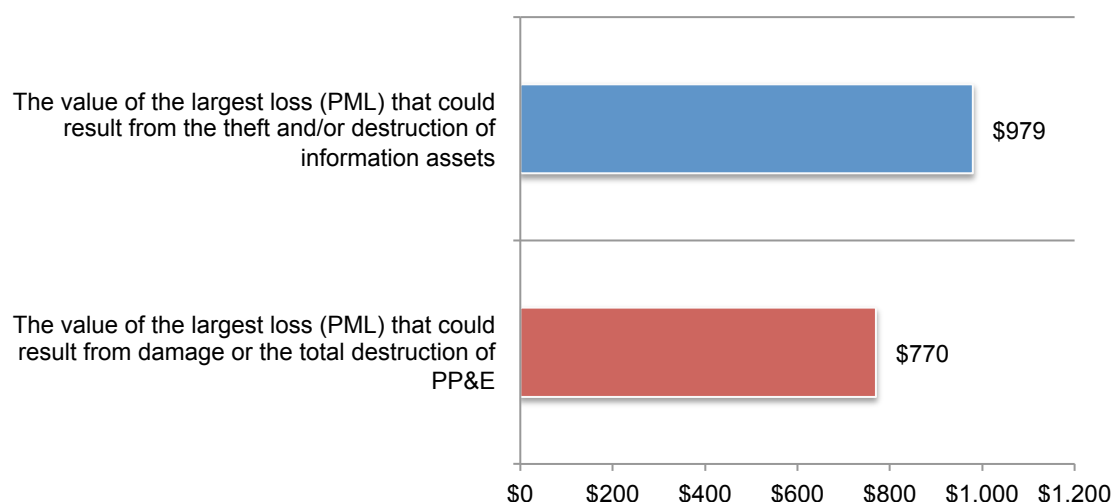
¹³ Respondents were asked to assume, with respect to PP&E assets, the root causes of loss (a.k.a. perils) include fire, flooding, weather events, earthquakes and other natural or man-made disasters.

The value of PML¹⁴ is higher for information assets than for PP&E. Companies estimate the PML if information assets are stolen or destroyed at an average of approximately \$979 million, according to Figure 3. This assumes the normal functioning of passive protective cybersecurity solutions such as perimeter controls, data loss prevention tools, data encryption, identity and access management systems and more.

In contrast, the value of the largest loss that could result from damage or total destruction of PP&E is approximately \$770 million on average. This also assumes the normal functioning of passive protective features such as firewalls, nonflammable materials, proper functioning of active suppression systems, fire sprinklers, raised flooring and more.

Figure 3. The PML value for PP&E and information assets

Extrapolated value (\$ millions)



¹⁴ Probable Maximum Loss (PML) is defined as the value of the largest loss that could result from a disaster, assuming the normal functioning of passive protective features (i.e., firewalls, nonflammable materials, etc.) and proper functioning of most (perhaps not all) active suppression systems (i.e., sprinklers).

What is the impact of business disruption to PP&E and information asset losses?

According to Figure 4, business disruption has a greater impact on information assets (\$266 million)¹⁵ than on PP&E (\$130 million).

Figure 4. The impact of business disruption to information assets and PP&E

Extrapolated value (\$ millions)

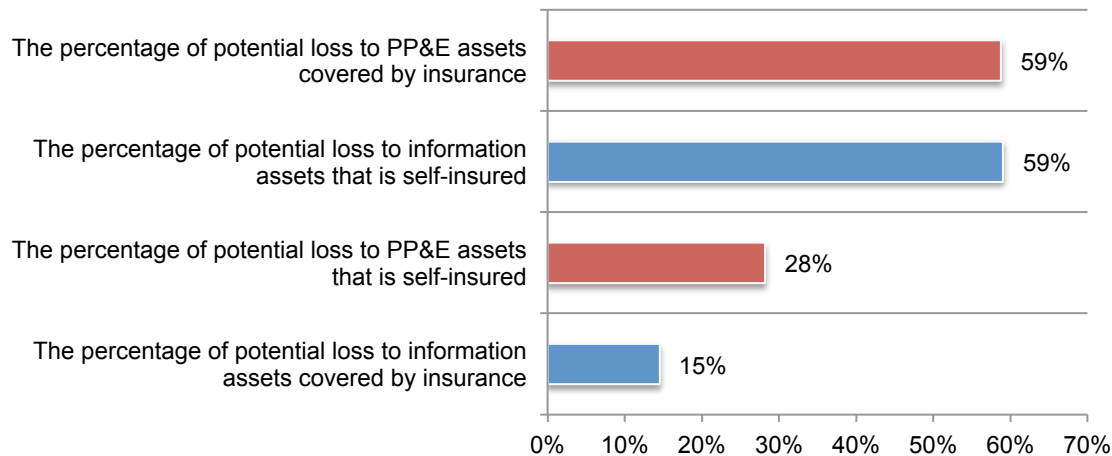


¹⁵ While the survey results suggest Probably Maximum Loss in the neighborhood of \$256 million, a growing number of companies are using Risk Decision Platform Analysis and Cyber Modeling to suggest potential losses in excess of \$500 million to over \$1 billion and seek cyber insurance limit premium quotes and policy terms for such amounts.

There is a significant difference between the insurance coverage of PP&E and information assets. On average, approximately 59 percent of PP&E assets are covered by insurance and approximately 28 percent of PP&E assets are self-insured (Figure 5)¹⁶. Only an average of 15 percent of information assets are covered by insurance. Self-insurance is higher for information assets at 59 percent.

Figure 5. Percentage of PP&E and information assets covered by insurance

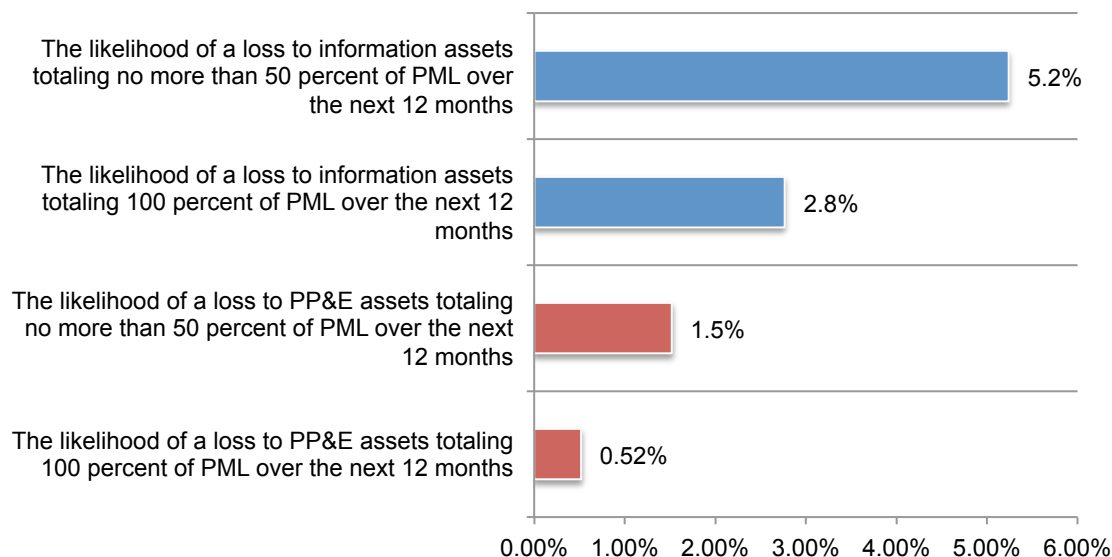
Extrapolated percentage



The likelihood of a loss is higher for information assets than for PP&E. Companies estimate the likelihood that they will sustain a loss to information assets totaling no more than 50 percent of PML over the next 12 months at 5.2 percent and 100 percent of PML at 2.8 percent, as shown in Figure 6. The likelihood of a loss to PP&E totaling no more than 50 percent of PML over the next 12 months is an average of 1.5 percent and at 100 percent of PML it is 0.52 percent.

