2019 Intangible Assets Financial Statement Impact Comparison Report

GLOBAL EDITION

Sponsored by Aon
Independently conducted by Ponemon Institute LLC
Publication Date: April 2019

Empower Results®

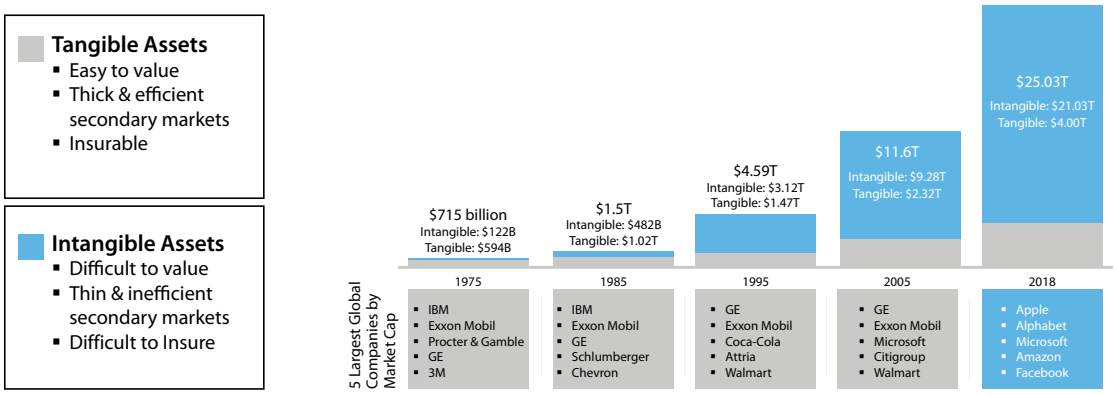
Table of Contents

Part 1. Introduction

The purpose of this research is to compare the relative insurance protection of certain tangible[1] versus intangible assets.[2] How do intangible asset values and potential losses compare to tangible asset values and potential losses from an organization's other perils, such as fires and weather? As technology disruption continues (i.e. 5G, machine learning, artificial intelligence, robotics, cloud computing, Internet of Things/connectedness, quantum computing, Big Data/predictive analytics, and blockchain/distributed ledger), organizations should consider how to develop, maximize, and protect the value of intangible assets.[3a]

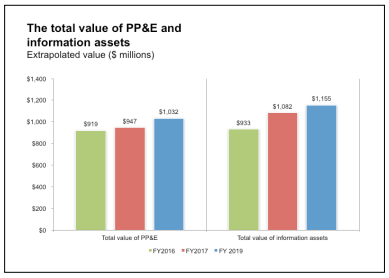
Figure A: Historical Evolution from Tangible to Intangible Assets

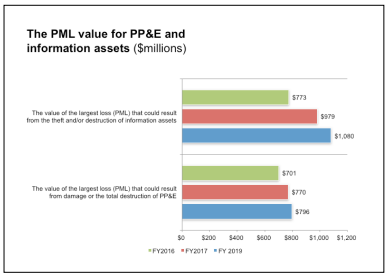
Tangible Assets vs. Intangible Assets for S&P 500 Companies, 1975 – 2018



**Five Largest Global Companies by Market Cap as of December 31, 2018*

Since 2015, Aon and Ponemon Institute have studied the financial statement impact of tangible property and network risk exposures. In this year's research, we have added threats to include intellectual property and what organizations are doing to manage those risks.[3b] 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 from such 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,

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

2 Note that organizations are not solely tangible or intangible asset organizations. For instance, Apple could be considered a manufacturer/retailer, but the figure demonstrates the point that there is a correlation between the investment in intangible assets and market capitalization. ***The S&P 500 Has a Tangible Net Worth Problem***. Stephen Gandel (Bloomberg 17 September 2018) https://www.bloomberg.com/opinion/articles/2018-09-17/s-p-500-has-a-tangible-net-worth-problem. Half of the Fortune 500 companies in 2000 have disappeared. ***Intangible Asset Market Value Study***. http://www.oceantomo.com/intangible-asset-market-value-study/

3a In a March 2019 keynote speech, Lloyd's of London CEO, John Neal, stated: ***"If you looked at a classic S&P 500 company 40 years ago, 83% of their balance sheet would have been tangible assets. Today, it's only 12%. Insurance is pretty good at insuring the tangible, but quite challenged at finding the appropriate covers for the intangible."***

