2015 Global Cyber Impact Report

Sponsored by Aon Risk Services

Independently conducted by Ponemon Institute LLC

Publication Date: April 2015

AON | Ponemon INSTITUTE

2015 Global Cyber Impact Report

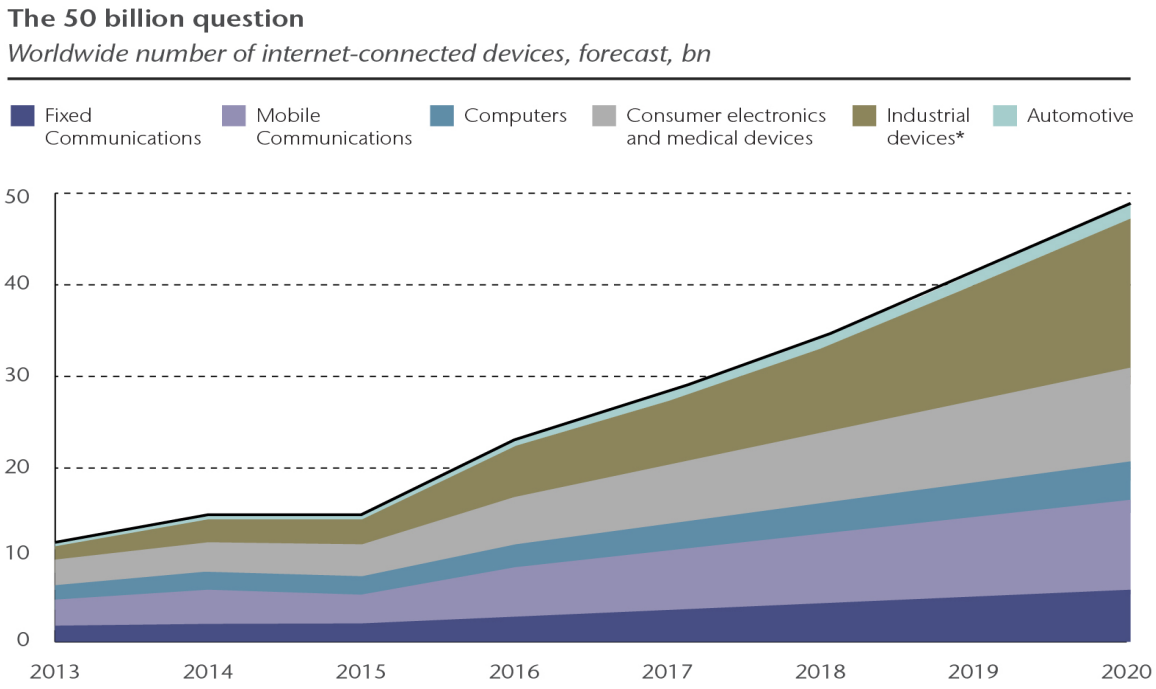
Ponemon Institute, April 2015

Part 1. Introduction

Ponemon Institute is pleased to present the *2015 Global Cyber Impact Report* sponsored by Aon Risk Services. The purpose of the research is to understand how organizations qualify and quantify the financial risk to their tangible and intangible assets in the event of a network privacy or security incident.

The transformation of the world's economies from historical tangible products and manual labor services to reliance on technology and information assets is rapid and severe. Cloud computing, mobile devices, social media, "big data" analytics and the explosion of the "Internet of Things" help facilitate this digital transformation. Figure 1 shows the projected growth in the use of Internet-connected devices to 50 billion by 2020. Just 5 short years from now.

Figure 1. The Internet-connected wonderland of devices
Billions, worldwide number of Internet-connected devices, forecast



Source: Cisco
* Includes military and aerospace

How do organizations qualify and quantify the corresponding financial statement exposure impact? 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 mitigate the financial statement impact of network risk exposures.

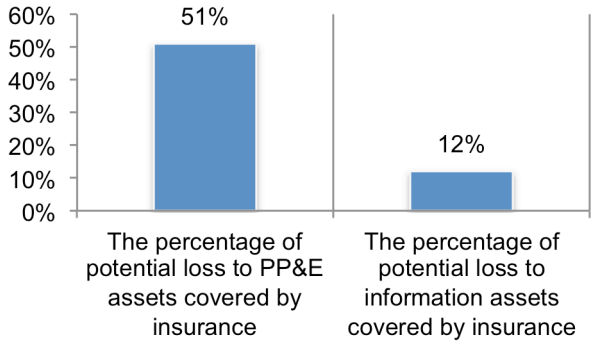
Network risk exposures can broadly include breach of privacy and security of personally identifiable information, stealing an organization's intellectual property, confiscating online bank accounts, creating and distributing viruses on computers, posting confidential business

information on the Internet, robotic malfunctions, and disrupting a country's critical national infrastructure.[1]

We surveyed 2,243 individuals in 37 countries in the following global regions: North America, Europe, Middle East, Africa ("EMEA"), Asia, Pacific, Japan ("APJ") and Latin America ("LATAM").[2] Participants in this research are involved in their companies' cyber risk management as well as enterprise risk management activities. Most respondents are either in finance, treasury and accounting (37 percent of respondents) or risk management (17 percent of respondents). Other respondents are in corporate compliance/audit (14 percent of respondents) and general management (14 percent of respondents).

All respondents are familiar with the cyber risks facing their companies to some degree. 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.[3]

Figure 2. The percentage of PP&E and information assets covered by insurance



As shown in Figure 2, despite the comparability of the average potential loss to information assets ($617 million) and Property, Plant & Equipment ("PP&E") ($648 million) the percentages of insurance coverage differs significantly.

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 occurring, even though PML can exceed $200 million.
- Disclosure of a material loss of PP&E and information assets differs. Fifty percent of respondents say their company would disclose the loss of PP&E in its financial statements as a footnote disclosure. However, 34 percent of respondents say a material loss to information assets does not require disclosure.
- Despite the risk, companies are reluctant to purchase cyber insurance coverage. Fifty-two percent of respondents believe their companies' exposure to cyber risk will increase over the next 24 months. However, only 19 percent of respondents say their company has cyber insurance coverage.
- Thirty-seven percent of 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 $2.1 million.

[1] 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 in terms of enterprise management financial statement impact.
[2] The regional findings are published in separate reports
[3] Source: Institute of Risk Management

Part 2. Key findings

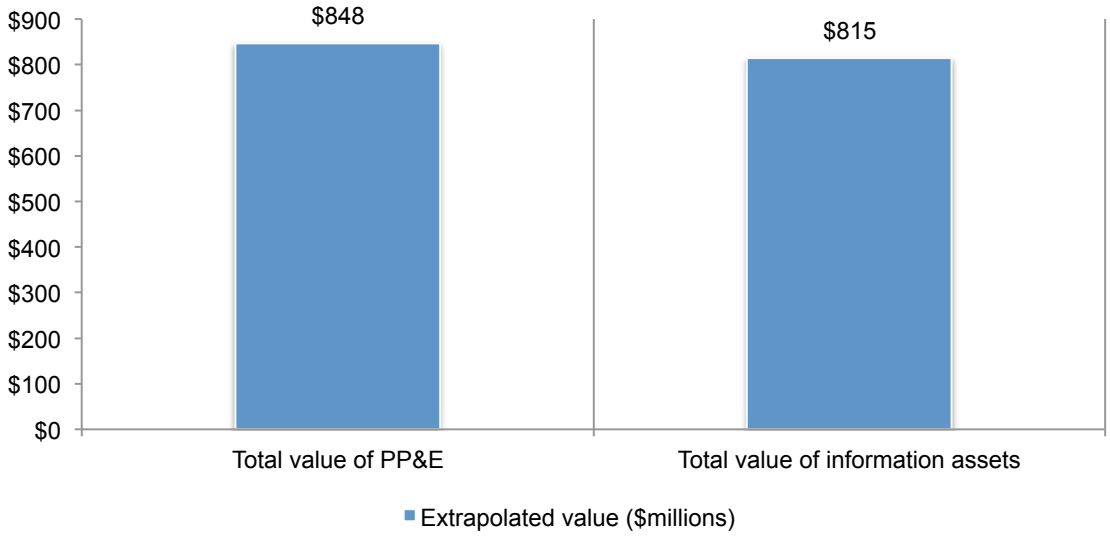
The complete audited findings are presented in the appendix of this report. We have organized the report according to the following topics:

- 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 PP&E[4] slightly higher than information assets. According to Figure 3, on average, the total value of PP&E, including all fixed assets plus supervisory control and data acquisition systems ("SCADA") and industrial control systems is approximately $848 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 less than PP&E at $815 million.