Figure 6. Likelihood of loss to PP&E and information assets totaling more than 50 percent and 100 percent of PML over the next 12 months

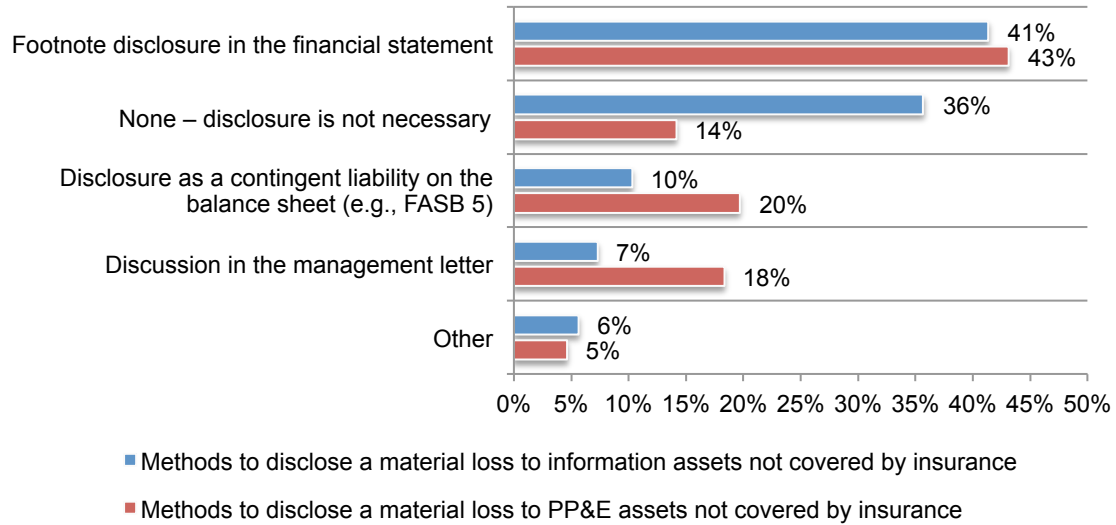
Extrapolated percentage



¹⁶ The percentages do not add up to 100 percent because they are extrapolated values from questions 3,4,10 and 11. These results are shown in the complete audited findings in the appendix of the report.

Disclosure of material loss to PP&E and disclosure of material loss to information assets also differs. Figure 7 focuses on how companies would disclose a material loss. Forty-three percent of respondents say their company would disclose a material loss to PP&E assets that is not covered by insurance in its financial statements as a footnote disclosure in the financial statement, followed by a disclosure as a contingent liability on the balance sheet, such as FASB 5, (20 percent of respondents). Forty-one percent say they would disclose a material loss to information assets as a footnote disclosure in the financial statements but 36 percent of respondents do not believe disclosure is necessary.

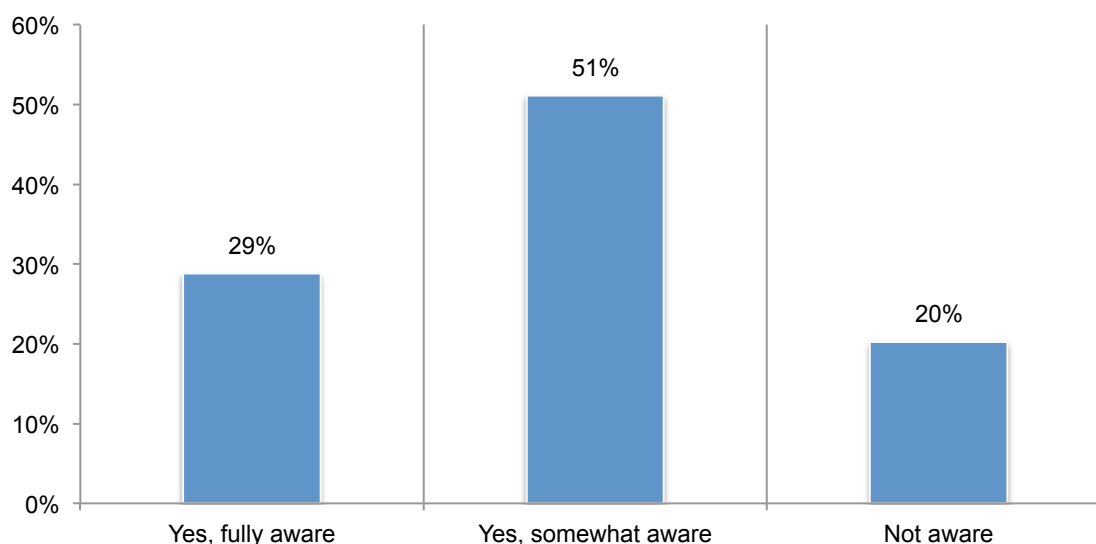
Figure 7. How would your company disclose a material loss to PP&E and information assets?



The cyber risk experience of companies

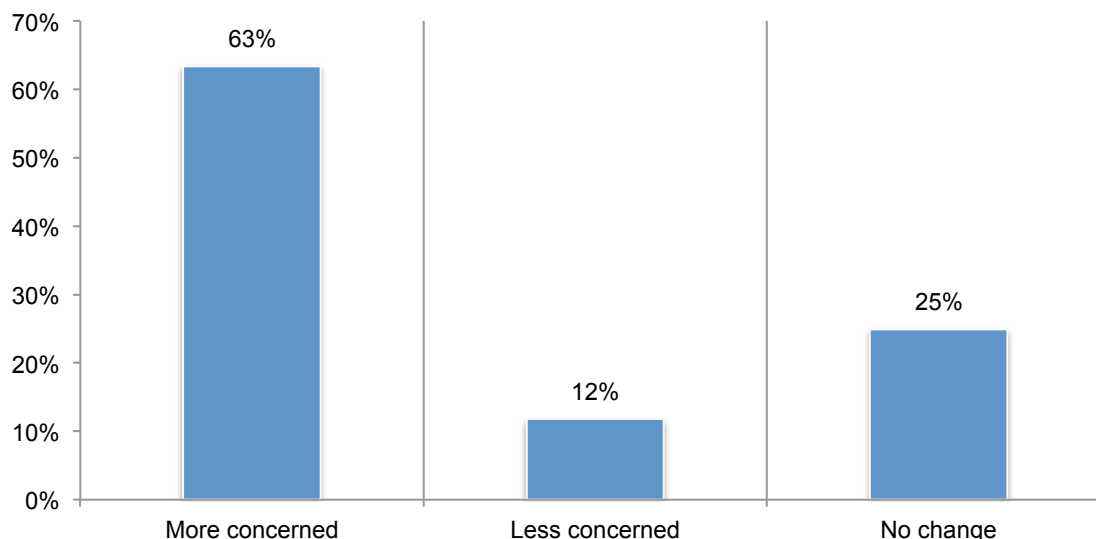
Awareness of the economic and legal consequences from an international data breach or security exploit is low. As revealed in Figure 8, only 29 percent of respondents are fully aware of the consequences that could result from a data breach or security exploit in other countries in which their company operates and 20 percent say they are not aware of the consequences.