3b In the United States, intellectual property that results from research and development in the regular course of business does not end up on the balance sheet, whereas IP acquired through M&A does end up on the balance sheet through a purchase price allocation process. A better understanding of intangible risks, whether or not they show up on financial statements, is important.

robotic malfunctions and disrupting a country's critical national infrastructure.[4] The 2017 NotPetya and WannaCry incidents demonstrated that business interruption losses can equal or exceed third-party liability losses. Furthermore, business interruption can affect organizations across industries, geographies and sizes, which requires collaboration among multiple lines of insurance to address cyber as a peril in addition to solely stand-alone cyber insurance.[5]

It turns out that organizations need to improve their understanding of the value of information assets.[6] Loss of personally identifiable information is overvalued compared with other information assets.[7] High-value information assets that are proprietary and confidential to an organization[8] include trade secrets and unpublished patent applications.[9] If such information is leaked, deleted or used by a competitor[10] there would be material negative consequences, such as loss of market share, reputational damage,[11] loss of customers and business partners, diminishment of advantage, and the time and expense associated with incident response.[12]

In order to better understand the relative value and risks from the rise of the intangible economy, we must start with a definition of intangible assets and how to measure their value.[13] There is no definitive definition regarding what constitutes an intangible asset. From an accounting perspective, International Accounting Standards 38 states that an intangible asset is an identifiable non-monetary asset without physical substance. The three attributes of an intangible asset are:

- identifiability[14]
- control (power to obtain benefits from the asset)[15]
- future economic benefits (such as revenues or reduced future costs)[16]

The following figure gives examples of some of the categories of intangible assets.[17]

4 In ***Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath***, author Ted Koppel suggests that a catastrophic cyberattack on America's power grid is likely and that we're unprepared. ***Lights Out! Can Insurance Help?*** Kevin Kalinich (Risk & Insurance 2016 January 25) http://www.riskandinsurance.com/lights-can-insurance-help/

5 ***Cyber Perils in a Growing Market.*** https://www.aon.com/unitedkingdom/insights/cyber-perils-in-a-growing-market.jsp. ***The Future of Insurance to Address Cyber Perils.*** Insurance Thought Leadership. http://insurancethoughtleadership.com/future-of-insurance-to-address-cyber-perils/

6 ***Understanding the Value of Information Assets.*** Ponemon Institute Research Report, November 2018. https://cdn2.hubspot.net/hubfs/4009356/Ponemon%20Research/Doc%20Authority%20Report%20Final%207MQ.pdf

7 ***What's Your Intellectual Property Worth? Chances Are You Don't Know.*** https://theonebrief.com/whats-your-intellectual-property-worth-chances-are-you-dont-know/

8 ***It's Time to Prepare for the IP Monetization Revolution.*** (2019 January 21). https://www.iam-media.com/law-policy/ip-monetisation-teeters-brink-disruption.

9 Granted patents are publicly available via the USPTO and commercial databases. Applications are typically confidential for at least an initial period.

10 ***IP Operations Are Facing Increased Risk and Growing Demands.*** https://clarivate.com/wp-content/uploads/2018/06/IP-Operations-Trends-Report.pdf

11 ***Reputation Risk in the Cyber Age: The Impact on Shareholder Value.*** Pentland Analytics. https://www.aon.com/getmedia/2882e8b3-2aa0-4726-9efa-005af9176496/Aon-Pentland-Analytics-Reputation-Report-2018-07-18.pdf

12 ***Understanding the Value of Information Assets.*** Ponemon Institute Research Report, November 2018. https://cdn2.hubspot.net/hubfs/4009356/Ponemon%20Research/Doc%20Authority%20Report%20Final%207MQ.pdf

13 ***Capitalism Without Capital: The Rise of the Intangible Economy.*** Jonathan Haskel and Stian Westlake (Princeton University Press 2018). ***What Ideas Are Worth: The Value of Intellectual Capital and Intangible Assets in the American Economy.*** Kevin Hassett and Robert Shapiro (Sonecon 2011). www.sonecon.com/docs/studies/Value_of_Intellectual_Capital_in_American_Economy.pdf

14 An intangible asset is identifiable when it is capable of being separated and sold, transferred, licensed, rented or exchanged, either individually or together with a related contract; or arises from contractual or other legal rights, regardless of whether those rights are transferable or separable from the entity or from other rights and obligations.