Figure 3. The total value of PP&E and information assets
Extrapolated value

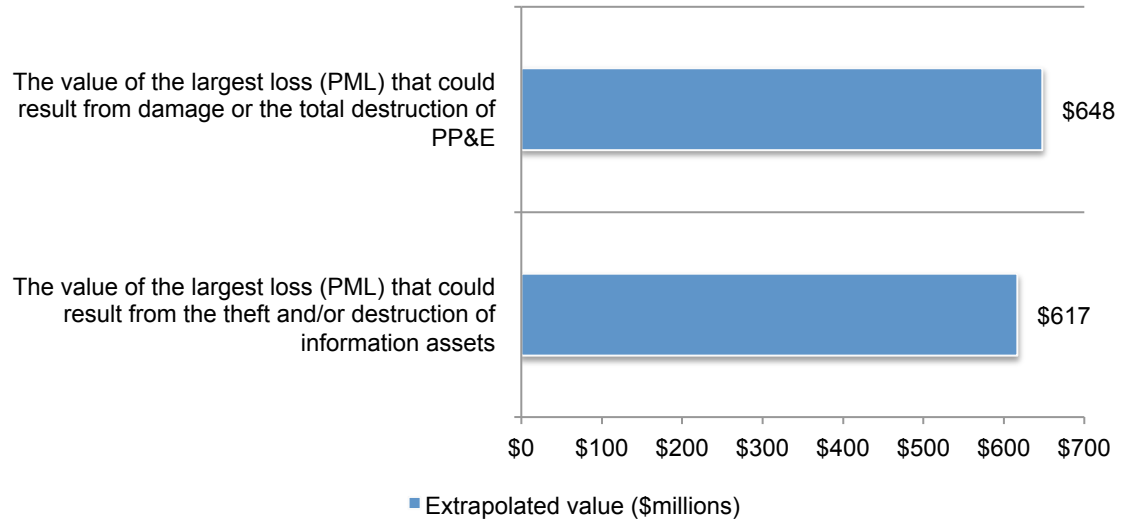


[4] Respondents were asked to assume, with respect to PP&E assets, the root causes of loss (a.k.a. perils) which include fire, flooding, weather events, earthquakes and other natural or man-made disasters.

The value of probable maximum loss (PML)[5] is higher for PP&E. Companies estimate the PML value of the largest loss that could result from damage or total destruction of PP&E is approximately $648 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.

In the case of information assets stolen or destroyed, the value of the largest loss is an average of approximately $617 million, according to Figure 4. 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.

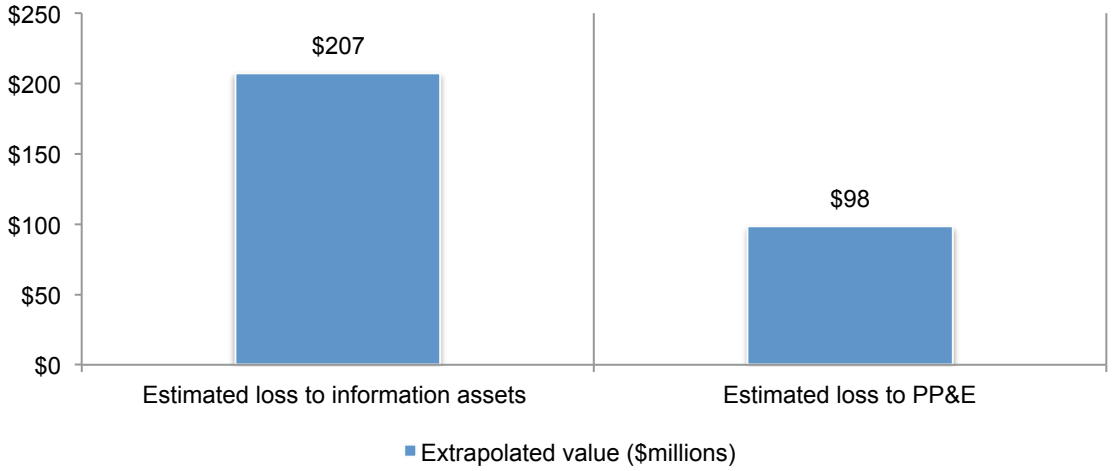
Figure 4. The PML value for PP&E and information assets



[5] 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 5, business disruption has a greater impact on information assets ($207 million)[6] than on PP&E ($98 million). This suggests the fundamental nature of PML varies considerably for intangible vs. tangible assets. In the present study, business disruption is only 15 percent of the PML for PP&E. In contrast, business disruption represents 34 percent of the PML for information assets.

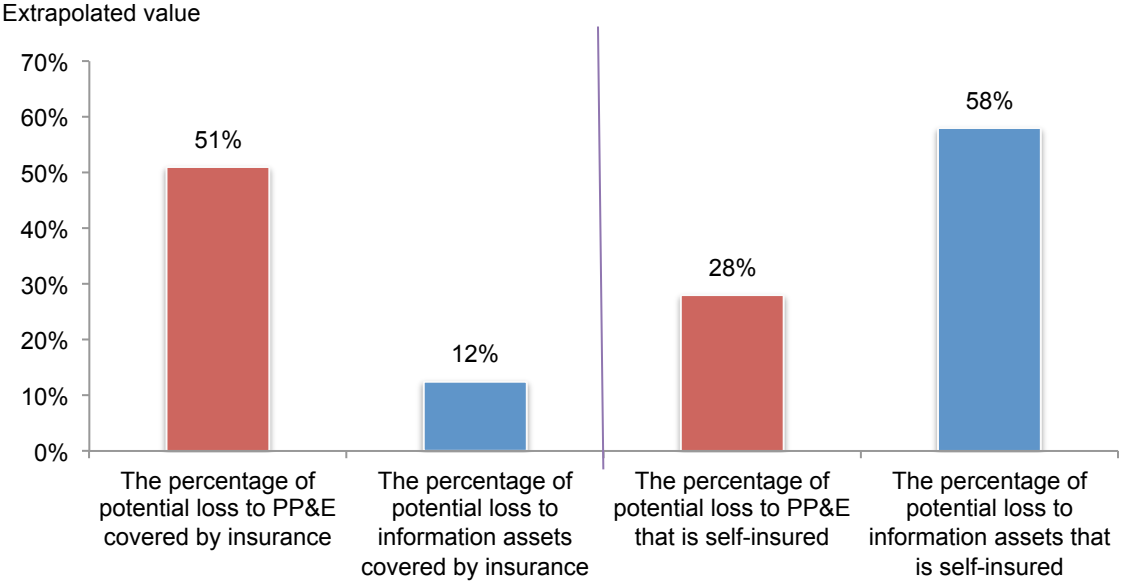
Figure 5. The impact of business disruption to information assets and PP&E



[6] While the survey results suggest Probable Maximum Loss in the neighborhood of $200 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.

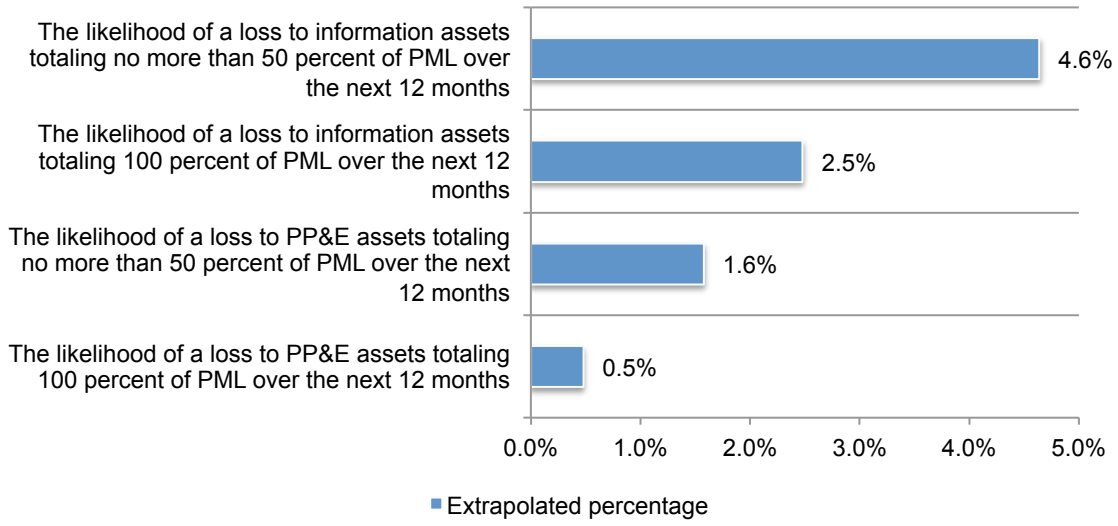
There is a significant difference between the insurance coverage of PP&E and information assets. On average, approximately 51 percent of PP&E assets are covered by insurance and approximately 28 percent of PP&E assets are self-insured (Figure 6).[7] Only an average of 12 percent of information assets are covered by insurance. Self-insurance is higher for information assets at 58 percent.