Figure 8. Awareness of the economic and legal consequences from an international data breach or security exploit



The majority of companies had a material¹⁷ or significantly disruptive security exploit or data breach one or more times in the past 24 months. Forty-six percent of respondents report their company had such a security incident. The average total financial impact of these incidents was \$3.6 million.¹⁸ According to Figure 9, 63 percent of these respondents say the incident increased their company's concerns over cyber liability.

Figure 9. How did the security exploit or data breach affect your company's concerns over cyber liability?



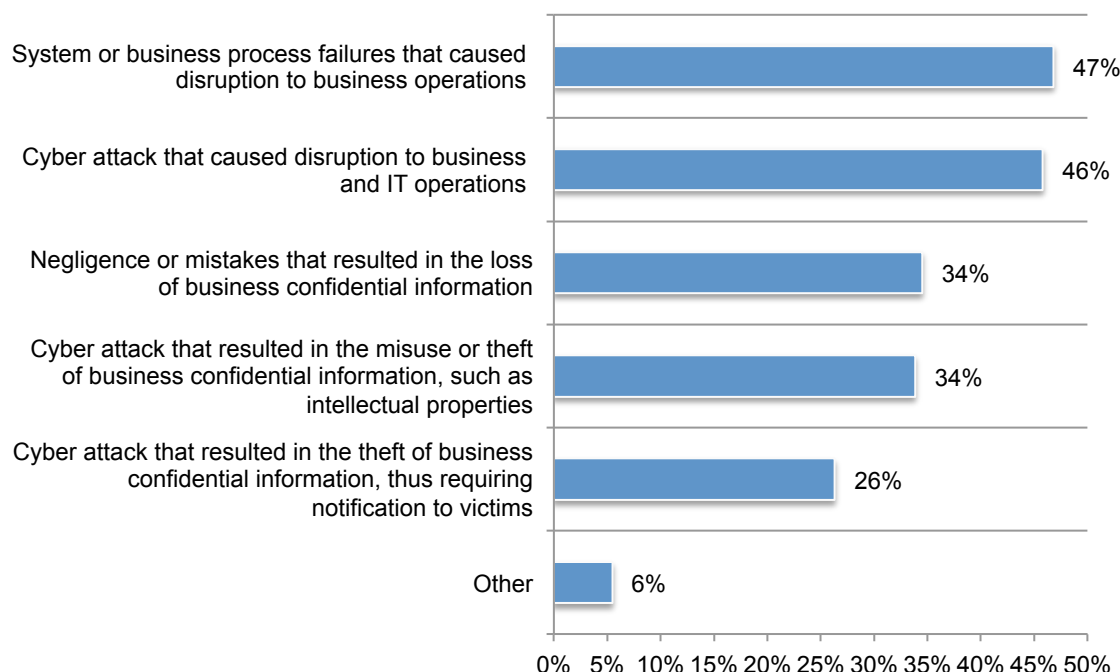
¹⁷ In the context of this study, the term materiality takes into consideration monies expended for first-party losses, potential third-party liabilities, value of lost time, litigation costs, reputation damages and revenue losses. This term is broader than materiality as defined by GAAP and SEC requirements.

¹⁸ This included all costs, including out-of-pocket expenditures such as consultant and legal fees, indirect business costs such as productivity losses, diminished revenues, legal actions, customer turnover and reputation damages.

The types of security incident that 46 percent of the companies in this research faced are displayed in Figure 10. The most frequent type of incident was a system or business process failure that caused disruption to business operations, such as software updates (47 percent of respondents) or a cyber attack that caused disruption to business and IT operations, such as denial of service attacks (46 percent of respondents). This is followed by 34 percent of respondents who say it is a cyber attack that resulted in the misuse or theft of business confidential information, such as intellectual properties, or negligence or mistakes that resulted in the loss of business confidential information.

Figure 11. What type of data breach or security exploit did your company experience?

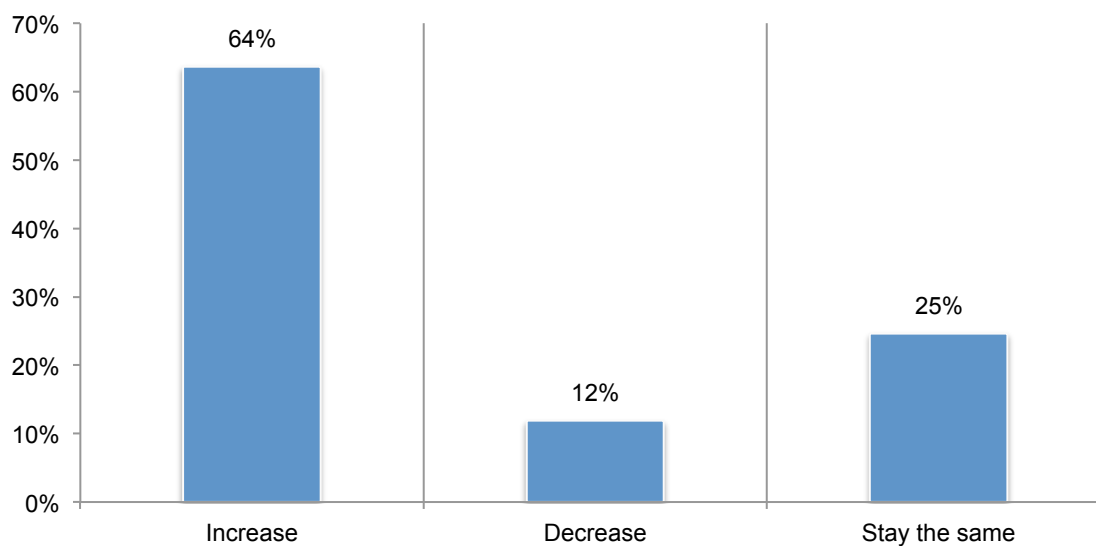
More than one response allowed



Perceptions about the financial impact of cyber exposures

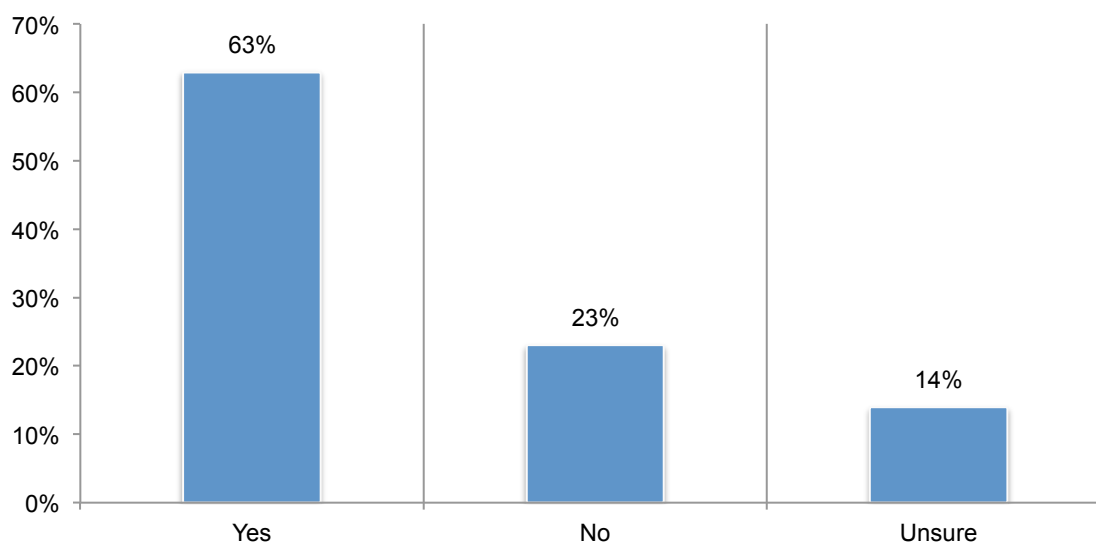
Companies' exposure to cyber risk is expected to increase, yet almost half (43 percent of respondents) say there is no plan to purchase cyber insurance. As the data in Figure 11 show, 64 percent of respondents believe their company's exposure to cyber risk will increase and 25 percent of respondents say it will stay the same. Only 12 percent of respondents expect it to actually decrease.