15 ***Why Financial Statements Don't Work for Digital Companies.*** https://www.teampay.co/insights/financial-statements-digital-companies/; https://hbr.org/2018/02/why-financial-statements-dont-work-for-digital-companies

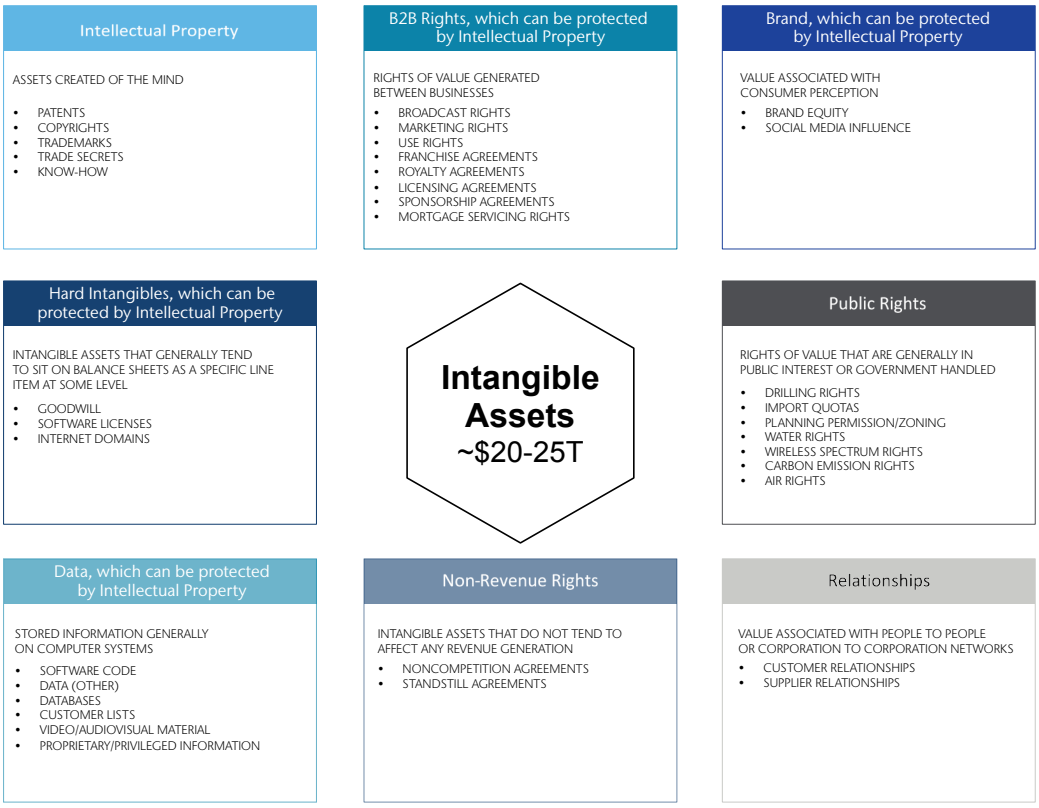
16 Recognition criteria: IAS 38 requires an entity to recognize an intangible asset, whether purchased or self-created (at cost), if and only if it is probable that the future economic benefits that are attributable to the asset will flow to the entity, and the cost of the asset can be measured reliably. The likelihood of economic benefits must be based on reasonable/supportable assumptions about conditions that will exist over the life of the asset.

The probability recognition criterion is considered to be satisfied for intangible assets that are acquired separately or in a business combination.

17 Aon Inpoint data and analytics.

Figure B: Total Value of Intangible Assets in the U.S.

(Aon has identified 35 individual assets in 8 groupings)



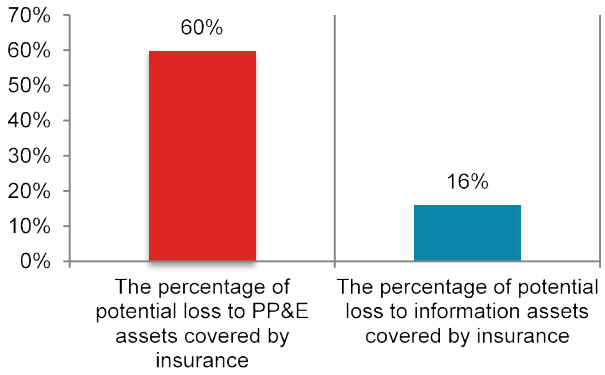
> "The risk industry has to keep up with a constantly evolving environment in a daily battle for relevance. As an industry, we have not kept up with a world where 75 percent of market capitalization is now driven by intangible assets."
>
> *Aon Q3 2018 Earnings call, Greg Case, Aon CEO*

We surveyed 2,348 individuals in North America, Europe, the Middle East, Africa, Asia Pacific, Japan and Latin America 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 (31 percent of respondents) or risk management (28 percent of respondents). Other respondents are in corporate compliance/audit (14 percent of respondents) and general management (11 percent of respondents).