Figure 6. Percentage of PP&E and information assets covered by insurance
Extrapolated value



The likelihood of a loss is higher for information assets than PP&E. Companies estimate the likelihood that they will sustain a loss to information assets totaling no more than 50 percent of PML in the next 12 months at 4.6 percent and 100 percent of PML at 2.5 percent, according to Figure 7. The likelihood of a loss to PP&E totaling no more than 50 percent of PML is an average of 1.6 percent and at 100 percent of PML it is 0.5 percent.

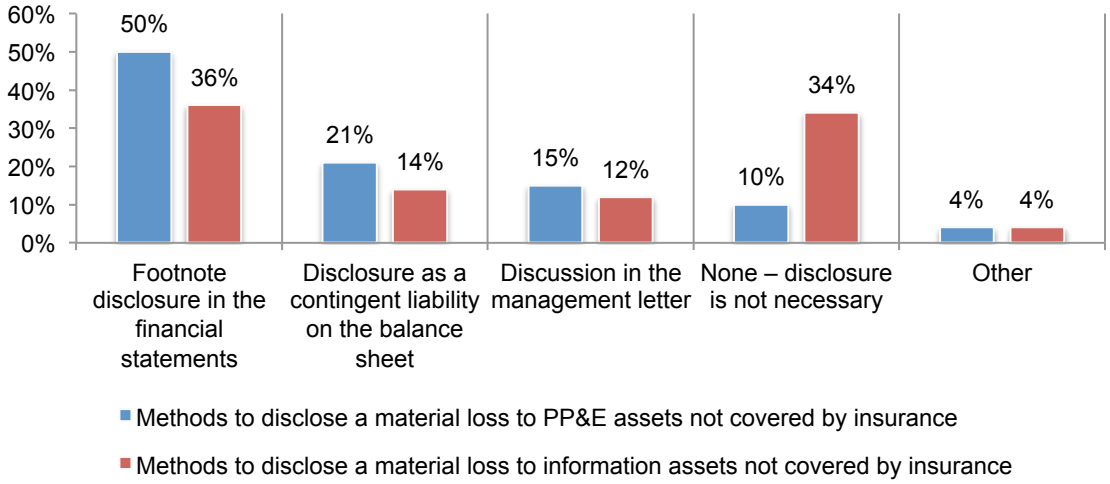
Figure 7. Likelihood of loss to PP&E and information assets totaling more than 50 percent and 100 percent of PML over the next 12 months



[7] The percentages do not add up to 100% 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 a material loss to PP&E and information assets differs as well. Figure 8 focuses on how companies would disclose a material loss. Fifty 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 statements followed by 21 percent who say they would disclose it as a contingent liability on the balance sheet (e.g. FASB 5). Thirty-six percent say they would disclose a material loss to information assets as a footnote disclosure in the financial statements, but 34 percent of respondents do not believe disclosure is necessary.

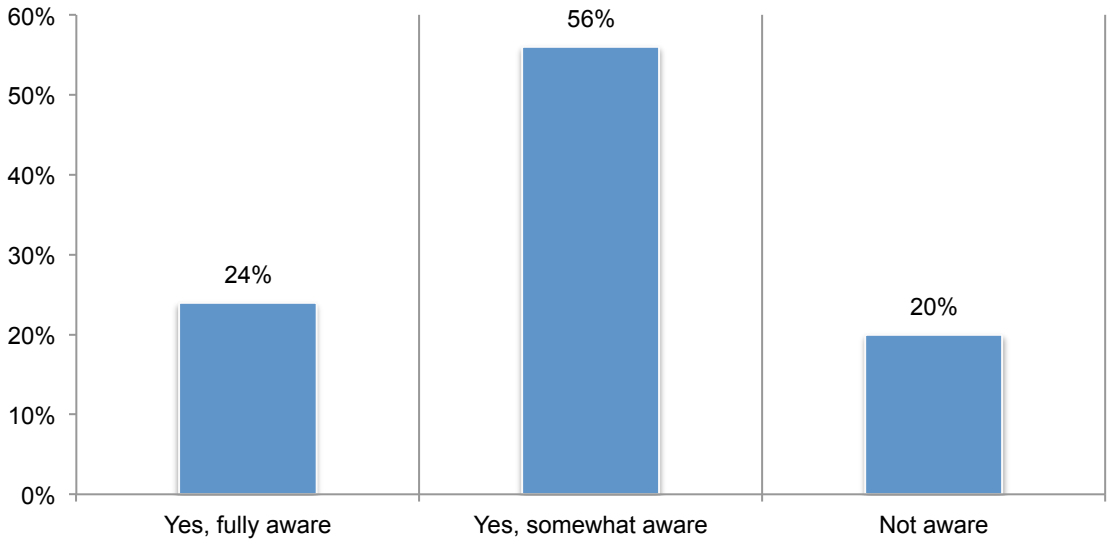
Figure 8. How would your company disclose a material loss to PP&E and information assets?



The cyber risk experience of companies

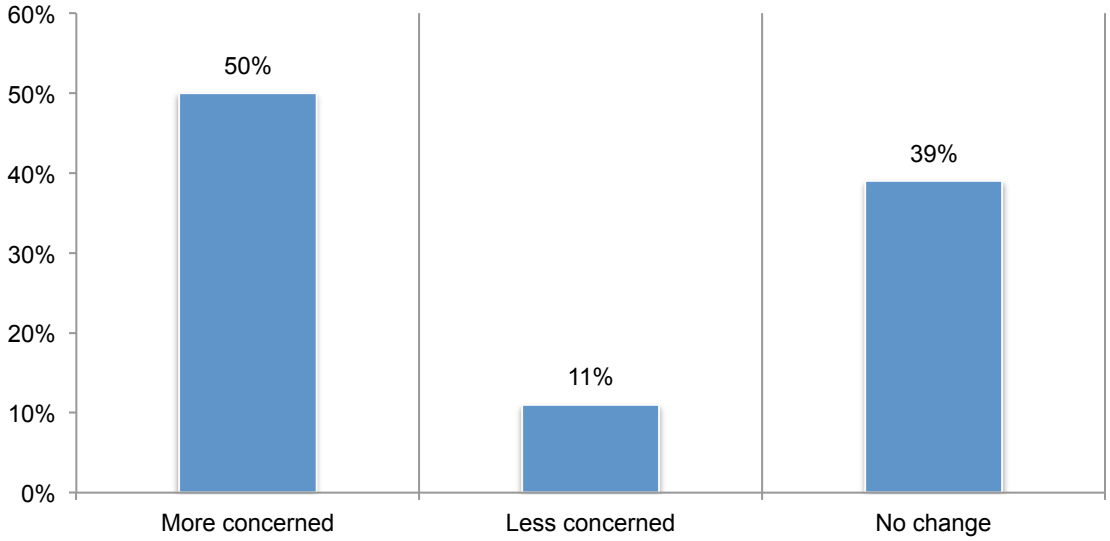
Awareness of the economic and legal consequences from an international data breach or security exploit is low. As revealed in Figure 9, only 24 percent of respondents are fully aware of the consequences that could result from a data breach or security exploit in other countries in which their company operates and 20 percent say they are not aware.

Figure 9. Awareness of the economic and legal consequences from an international data breach or security exploit



Thirty-seven percent of companies represented in this study had a material[8] or significantly disruptive security exploit or data breach one or more times in the past 24 months. The average total financial impact of these incidents was $2.1 million[9]. According to Figure 10, 50 percent of these respondents say the incident made their companies more concerned about cyber liability.

Figure 10. How did the security exploit or data breach change your company's concerns about cyber liability?