Figure 11. Will your company's cyber risk exposure increase, decrease or stay the same over the next 24 months?



Despite the extent of cyber risk, which exceeds that of PP&E risk, only 30 percent of respondents say their companies currently have cyber insurance coverage with an average limit of \$15 million. As Figure 12 reveals, 63 percent of respondents believe this insurance is sufficient with respect to coverage terms and conditions, exclusions, retentions, limits and insurance carrier financial security.

Figure 12. Is your company's cyber insurance coverage sufficient?



According to Figure 13, the adequacy of coverage is determined mainly by policy terms and conditions reviewed by a third-party specialist (22 percent of respondents) or a formal risk assessment by a third-party (22 percent of respondents). Only 13 percent say it was determined by a formal risk assessment conducted by the insurer, and 13 percent say it was a formal risk assessment by in-house staff.

Figure 13. How companies determine the adequacy of coverage

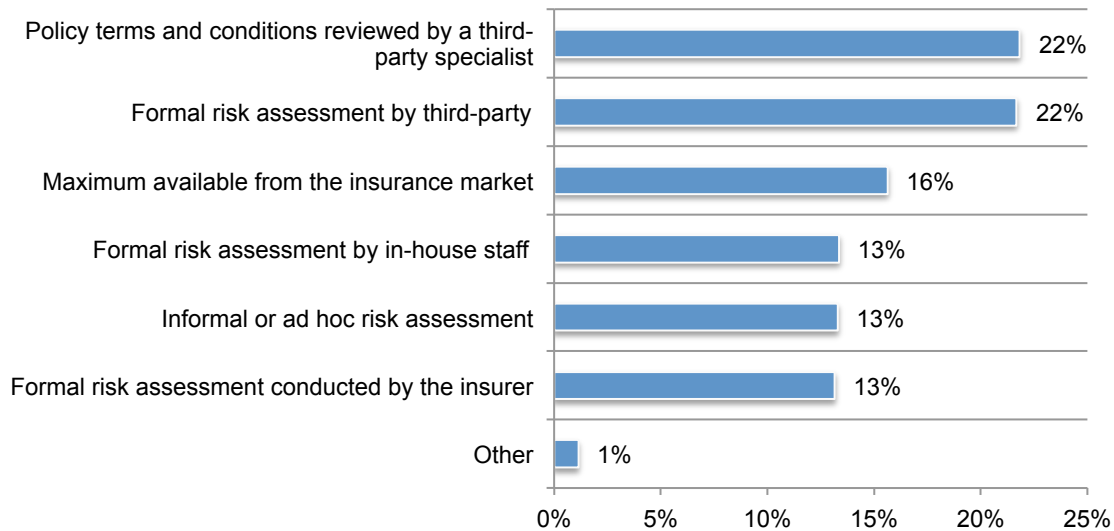


Figure 14 displays the incidents typically covered by cyber insurance. Most incidents covered are external attacks by cyber criminals (86 percent of respondents), malicious or criminal insiders (84 percent of respondents), and system or business process failures (43 percent of respondents).

Figure 14. Types of incidents covered by cyber insurance

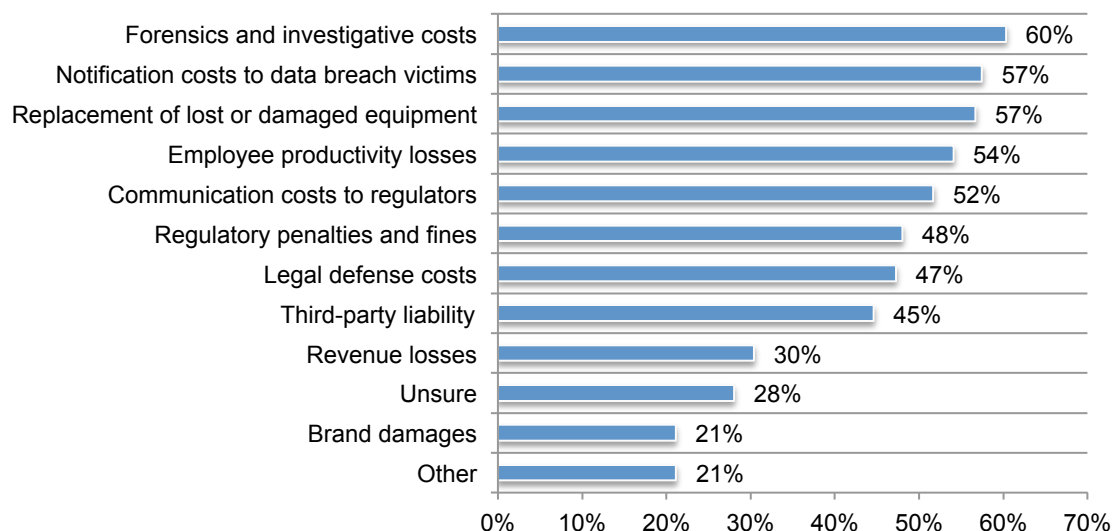
More than one response allowed



Figures 15 and 16 present the coverage and services provided by insurance companies. The top five costs covered are: forensics and investigative costs (60 percent of respondents), data breach notification costs (57 percent of respondents), replacement of lost or damaged equipment (57 percent of respondents), employee productivity losses (54 percent of respondents) and communication costs to regulators (52 percent of respondents).

Figure 15. Coverage provided by the insurance company

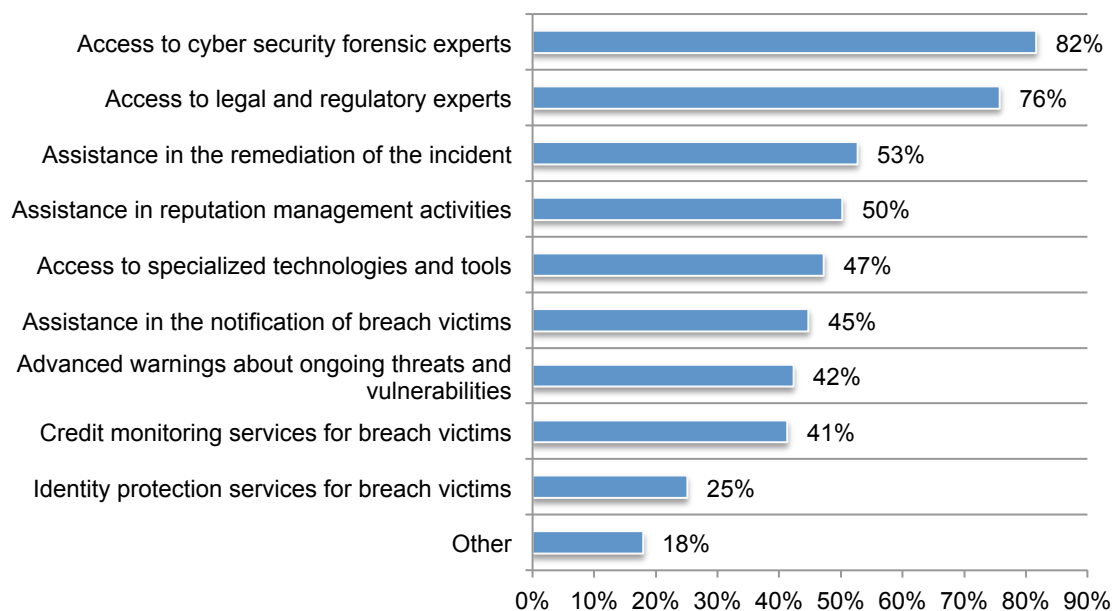
More than one response allowed



In addition to this coverage, other services provided are access to cybersecurity forensic experts (82 percent of respondents), access to legal and regulatory experts (76 percent of respondents), assistance in the remediation of the incident (53 percent of respondents), assistance in reputation management activities (50 percent of respondents) and access to specialized technologies and tools (47 percent of respondents), as shown in Figure 16.