As shown in Figure 1, despite the greater average potential loss to information assets ($1.08 billion) compared with property, plant and equipment (PP&E) ($795 million), the latter has much higher insurance coverage (60 percent vs. 16 percent).[18]

Yet, the return on investment to address intangible assets, in general, and intellectual property assets, specifically, would be much higher than the return on investment with respect to tangible assets.[19]

Figure 1. The percentage of PP&E and information assets covered by insurance



18 ***Airmic: Intangible Assets "Changing Everything" for Risk Managers.*** https://www.insurancebusinessmag.com/us/risk-management/operational/airmic-intangible-assets-changing-everything-for-risk-managers-103570.aspx

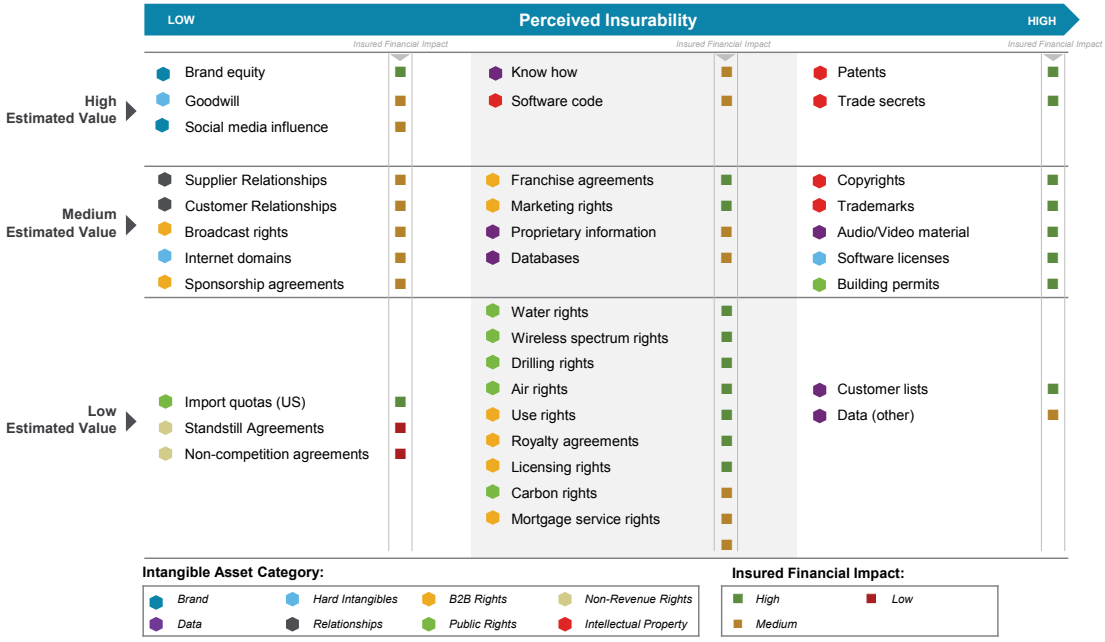
19 *"Today the most valuable assets are more likely to be stored in the cloud than in a warehouse." Inga Beale, Chief Executive Officer of Lloyd's of London. + "Intangible assets are twice as valuable as tangible assets across 19* different industries and represents a substantial portion of many companies' overall value." World Intellectual Property Organization Study and Report. https://www.wipo.int/portal/en/index.html

Figure C: Perceived Level of Insurability[20]

Below is a preliminary organization of identified intangible assets across:

1.Likelihood of insurability
2. Estimated value (potential sums insured)
3. Insured concern

Figure C illustrates an initial view regarding the potential insurability of identified intangibles assets. [1] Intangible asset values, PML and insurability are fluid and dynamic. As intangible asset values and related risks/probable maximum loss/maximum foreseeable loss are better quantified, insurability is likely to evolve.