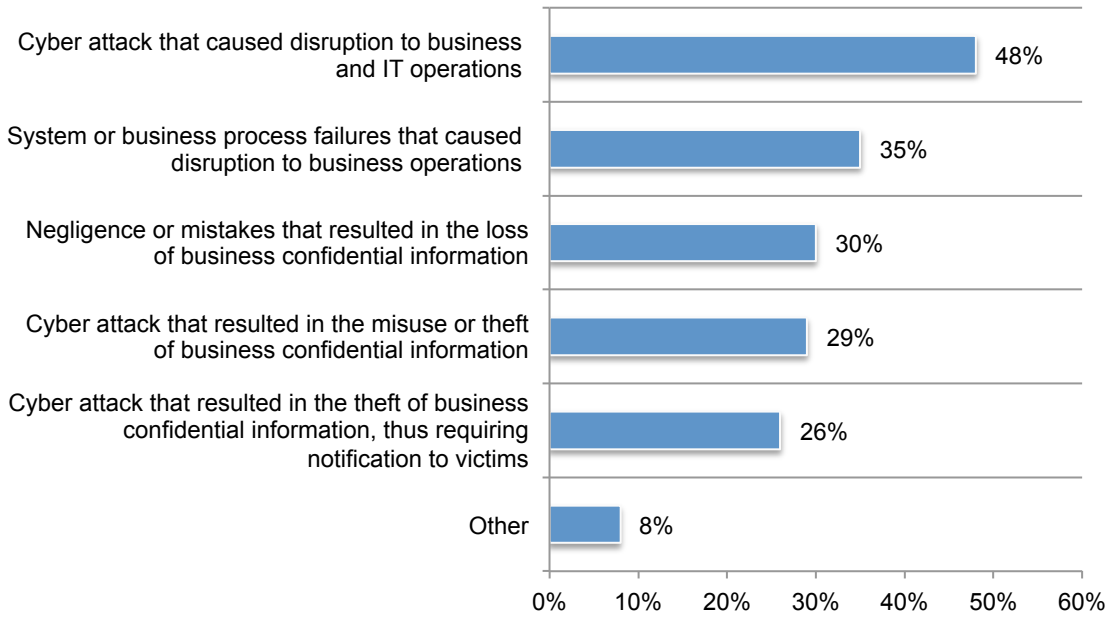


[8] In the context of this study, the term materiality takes into consideration monies expended for first-party losses, potential third-party liabilities, value of lost time, litigation costs, reputation damages and revenue losses. This term is broader than materiality as defined by GAAP and SEC requirements.
[9] 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.

Figure 11 reveals the type of security incidents by percent of the companies represented in this research. The most frequent type of incident was a cyber attack that caused disruption to business and IT operations (48 percent of respondents) followed by 35 percent of respondents who say it was a system or business process failure that caused disruption to business operations.

Incidents involving the loss or theft of information assets were not as prevalent as those causing business disruptions. Cyber attacks that resulted in the misuse or theft of business confidential information (such as intellectual properties) and the theft of business confidential information requiring notification occurred according to 29 percent and 26 percent of respondents, respectively. Thirty percent of respondents say the security incident was caused by negligence or mistakes that resulted in the loss of business confidential information.

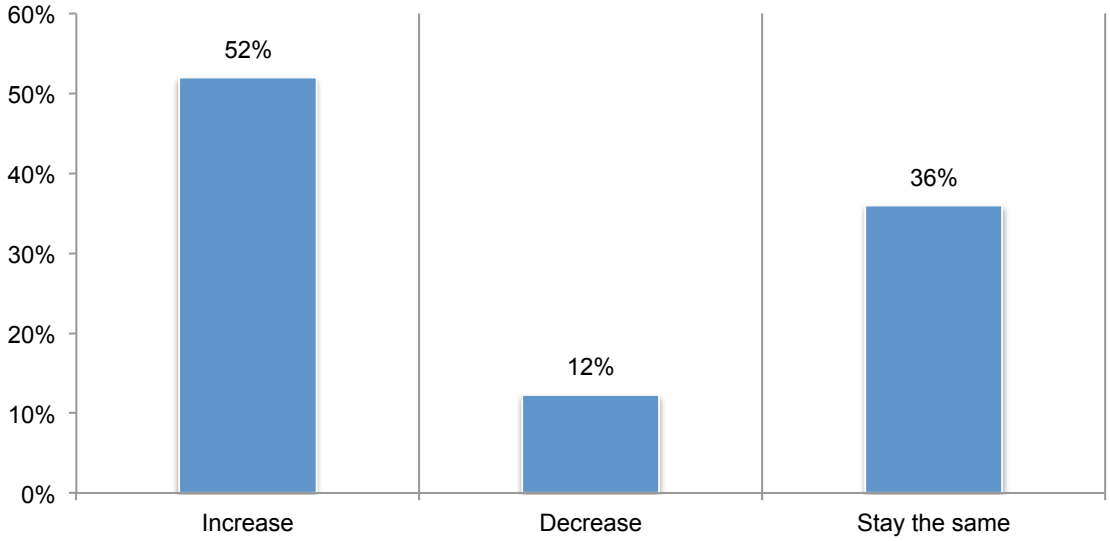
Figure 11. What type of data breach or security exploit did your company experience?
More than one response permitted



Perceptions about the financial impact of cyber exposures

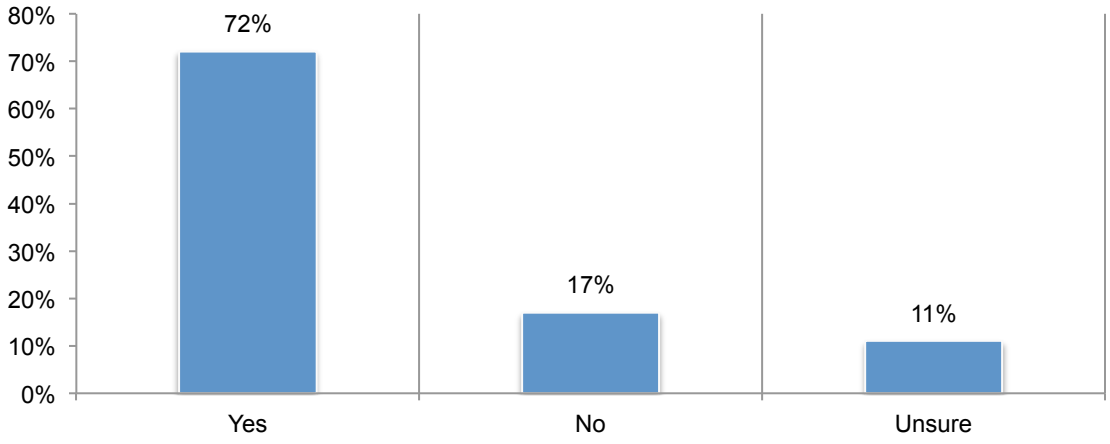
Companies' exposure to cyber risk is expected to increase, but the majority of respondents (54 percent) say there is no plan to purchase cyber insurance. According to Figure 12, 52 percent of respondents believe their companies' exposure to cyber risk will increase and 36 percent of respondents say it will stay the same. Only 12 percent of respondents expect it to actually decrease.

Figure 12. Will your company's cyber risk exposure increase, decrease or stay the same over the next two years?



Despite the cyber risk, only 19 percent of respondents say their companies currently have cyber insurance coverage with an average limit of $13 million. As shown in Figure 13, 72 percent of respondents believe this is sufficient with respect to coverage terms and conditions, exclusions, retentions, limits and insurance carrier financial security.

Figure 13. Is your company's cyber insurance coverage sufficient?



According to Figure 14, third parties are mainly determining the adequacy of coverage. Twenty-two percent of respondents say they had a formal risk assessment by a third party and 20 percent of respondents say a third-party specialist reviewed policy terms and conditions. This is followed by a formal risk assessment by in-house staff (18 percent of respondents). Fourteen percent say they had an informal or ad hoc risk assessment and 13 percent say it was a formal risk assessment conducted by the insurer.