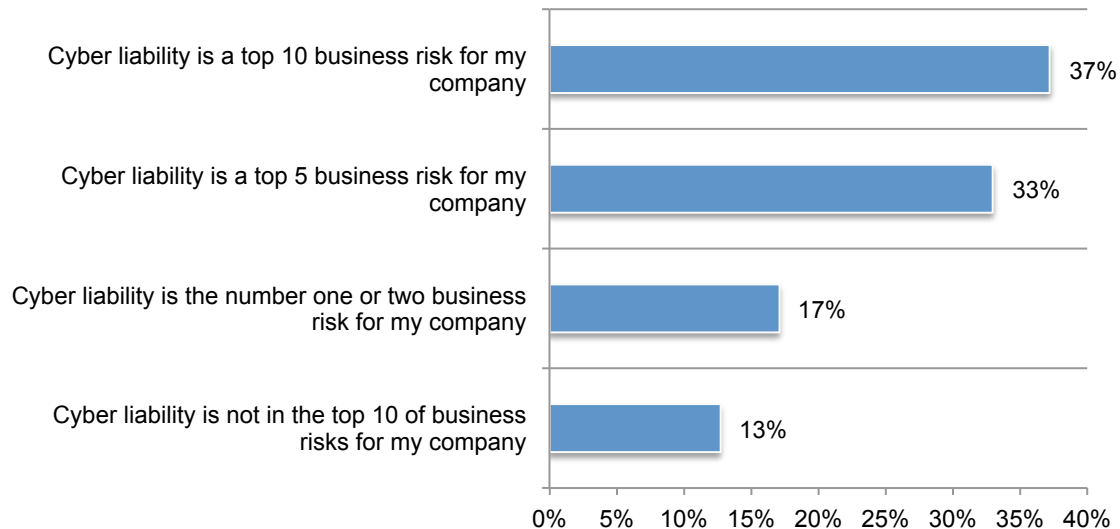
Figure 16. Other services provided by the cyber insurer

More than one response allowed



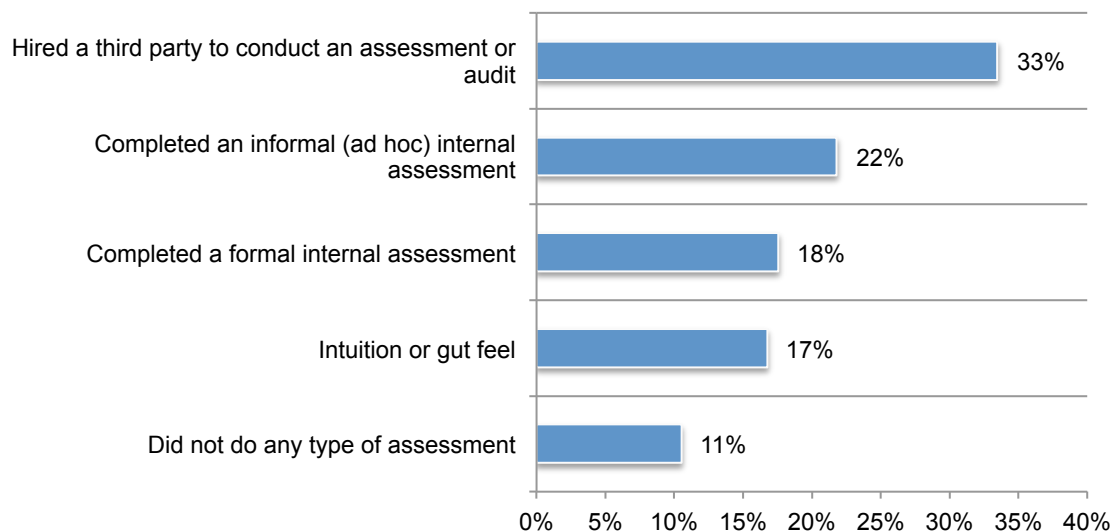
Cyber liability ranks in the top 10 of all business risks facing companies. Figure 17 demonstrates that 87 percent of respondents consider a cyber risk as the number one or two business risk (17 percent of respondents), in the top five (33 percent of respondents) and in the top 10 (37 percent). Only 11 percent of respondents believe it is not in the top 10 of all business risks facing their companies.

Figure 17. How do cyber risks compare to other business risks?



To determine the cyber risk to their company, 33 percent of respondents say the company hired a third-party to conduct an assessment or audit and 22 percent of respondents say it was an informal (ad hoc) internal assessment (Figure 18). Only 18 percent of respondents say their company completed a formal internal assessment, but 17 percent of respondents say it was intuition or gut feel.

Figure 18. How did you determine the level of cyber risk to your company?

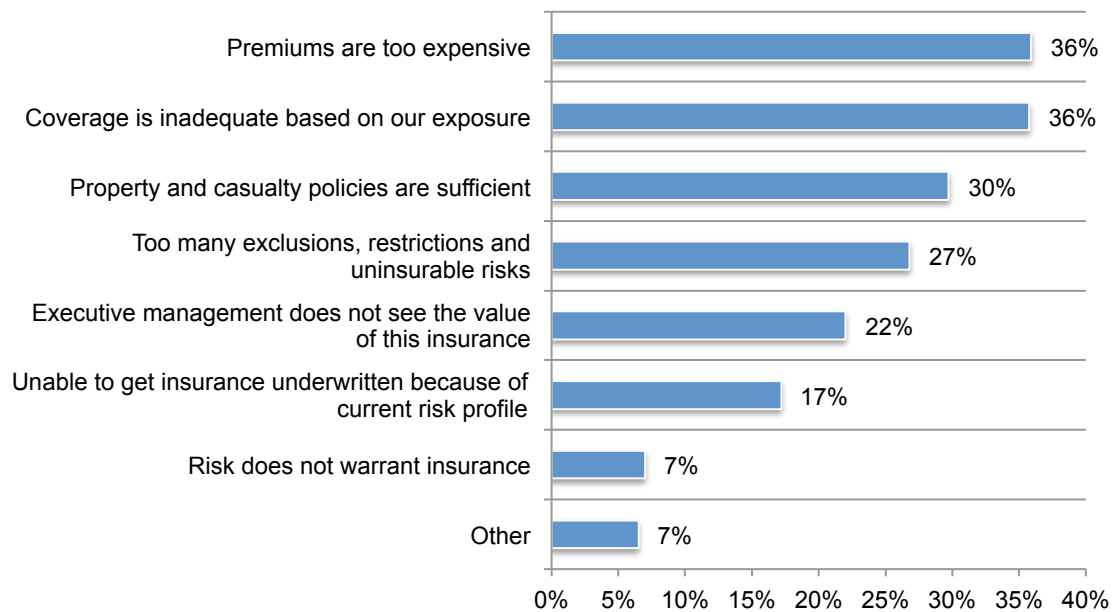


Will the purchase of cyber insurance increase because of concerns about security exploits and data breaches? Fourteen percent of respondents say their company will purchase cyber insurance in the next 12 months, 24 percent of respondents say they will in two years and 18 percent of respondents say they will in more than two years.