Consider the following recent intellectual property protection situations.[20] What could be done to protect the assets – maximize the value and minimize the risks – in the following situations?[21]

- Uber's self-driving truck subsidiary, Otto, was accused of stealing trade secrets from Google's autonomous driving subsidiary, Waymo, and settled in February 2018 by providing Google with a $245M equity stake in Uber, all while maintaining its innocence.[22]
- AstroTurf, maker of synthetic grass products, filed for bankruptcy protection in 2016 after a $30 million patent infringement loss to rival product manufacturer Tarkett.[23]
- Kraft Heinz, which combined Kraft Foods and H.J. Heinz in a 2015 merger, wrote down its assets by $15.4 billion on February 21, 2019, including $7.1 billion of goodwill and $8.3 billion in intangible assets (the merger put a $47.8 billion value on intangible assets).

20 ***Estimated values for each "Intangible Asset Category" can vary between "Low," "Medium" and "High" depending upon the unique circumstances of each situation.***

21 ***Benefits of Intellectual Property Insurance.*** http://safeguardip.com/our-products/benefits-of-insurance/

22 https://www.newyorker.com/magazine/2018/10/22/did-uber-steal-googles-intellectual-property

23 https://www.wsj.com/articles/astroturf-files-for-bankruptcy-protection-1467219617

- McDonald's lost its European Union trademark registration for BIG MAC pursuant to a January 2019 decision by the European Union Intellectual Property Office.[24]
- D&O insurer not obligated under a policy exclusion in its directors and officers liability insurance policy to defend a travel agency charged with misappropriating trade data, says a federal district court.[25]
- Amazon health startup trade secrets case: A Massachusetts federal judge ruled February 22, 2019, that a former employee of UnitedHealth unit Optum Inc. can continue his role with a health care startup created by Amazon.com Inc., Berkshire Hathaway Inc. and JPMorgan after a ruling that Optum had not shown the two companies are likely to be rivals anytime soon.[26]

Following are some of the key takeaways from this research:

Companies value information assets slightly higher than they do PP&E.[27] The total value of PP&E is approximately $1.032 million for the companies represented in this research. The average total value of information assets is slightly more than PP&E at $1.155 million .

The value of PML[28] 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 $1,080 million.[29]

In contrast, the value of the largest loss that could result from damage or total destruction of PP&E is approximately $796 million on average. Business disruption has a greater impact on information assets ($299 million)[30] than on PP&E ($138 million).

Insurance coverage is higher for PP&E than information assets. On average, approximately 60 percent of PP&E assets are covered by insurance and approximately 29 percent of PP&E assets are self-insured.[31] An average of only 16 percent of information assets are covered by insurance. Self-insurance is higher for information assets at 62 percent. Further, the likelihood of a loss is higher for information assets than for PP&E.[32]

More than one-third of respondents believe no disclosure of a material loss to information assets is required. Forty-four percent of respondents say their company would disclose a material loss to PP&E or information assets that is not covered by insurance as a footnote disclosure in the financial statement.

24 Maybe John Travolta's Vincent Vega and Samuel L. Jackson's Jules Winnfield can devise a new name for the Big Mac like they did in the film *Pulp Fiction*, when they discussed the fact that in Paris, a Quarter Pounder with Cheese is called a Royale with Cheese due to the metric system.

25 *Benjamin & Brothers LLC v. Scottsdale Indemnity Co.* https://www.businessinsurance.com/article/20190321/NEWS06/912327424/Scottsdale-wins-in-directors-and-officers-litigation-based-on-intellectual-prope

26 https://www.wsj.com/articles/unitedhealth-employee-cleared-to-join-health-venture-of-amazon-berkshire-jpmorgan-11550859259

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

28 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 (e.g., firewalls, nonflammable materials) and proper functioning of most (perhaps not all) active suppression systems (e.g., sprinklers).

29 Baker McKenzie's 2018 Theft Report states that the U.S. Chamber of Commerce suggests that trade secrets value is 1 to 3 percent of GDP. Theft and destruction is a trade secrets exposure. https://insight.bakermckenzie.com/trade-secret-theft-a-trillion-dollar-problem

30 While the survey results suggest probable 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.

31 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.

32 We estimate that the lack of insurance coverage for patent infringement and trade secrets is much higher, since almost all standard non-intellectual property-specific insurance policies exclude coverage. ***Does Your Insurance Policy Cover Your Intellectual Property?*** (2019 February 27) https://www.iam-media.com/does-your-insurance-policy-cover-your-intellectual-property

Almost half of companies had a material or significantly disruptive security exploit or data breach one or more times in the past 24 months.[33] Almost half (48 percent of respondents) report their company had such a security incident. The average total financial impact of these incidents was $4.9 million.[34] Sixty-five percent of these respondents say the incident increased their company's concerns over cyber liability.