Figure 14. How companies determine the adequacy of coverage

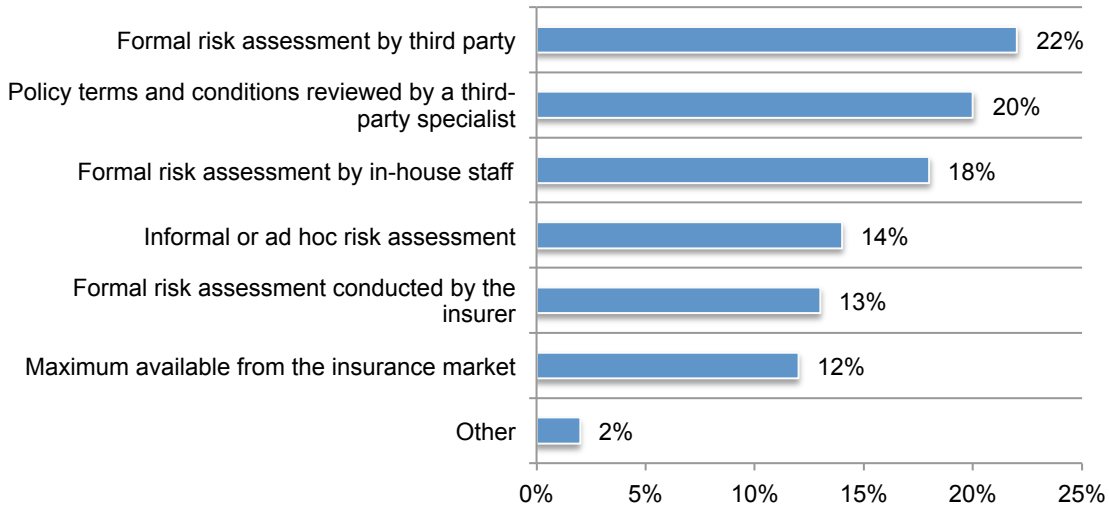
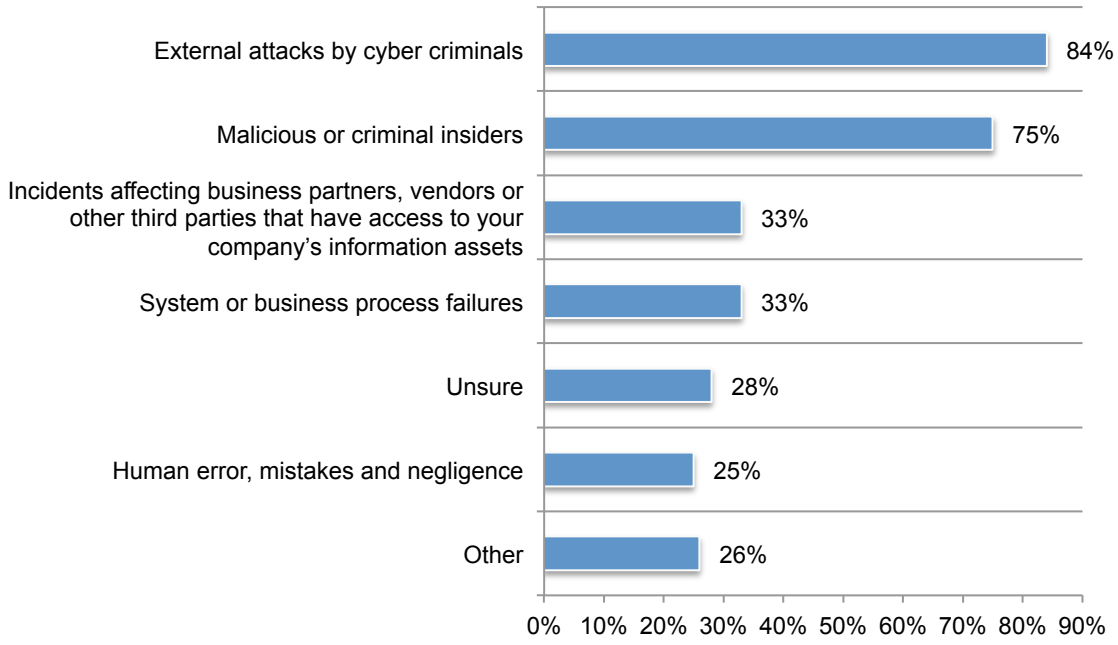


Figure 15 addresses incidents covered by cyber insurance. Most incidents covered are external attacks by cyber criminals (84 percent of respondents), malicious or criminal insiders (75 percent of respondents) and incidents affecting business partners, vendors or other third parties that have access to company's information assets (33 percent of respondents).

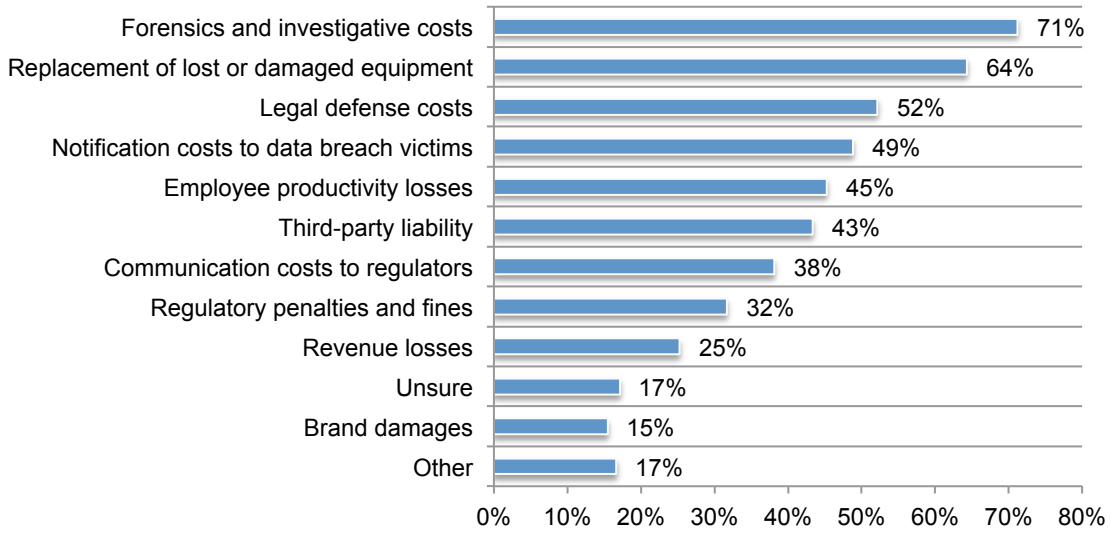
While system or business process failures were the most often cited as the cause of the data breach or exploit, only 33 percent of respondents say these incidents are covered by their cyber insurance. Twenty-eight percent are unsure what incidents are covered.

Figure 15. Types of incidents covered by cyber insurance
More than one response permitted



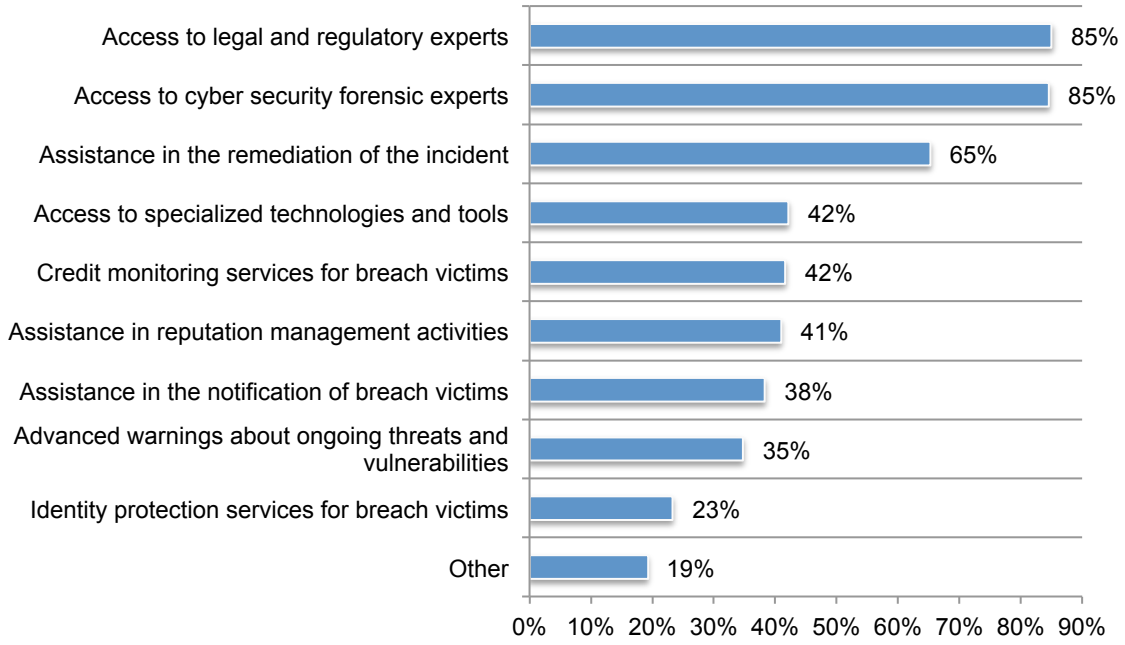
Figures 16 and 17 present the coverage and services provided by insurance companies. The top five costs covered are: forensics and investigative costs (71 percent of respondents), replacement of lost or damaged equipment (64 percent of respondents) legal defense costs (52 percent of respondents), notification costs to data breach victims (49 percent of respondents) and employee productivity losses (45 percent of respondents). Seventeen percent of respondents are unsure what coverage is provided.