According to Figure 19, the main reasons for not purchasing cyber security insurance are: premiums are too expensive (36 percent of respondents), coverage is inadequate based on their exposure (36 percent of respondents), property and casualty policies are sufficient (30 percent of respondents) and there are too many exclusions, restrictions and uninsurable risks (27 percent of respondents).

Figure 19. What are the main reasons why your company will not purchase cyber security insurance?

More than one response allowed



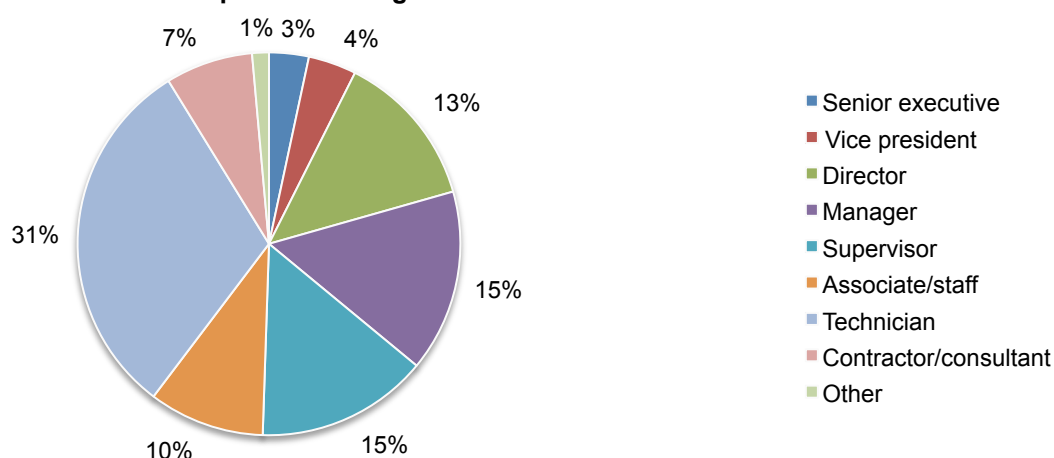
Part 3. Methods

The consolidated sampling frame is composed of 60,220 individuals located in North America, Europe, the Middle East, Africa, Asia Pacific, Japan and Latin America. Respondents are involved in their company's cyber risk and enterprise risk management activities. As Table 1 shows, 2,465 respondents completed the survey, of which 297 were rejected for reliability issues. The final sample consisted of 2,168 surveys (a 3.6 percent response rate).

Table 1. Sample response	Freq	Pct%
Total sampling frame	60,220	100.0%
Total returns	2,465	4.1%
Rejected or screened surveys	297	0.5%
Final sample	2,168	3.6%

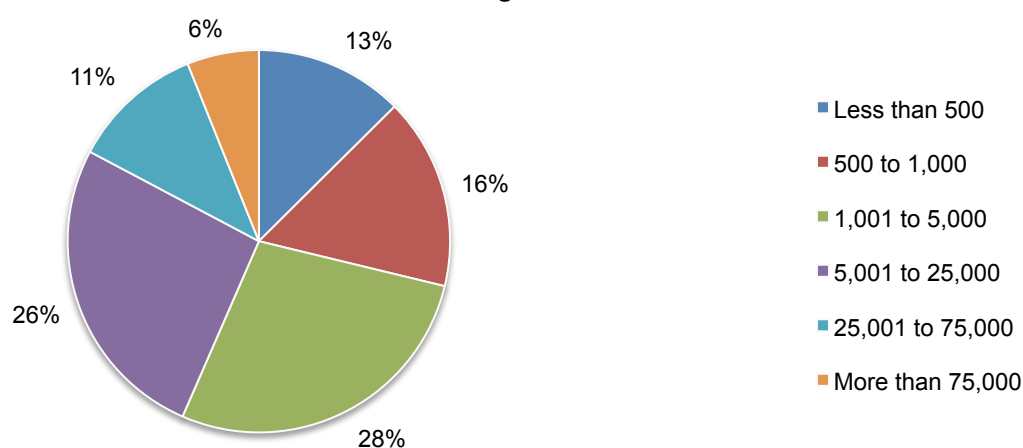
Pie Chart 1 reports the current position or organizational level of the respondents. Half of the respondents (50 percent) reported their current position as supervisory level or above.

Pie Chart 1. Current position or organizational level



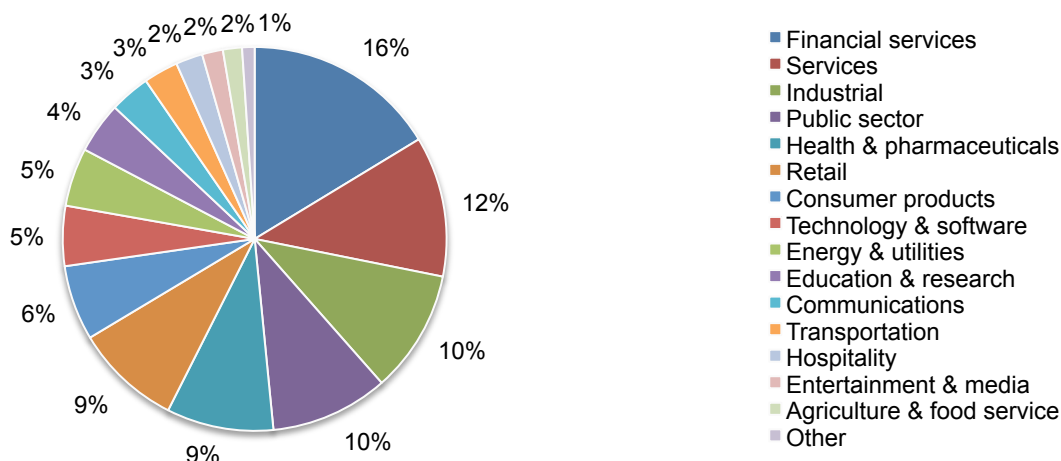
As Pie Chart 2 reveals, 71 percent of the respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 2. Worldwide headcount of the organization



Pie Chart 3 reports the primary industry classification of respondents' organizations. This chart identifies financial services (16 percent of respondents) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by services (12 percent of respondents) and industrial (10 percent of respondents).

Pie Chart 3. Primary industry focus



Part 4. Caveats

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

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

Sampling frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are involved in their company's cyber and enterprise risk management. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period.

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

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured December 2016 through February 2017.