Figure 16. Coverage provided by the insurance company
More than one response permitted



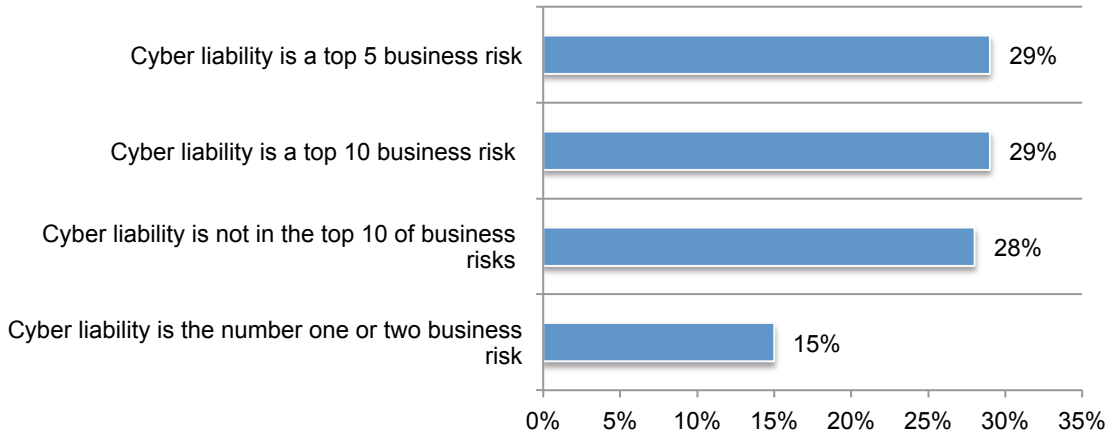
Other services provided are: access to legal and regulatory experts and cyber security forensic experts (both 85 percent of respondents), assistance in the remediation of the incident (65 percent of respondents) and access to specialized technologies and tools (42 percent of respondents). Forty-two percent of respondents say they receive credit monitoring services for breach victims.

Figure 17. Other services provided by the cyber insurer
More than one response permitted



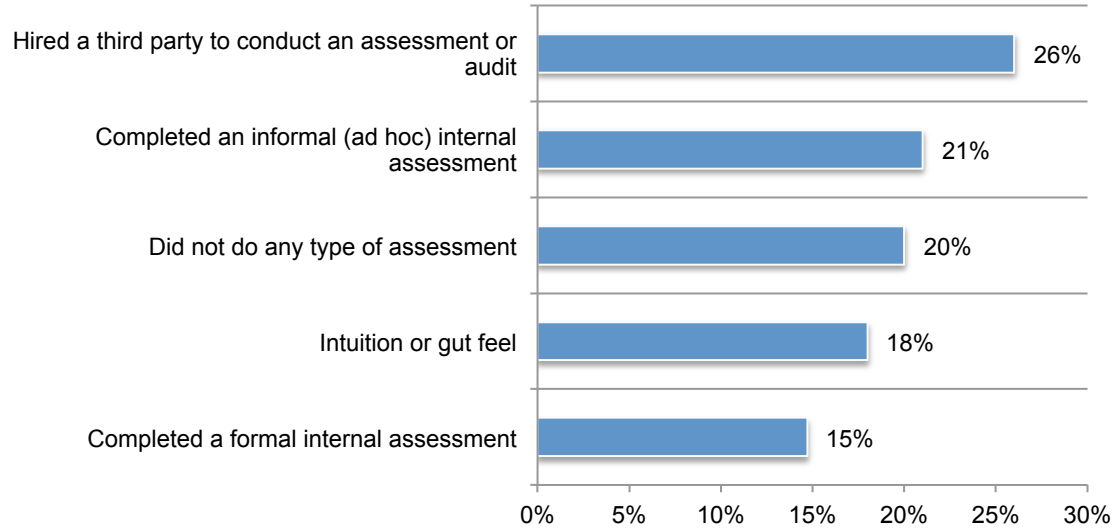
Cyber liability ranks in the top 10 of all business risks facing companies. As shown in Figure 18, 72 percent of respondents consider cyber risk as a top 10 business risk. Cyber risk ranks as number one or two of all business risks (15 percent of respondents), in the top five (29 percent of respondents) and in the top 10 (29 percent). Twenty-eight percent of respondents believe it is not in the top 10 of all business risks facing their companies.

Figure 18. How do cyber risks compare to other business risks?



To determine the cyber risk to their companies, 26 percent of respondents say the company hired a third party to conduct an assessment or audit and 21 percent of respondents say it was an informal (ad hoc) internal assessment (Figure 19). Only 15 percent of respondents say their companies' completed a formal internal assessment but 18 percent of respondents say it was intuition or gut feel.

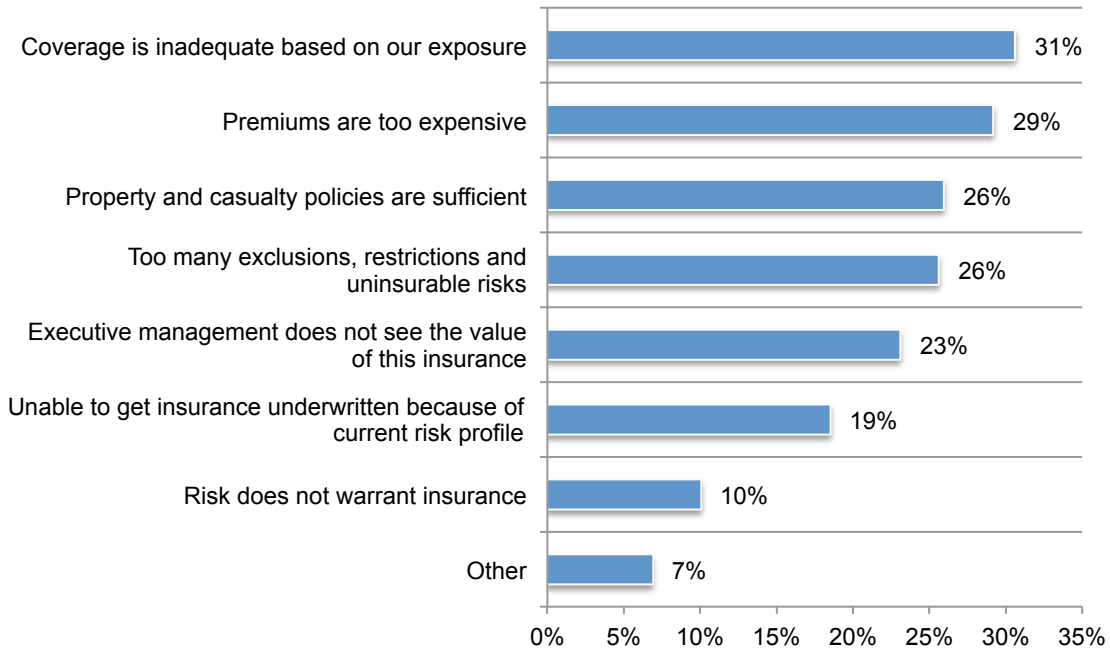
Figure 19. How did you determine the level of cyber risk to your company?



Will the purchase of cyber insurance increase because of concerns about security exploits and data breaches? Fifty-four percent of respondents do not have plans to purchase cyber insurance. Thirteen percent of respondents say their companies will purchase cyber insurance in the next 12 months, 22 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 20, the main reasons for not purchasing cyber security insurance are: coverage is inadequate based on their exposure (31 percent of respondents), premiums are too expensive (29 percent of respondents) and property and casualty policies are sufficient (26 percent of respondents) there are too many exclusions, restriction and uninsurable risks (26 percent of respondents).

Figure 20. What are the main reasons why your company will not purchase cyber security insurance?
More than one response permitted



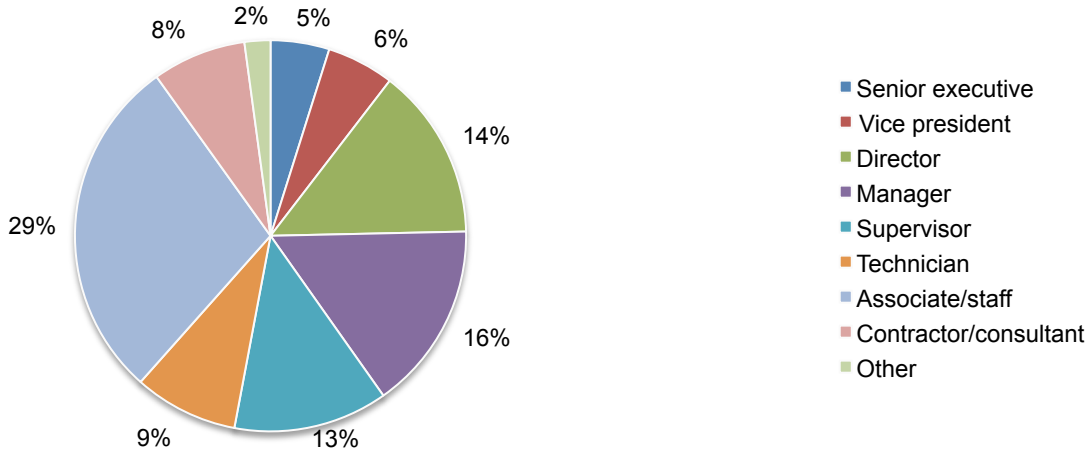
Part 3. Methods

The global sampling frame is composed of 60,121 individuals that are involved in their companies' cyber risk and enterprise risk management activities. As shown in Table 1, 2,525 respondents completed the survey. Screening removed 282 surveys. The final sample was 2,243 surveys (or a 3.7 percent response rate).

Table 1. Sample response	Freq	Pct%
Total sampling frame	60,121	100.0%
Total returns	2,525	4.2%
Rejected or screened surveys	282	0.5%
Final sample	2,243	3.7%

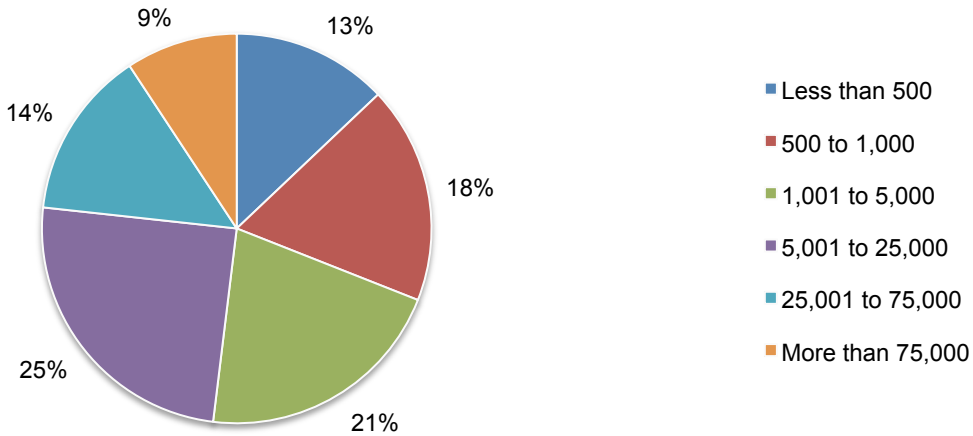
Pie Chart 1 reports the current position or organizational level of the respondents. More than half of respondents (53 percent) reported their current position as supervisory or above.

Pie Chart 1. Current position or organizational level



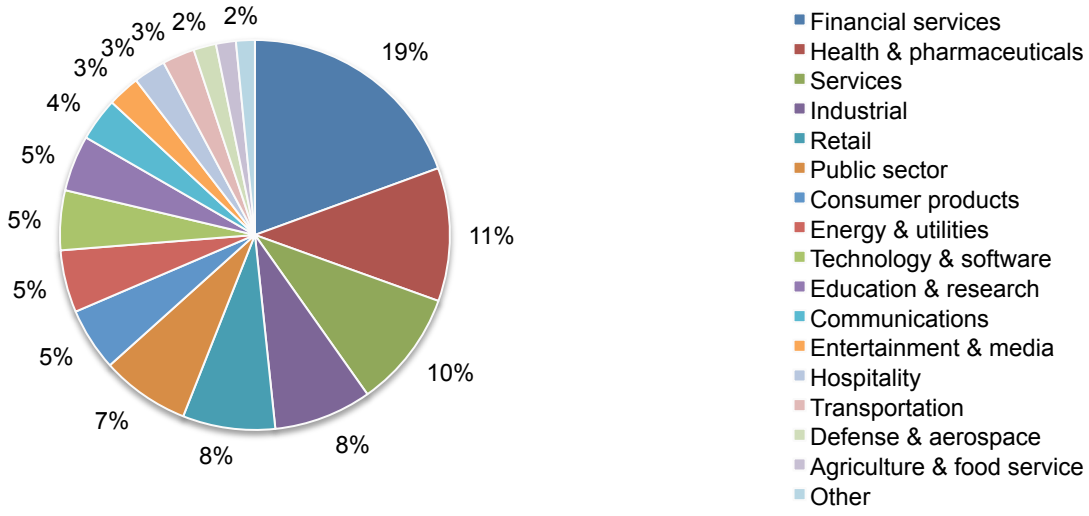
According to Pie Chart 2, sixty-nine percent of the respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 2. Worldwide headcount of the organization



Pie Chart 3 reports the primary industry classification of respondents' organizations. This chart identifies financial services (19 percent) as the largest segment, followed by health and pharmaceuticals (11 percent) and services (10 percent).

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 companies' 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 in February 2015.

Survey response	GLOBAL
Sampling frame	60,121
Total returns	2,525
Final sample	2,243
Response rate	3.7%

Screening questions

S1. How familiar are you with cyber risks facing your company today?	GLOBAL
Very familiar	14%
Familiar	34%
Somewhat familiar	52%
Not familiar	0%
Total	100%

S2. Are you involved in your company's cyber risk management activities?	GLOBAL
Yes, significant involvement	24%
Yes, some involvement	76%
No involvement	0%
Total	100%

S3. Are you involved in your company's enterprise risk management activities?	GLOBAL
Yes, significant involvement	29%
Yes, some involvement	71%
No involvement	0%
Total	100%

S4. What best defines your role?	GLOBAL
Risk management	17%
Finance, treasury & accounting	37%
Corporate compliance/audit	14%
Security/information security	13%
General management	14%
Legal (OGC)	5%
None of the above	0%
Total	100%

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

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	8%
$1 to 10 million	15%
$11 to 50 million	12%
$51 to 100 million	24%
$101 to 500 million	22%
$501 to 1 billion	11%
$1 to 10 billion	4%
More than $10 billion	4%
Total	100%
Extrapolated value	847.55

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	10%
$1 to 10 million	15%
$11 to 50 million	16%
$51 to 100 million	25%
$101 to 500 million	19%
$501 to 1 billion	9%
$1 to 10 billion	5%
More than $10 billion	2%
Total	100%
Extrapolated value	647.99

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	21%
$1 to 10 million	29%
$11 to 50 million	24%
$51 to 100 million	18%
$101 to 500 million	6%
$501 to 1 billion	1%
$1 to 10 billion	0%
More than $10 billion	0%
Total	100%
Extrapolated value	98.28

Q3. What percentage of this potential loss to PP&E assets is covered by insurance?	GLOBAL
Less than 5%	6%
5% to 10%	8%
11%to 20%	5%
21% to 30%	7%
31% to 40%	8%
41% to 50%	10%
51% to 60%	17%
61% to 70%	12%
71% to 80%	12%
81% to 90%	9%
91% to 100%	6%
Total	100%
Extrapolated value	51%

Q4. What percentage of this potential loss to PP&E assets is self-insured?	GLOBAL
Less than 5%	14%
5% to 10%	16%
11% to 20%	14%
21% to 30%	16%
31% to 40%	11%
41% to 50%	12%
51% to 60%	5%
61% to 70%	6%
71% to 80%	3%
81% to 90%	1%
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%	25%
0.1% to 0.5%	20%
0.6% to 1.0%	14%
1.1% to 2.0%	12%
2.1% to 3.0%	15%
3.1% to 4.0%	6%
4.1% to 5.0%	5%
5.1% to 10.0%	1%
More than 10.0%	3%
Total	100%
Extrapolated value	1.58%