Survey response	Global
Sampling frame	60,220
Total returns	2,465
Final sample	2,168
Response rate	3.6%
Sample weights	100.0%

Screening questions

S1. How familiar are you with cyber risks facing your company today?	Global
Very familiar	20%
Familiar	36%
Somewhat familiar	44%
Not familiar (stop)	0%
Total	100%

S2. Are you involved in your company's cyber risk management activities?	Global
Yes, significant involvement	32%
Yes, some involvement	68%
No involvement (stop)	0%
Total	100%

S3. Are you involved in your company's enterprise risk management activities?	Global
Yes, significant involvement	37%
Yes, some involvement	63%
No involvement (stop)	0%
Total	100%

S4. What best defines your role?	Global
Risk management	26%
Finance, treasury & accounting	32%
Corporate compliance/audit	14%
Security/information security	10%
General management	12%
Legal (OGC)	7%
None of the above (stop)	0%
Total	100%

The following questions pertain to your company's property, plant and equipment (PP&E)

Part 1. Sizing the economic impact

Q1. What is the total value of your company's PP&E, including all fixed assets plus SCADA and industrial control systems? Please exclude and assume a value based on full replacement cost (and not historic cost).	Global
Less than \$1 million	4%
\$1 to 10 million	11%
\$11 to 50 million	15%
\$51 to 100 million	27%
\$101 to 500 million	22%
\$501 to 1 billion	12%
\$1 to 10 billion	5%
More than \$10 billion	5%
Total	100%
Extrapolated value	946.74

Q2a. What is the value of the largest loss (PML) that could result from damage or the total destruction of PP&E. Please assume the normal functioning of passive protective features – such as firewalls, nonflammable materials, proper functioning of active suppression systems, fire sprinklers, raised flooring and more.	Global
Less than \$1 million	5%
\$1 to 10 million	12%
\$11 to 50 million	18%
\$51 to 100 million	27%
\$101 to 500 million	21%
\$501 to 1 billion	9%
\$1 to 10 billion	7%
More than \$10 billion	3%
Total	100%
Extrapolated value	769.87

Q2b. What is the value of your largest loss (PML) due to business interruption? Please assume the normal functioning of passive protective features – such as firewalls, nonflammable materials, proper functioning of active suppression systems, fire sprinklers, raised flooring and more.	Global
Less than \$1 million	15%
\$1 to 10 million	26%
\$11 to 50 million	26%
\$51 to 100 million	20%
\$101 to 500 million	9%
\$501 to 1 billion	2%
\$1 to 10 billion	1%
More than \$10 billion	0%
Total	100%
Extrapolated value	129.50

Q3. What percentage of this potential loss to PP&E assets is covered by insurance, including captives reinsured but not including captives not reinsured?	Global
Less than 5%	1%
5% to 10%	2%
11% to 20%	5%
21% to 30%	6%
31% to 40%	9%
41% to 50%	10%
51% to 60%	19%
61% to 70%	14%
71% to 80%	15%
81% to 90%	12%
91% to 100%	9%
Total	100%
Extrapolated value	59%

Q4. What percentage of this potential loss to PP&E assets is self-insured, including captives not reinsured?	Global
Less than 5%	12%
5% to 10%	14%
11% to 20%	16%
21% to 30%	18%
31% to 40%	13%
41% to 50%	12%
51% to 60%	6%
61% to 70%	7%
71% to 80%	2%
81% to 90%	0%
91% to 100%	0%
Total	100%
Extrapolated value	28%

Q5. What is the likelihood that your company will sustain a loss to PP&E assets totaling no more than 50 percent of PML over the next 12 months?	Global
Less than 0.1%	22%
0.1% to 0.5%	17%
0.6% to 1.0%	17%
1.1% to 2.0%	13%
2.1% to 3.0%	17%
3.1% to 4.0%	7%
4.1% to 5.0%	5%
5.1% to 10.0%	1%
More than 10.0%	1%
Total	100%
Extrapolated value	1.5%

Q6. What is the likelihood that your company will sustain a loss to PP&E assets totaling 100 percent of PML over the next 12 months?	Global
Less than 0.1%	67%
0.1% to 0.5%	14%
0.6% to 1.0%	9%
1.1% to 2.0%	5%
2.1% to 3.0%	2%
3.1% to 4.0%	2%
4.1% to 5.0%	1%
5.1% to 10.0%	1%
More than 10.0%	0%
Total	100%
Extrapolated value	0.52%

Q7. In your opinion, how would your company disclose a material loss to PP&E assets that is not covered by insurance in its financial statements?	Global
Disclosure as a contingent liability on the balance sheet (e.g., FASB 5)	20%
Footnote disclosure in the financial statements	43%
Discussion in the management letter	18%
None – disclosure is not necessary	14%
Other	5%
Total	100%

The following questions pertain to your company's information assets.

Q8. What is the total value of your company's information assets, including customer records, employee records, financial reports, analytical data, source code, models, methods and other intellectual properties? Please assume a value based on full replacement cost (and not historic cost). Please note this value can be a precise quantification or estimate.	Global
Less than \$1 million	5%
\$1 to 10 million	9%
\$11 to 50 million	14%
\$51 to 100 million	27%
\$101 to 500 million	20%
\$501 to 1 billion	13%
\$1 to 10 billion	7%
More than \$10 billion	5%
Total	100%
Extrapolated value	1,082.46

Q9a. What is the value of the largest loss (PML) that could result from the theft and/or destruction of information assets. Please assume the normal functioning of passive protective cybersecurity features – such as perimeter controls, data loss prevention tools, data encryption, identity and access management systems and more.	Global
Less than \$1 million	9%
\$1 to 10 million	14%
\$11 to 50 million	14%
\$51 to 100 million	23%
\$101 to 500 million	16%
\$501 to 1 billion	13%
\$1 to 10 billion	8%
More than \$10 billion	4%
Total	100%
Extrapolated value	979.05

Q9b. What is the value of your largest loss (PML) due to cyber business interruption? Please assume the normal functioning of passive protective features – such as perimeter controls, data loss prevention tools, data encryption, identity and access management systems and more.	Global
Less than \$1 million	21%
\$1 to 10 million	25%
\$11 to 50 million	19%
\$51 to 100 million	15%
\$101 to 500 million	11%
\$501 to 1 billion	6%
\$1 to 10 billion	3%
More than \$10 billion	0%
Total	100%
Extrapolated value	265.66

Q10. What percentage of this potential loss to information assets is covered by insurance, including captives reinsured but not including captives not reinsured?	Global
Less than 5%	34%
5% to 10%	31%
11% to 20%	13%
21% to 30%	7%
31% to 40%	6%
41% to 50%	3%
51% to 60%	3%
61% to 70%	2%
71% to 80%	1%
81% to 90%	1%
91% to 100%	0%
Total	100%
Extrapolated value	0.15

Q11. What percentage of this potential loss to information assets is self-insured, including captives not reinsured?	Global
Less than 5%	1%
5% to 10%	4%
11% to 20%	2%
21% to 30%	3%
31% to 40%	6%
41% to 50%	11%
51% to 60%	19%
61% to 70%	21%
71% to 80%	19%
81% to 90%	9%
91% to 100%	5%
Total	100%
Extrapolated value	0.59

Q12. What is the likelihood your company will sustain a loss to information assets totaling no more than 50 percent of PML over the next 12 months?	Global
Less than 0.1%	2%
0.1% to 0.5%	3%
0.6% to 1.0%	5%
1.1% to 2.0%	10%
2.1% to 3.0%	10%
3.1% to 4.0%	17%
4.1% to 5.0%	16%
5.1% to 10.0%	19%
More than 10.0%	18%
Total	100%
Extrapolated value	5.2%

Q13. What is the likelihood your company will sustain a loss to information assets totaling 100 percent of PML over the next 12 months?	Global
Less than 0.1%	10%
0.1% to 0.5%	9%
0.6% to 1.0%	11%
1.1% to 2.0%	12%
2.1% to 3.0%	17%
3.1% to 4.0%	16%
4.1% to 5.0%	16%
5.1% to 10.0%	6%
More than 10.0%	3%
Total	100%
Extrapolated value	2.8%

Q14. In your opinion, how would your company disclose a material loss to information assets that is not covered by insurance in its financial statements?	Global
Disclosure as a contingent liability on the balance sheet (FASB 5)	10%
Footnote disclosure in the financial statements	41%
Discussion in the management letter	7%
None – disclosure is not necessary	36%
Other	6%
Total	100%