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%	70%
0.1% to 0.5%	15%
0.6% to 1.0%	8%
1.1% to 2.0%	3%
2.1% to 3.0%	2%
3.1% to 4.0%	0%
4.1% to 5.0%	1%
5.1% to 10.0%	1%
More than 10.0%	1%
Total	100%
Extrapolated value	0.48%

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)	21%
Footnote disclosure in the financial statements	50%
Discussion in the management letter	15%
None – disclosure is not necessary	10%
Other	4%
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	10%
$1 to 10 million	14%
$11 to 50 million	14%
$51 to 100 million	20%
$101 to 500 million	17%
$501 to 1 billion	18%
$1 to 10 billion	5%
More than $10 billion	4%
Total	100%
Extrapolated value	814.76

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	10%
$1 to 10 million	17%
$11 to 50 million	14%
$51 to 100 million	26%
$101 to 500 million	17%
$501 to 1 billion	9%
$1 to 10 billion	6%
More than $10 billion	2%
Total	100%
Extrapolated value	617.06

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	23%
$1 to 10 million	23%
$11 to 50 million	24%
$51 to 100 million	12%
$101 to 500 million	10%
$501 to 1 billion	5%
$1 to 10 billion	2%
More than $10 billion	0%
Total	100%
Extrapolated value	207.34

Q10. What percentage of this potential loss to information assets is covered by insurance?	GLOBAL
Less than 5%	32%
5% to 10%	43%
11% to 20%	9%
21% to 30%	6%
31% to 40%	3%
41% to 50%	2%
51% to 60%	2%
61% to 70%	1%
71% to 80%	1%
81% to 90%	1%
91% to 100%	0%
Total	100%
Extrapolated value	12%

Q11. What percentage of this potential loss to information assets is self-insured?	GLOBAL
Less than 5%	5%
5% to 10%	6%
11% to 20%	2%
21% to 30%	2%
31% to 40%	3%
41% to 50%	7%
51% to 60%	18%
61% to 70%	20%
71% to 80%	24%
81% to 90%	9%
91% to 100%	4%
Total	100%
Extrapolated value	58%

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%	7%
0.1% to 0.5%	9%
0.6% to 1.0%	6%
1.1% to 2.0%	7%
2.1% to 3.0%	9%
3.1% to 4.0%	13%
4.1% to 5.0%	14%
5.1% to 10.0%	21%
More than 10.0%	14%
Total	100%
Extrapolated value	4.64%

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%	14%
0.1% to 0.5%	11%
0.6% to 1.0%	9%
1.1% to 2.0%	12%
2.1% to 3.0%	18%
3.1% to 4.0%	12%
4.1% to 5.0%	18%
5.1% to 10.0%	6%
More than 10.0%	0%
Total	100%
Extrapolated value	2.48%

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)	14%
Footnote disclosure in the financial statements	36%
Discussion in the management letter	12%
None – disclosure is not necessary	34%
Other	4%
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?	GLOBAL
Yes, fully aware	23%
Yes, somewhat aware	56%
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	37%
No [skip to Q17]	63%
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)	48%
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	29%
Negligence or mistakes that resulted in the loss of business confidential information	30%
System or business process failures that caused disruption to business operations (e.g. software updates)	35%
Other	8%
Total	177%

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	5%
Less than $10,000	13%
$10,001 to $100,000	12%
$100,001 to $250,000	18%
$250,001 to $500,000	19%
$500,001 to $1,000,000	13%
$1,000,001 to $5,000,000	10%
$5,000,001 to $10,000,000	5%
$10,000,001 to $25,000,000	2%
$25,000,001 to $50,000,000	2%
$50,00,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	2,099,656

Q16d. If yes, how has the above security exploit or data breach changed your company's concerns about cyber liability?	GLOBAL
More concerned	50%
Less concerned	11%
No change	39%
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	52%
Decrease	12%
Stay the same	36%
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	15%
Cyber liability is a top 5 business risk for my company	29%
Cyber liability is a top 10 business risk for my company	29%
Cyber liability is not in the top 10 of business risks for my company	28%
Total	100%

Q18b. How did you determine the level of cyber risk to your company?	GLOBAL
Completed a formal internal assessment	20%
Completed an informal (ad hoc) internal assessment	21%
Hired a third party to conduct an assessment or audit	26%
Intuition or gut feel	18%
Did not do any type of assessment	15%
Total	100%

Q19a. Does your company have cyber insurance coverage?	GLOBAL
Yes	19%
No [skip to Q20a]	81%
Total	100%

Q19b. If yes, what limits do you purchase	GLOBAL
Less than $1 million	24%
$1 million to $5 million	32%
$6 million to $20 million	35%
$21 million to $100 million	5%
More than $100 million	4%
Total	100%
Extrapolated value	12.70

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	72%
No	17%
Unsure	11%
Total	100%

Q19d. How does your company determine the level of coverage it deems adequate?	GLOBAL
Formal risk assessment by in-house staff	18%
Formal risk assessment conducted by the insurer	13%
Formal risk assessment by third party	22%
Informal or ad hoc risk assessment	14%
Policy terms and conditions reviewed by a third-party specialist	20%
Maximum available from the insurance market	12%
Other	2%
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	84%
Malicious or criminal insiders	75%
System or business process failures	33%
Human error, mistakes and negligence	25%
Incidents affecting business partners, vendors or other third parties that have access to your company's information assets	33%
Other	26%
Unsure	28%
Total	304%

Q19f. What coverage does this insurance offer your company? Please select all that apply.	GLOBAL
Forensics and investigative costs	71%
Notification costs to data breach victims	49%
Communication costs to regulators	38%
Employee productivity losses	45%
Replacement of lost or damaged equipment	64%
Revenue losses	25%
Legal defense costs	52%
Regulatory penalties and fines	32%
Third-party liability	43%
Brand damages	15%
Other	17%
Unsure	17%
Total	469%

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? Check all that apply.	GLOBAL
Access to cyber security forensic experts	85%
Access to legal and regulatory experts	85%
Access to specialized technologies and tools	42%
Advanced warnings about ongoing threats and vulnerabilities	35%
Assistance in the remediation of the incident	65%
Assistance in the notification of breach victims	38%
Identity protection services for breach victims	23%
Credit monitoring services for breach victims	42%
Assistance in reputation management activities	41%
Other	19%
Total	475%

Q20a. Does your company plan to purchase cyber insurance?	GLOBAL
Yes, in the next 12 months	13%
Yes, in the next 24 months	22%
Yes, in more than 24 months	18%
No	46%
Total	100%

Q20b. If no, what are the main reasons why your company is not planning to purchase cyber security insurance?	GLOBAL
Premiums are too expensive	29%
Coverage is inadequate based on our exposure	31%
Too many exclusions, restrictions and uninsurable risks	26%
Risk does not warrant insurance	10%
Property and casualty policies are sufficient	26%
Executive management does not see the value of this insurance	23%
Unable to get insurance underwritten because of current risk profile	19%
Other	7%
Total	170%

Q21. Who in your company is most responsible for cyber risk management? Please select your two top choices.	GLOBAL
CEO/board of directors	4%
Chief financial officer	6%
Business unit (LOB) leaders	15%
Chief information officer	30%
Chief information security officer	15%
Risk management	13%
Procurement	6%
General counsel	7%
Compliance/audit	4%
Other (please select)	1%
Total	100%

Part 3. Role & Organizational Characteristics

D1. What level best describes your current position?	GLOBAL
Senior executive	5%
Vice president	6%
Director	14%
Manager	16%
Supervisor	13%
Technician	9%
Associate/staff	29%
Contractor/consultant	8%
Other	2%
Total	100%

D2. What is the worldwide employee headcount of your company?	GLOBAL
Less than 500	13%
500 to 1,000	18%
1,001 to 5,000	21%
5,001 to 25,000	25%
25,001 to 75,000	14%
More than 75,000	9%
Total	100%

D3. What best describes your company's industry focus?	GLOBAL
Agriculture & food service	2%
Communications	4%
Consumer products	5%
Defense & aerospace	2%
Education & research	5%
Energy & utilities	5%
Entertainment & media	3%
Financial services	19%
Health & pharmaceuticals	11%
Hospitality	3%
Industrial	8%
Other	2%
Public sector	7%
Retail	8%
Services	10%
Technology & software	5%
Transportation	3%
Total	100%

ACKNOWLEDGEMENTS

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

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.