Part 2. Other Questions

Q15. Are you aware of the economic and legal consequences resulting from a data breach or security exploit in other countries in which your company operates, such as the European Union's General Data Protection Regulation (GDPR), which may issue a fine of up to 5 percent of an organization's worldwide revenue?	Global
Yes, fully aware	29%
Yes, somewhat aware	51%
Not aware	20%
Total	100%

Q16a. Has your company experienced a material or significantly disruptive security exploit or data breach one or more times over the past 24 months? Please refer to the definition of materiality provided above.	Global
Yes	46%
No [skip to Q17]	54%
Total	100%

Q16b. If yes, what best describes the data breaches or security exploits experienced by your company over the past 24 months? Please select all that apply.	Global
Cyber attack that caused disruption to business and IT operations (such as denial of service attacks)	46%
Cyber attack that resulted in the theft of business confidential information, thus requiring notification to victims	26%
Cyber attack that resulted in the misuse or theft of business confidential information, such as intellectual properties	34%
Negligence or mistakes that resulted in the loss of business confidential information	34%
System or business process failures that caused disruption to business operations (e.g. software updates)	47%
Other	6%
Total	193%

Q16c. If yes, what was the total financial impact of security exploits and data breaches experienced by your company over the past 24 months. Please include all costs including out-of-pocket expenditures such as consultant and legal fees, indirect business costs such as productivity losses, diminished revenues, legal actions, customer turnover and reputation damages.	Global
Zero	0%
Less than \$10,000	8%
\$10,001 to \$100,000	10%
\$100,001 to \$250,000	17%
\$250,001 to \$500,000	24%
\$500,001 to \$1,000,000	11%
\$1,000,001 to \$5,000,000	13%
\$5,000,001 to \$10,000,000	9%
\$10,000,001 to \$25,000,000	4%
\$25,000,001 to \$50,000,000	2%
\$50,000,001 to \$100,000,000	1%
More than \$100,000,000	0%
Total	100%
Extrapolated value	3,556,298

Q16d. If yes, how has the above security exploit or data breach changed your company's concerns about cyber liability?	Global
More concerned	63%
Less concerned	12%
No change	25%
Total	100%

Q17. Do you believe your company's exposure to cyber risk will increase, decrease or stay the same over the next 24 months?	Global
Increase	64%
Decrease	12%
Stay the same	25%
Total	100%

Q18a. From a business risk perspective, how do cyber risks compare to other business risks. Please select one best choice.	Global
Cyber liability is the number one or two business risk for my company	17%
Cyber liability is a top 5 business risk for my company	33%
Cyber liability is a top 10 business risk for my company	37%
Cyber liability is not in the top 10 of business risks for my company	13%
Total	100%

Q18b. How did you determine the level of cyber risk to your company?	Global
Completed a formal internal assessment	18%
Completed an informal (ad hoc) internal assessment	22%
Hired a third party to conduct an assessment or audit	33%
Intuition or gut feel	17%
Did not do any type of assessment	11%
Total	100%

Q19a. Does your company have cyber insurance coverage, including within a technology Errors & Omission or similar policy not including Property, General Liability or Crime policy?	Global
Yes	24%
No [skip to Q20a]	76%
Total	100%

Q19b. If yes, what limits do you purchase	Global
Less than \$1 million	7%
\$1 million to \$5 million	33%
\$6 million to \$20 million	49%
\$21 million to \$100 million	7%
More than \$100 million	4%
Total	100%

Q19c. Is your company's cyber insurance coverage sufficient with respect to coverage terms and conditions, exclusions, retentions, limits and insurance carrier financial security?	Global
Yes	63%
No	23%
Unsure	14%
Total	100%

Q19d. How does your company determine the level of coverage it deems adequate?	Global
Formal risk assessment by in-house staff	13%
Formal risk assessment conducted by the insurer	13%
Formal risk assessment by third party	22%
Informal or ad hoc risk assessment	13%
Policy terms and conditions reviewed by a third-party specialist	22%
Maximum available from the insurance market	16%
Other	1%
Total	100%

Q19e. What types of incidents does your organization's cyber insurance cover? Please select all that apply.	Global
External attacks by cyber criminals	86%
Malicious or criminal insiders	84%
System or business process failures	43%
Human error, mistakes and negligence	34%
Incidents affecting business partners, vendors or other third parties that have access to your company's information assets	42%
Other	33%
Total	321%

Q19f. What coverage does this insurance offer your company? Please select all that apply.	Global
Forensics and investigative costs	60%
Notification costs to data breach victims	57%
Communication costs to regulators	52%
Employee productivity losses	54%
Replacement of lost or damaged equipment	57%
Revenue losses	30%
Legal defense costs	47%
Regulatory penalties and fines	48%
Third-party liability	45%
Brand damages	21%
Other	21%
Unsure	28%
Total	521%

Q19g. In addition to cost coverage, what other services does the cyber insurer provide your company in the event of a security exploit or data breach? Please check all that apply.	Global
Access to cyber security forensic experts	82%
Access to legal and regulatory experts	76%
Access to specialized technologies and tools	47%
Advanced warnings about ongoing threats and vulnerabilities	42%
Assistance in the remediation of the incident	53%
Assistance in the notification of breach victims	45%
Identity protection services for breach victims	25%
Credit monitoring services for breach victims	41%
Assistance in reputation management activities	50%
Other	18%
Total	479%

Q20a. Does your company plan to purchase standalone cyber insurance?	Global
Yes, in the next 12 months	14%
Yes, in the next 24 months	24%
Yes, in more than 24 months	18%
No	43%
Total	100%

Q20b. If no, what are the main reasons why your company is not planning to purchase standalone cyber security insurance?	Global
Premiums are too expensive	36%
Coverage is inadequate based on our exposure	36%
Too many exclusions, restrictions and uninsurable risks	27%
Risk does not warrant insurance	7%
Property and casualty policies are sufficient	30%
Executive management does not see the value of this insurance	22%
Unable to get insurance underwritten because of current risk profile	17%
Other	7%
Total	181%

Q21. Who in your company is most responsible for cyber risk management? Please select your one top choice.	Global
CEO/board of directors	2%
Chief financial officer	6%
Business unit (LOB) leaders	23%
Chief information officer	24%
Chief information security officer	15%
Risk management	15%
Procurement	5%
General counsel	7%
Compliance/audit	3%
Other	1%
Total	100%

Part 3. Role & Organizational Characteristics

D1. What level best describes your current position?	Global
Senior executive	3%
Vice president	4%
Director	13%
Manager	15%
Supervisor	15%
Associate/staff	10%
Technician	31%
Contractor/consultant	7%
Other	1%
Total	100%

D2. What is the worldwide employee headcount of your company?	Global
Less than 500	13%
500 to 1,000	16%
1,001 to 5,000	28%
5,001 to 25,000	26%
25,001 to 75,000	11%
More than 75,000	6%
Total	100%

D3. What best describes your company's industry focus?	Global
Agriculture & food service	2%
Communications	3%
Consumer products	6%
Defense & aerospace	0%
Education & research	4%
Energy & utilities	5%
Entertainment & media	2%
Financial services	16%
Health & pharmaceuticals	9%
Hospitality	2%
Industrial	10%
Other	1%
Public sector	10%
Retail	9%
Services	12%
Technology & software	5%
Transportation	3%
Total	100%

ACKNOWLEDGEMENTS

We appreciate the past review and input of Massachusetts Institute of Technology 2016 Graduate, Adam Kalinich, major Course 18C: "Mathematics with Computer Science."

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling our toll free line at 1.800.887.3118.

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.