Despite the extent of cyber risk, only 28 percent of respondents say their companies currently have cyber insurance coverage with an average limit of $17 million. Fifty-eight percent of these respondents believe this insurance is sufficient with respect to coverage terms and conditions, exclusions, retentions, limits and insurance carrier financial security.

Cyber liability and intellectual property risks rank in the top 10 of all business risks facing companies. Eight-six percent of respondents consider a cyber risk as the number one or two business risk (19 percent of respondents), in the top five (34 percent of respondents) or in the top 10 (33 percent of respondents). Similarly, 81 percent of respondents rate the risk to their company's intellectual property in the top 10 of all business risks.

In the past two years, 28 percent of respondents say their company experienced a material IP event.[35] Most of these incidents involved infringements of, or challenges to, the company's IP (69% of respondents), with a smaller percentage arising from the company's alleged infringement of third-party IP (31%). Company experience also differed based upon the type of IP at issue, with most of these incidents involving trade secrets (42 percent of respondents).[36] Fewer events involved copyrights and patents (26 percent and 24 percent of respondents, respectively). Companies represented in this research estimate that the average total value of their IP assets such as trademarks, patents, copyrights, trade secrets and know-how is $473 million.

Most companies' insurance policy does not cover all the consequences of an IP event.[37] Only 37 percent of respondents say it covers a challenge to their company's IP assets. Thirty-four percent of respondents say the policy covers third-party infringement of their company's IP assets and 33 percent of respondents say it covers an allegation that their company is infringing third-party IP rights. More than one-third of respondents say the policy does not cover IP events.

33 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.

34 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.

35 According to Figure 24, the event can be described as an infringement of company rights (40 percent of respondents), allegation of company infringement of third-party rights (31 percent of respondents) or a challenge to company rights (29 percent of respondents).

36 One in five companies think or know they have had trade secrets stolen. Baker McKenzie 2018 Theft Report. https://insight.bakermckenzie.com/trade-secret-theft-a-trillion-dollar-problem

As a complement to a cyber risk policy, few companies have a trade secret theft insurance policy and/or an intellectual property liability policy. Only 24 percent of respondents say they have a trade secret theft insurance policy and a similar percentage of respondents (30 percent) have an intellectual property liability policy. However, there is significant interest in purchasing such policies.[37]

37 We estimate that the lack of insurance coverage for patent infringement and trade secrets is much higher, since almost all standard non-intellectual property-specific insurance policies exclude coverage. ***Does Your Insurance Policy Cover Your Intellectual Property?*** (2019 February 27) https://www.iam-media.com/does-your-insurance-policy-cover-your-intellectual-property

Part 2. Key findings

This report features the consolidated findings of all regions in this research. 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.[38] The complete audited findings are presented in the appendix of this report. We have organized the report according to the following topics:

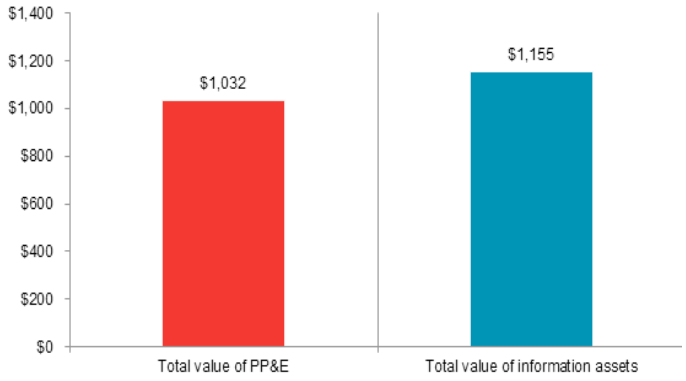
- Differences between the valuation and PML of PP&E and information assets
- The cyber risk experience of companies
- Perceptions about the financial impact of cyber exposures
- The cyber risk to intellectual property

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

Companies value information assets slightly higher than they do PP&E.[39] According to Figure 2, on average, the total value of PP&E, including all fixed assets plus SCADA and industrial control systems, is approximately $1,032 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, model methods and other intellectual properties, is slightly more than PP&E at $1,155 million .

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

Extrapolated value ($ millions)



The value of PML[40] 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 $1,080 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 $796 million on average. This also assumes the normal functioning of passive protective features such as firewalls, nonflammable materials and raised flooring, and active suppression systems such as fire sprinklers.

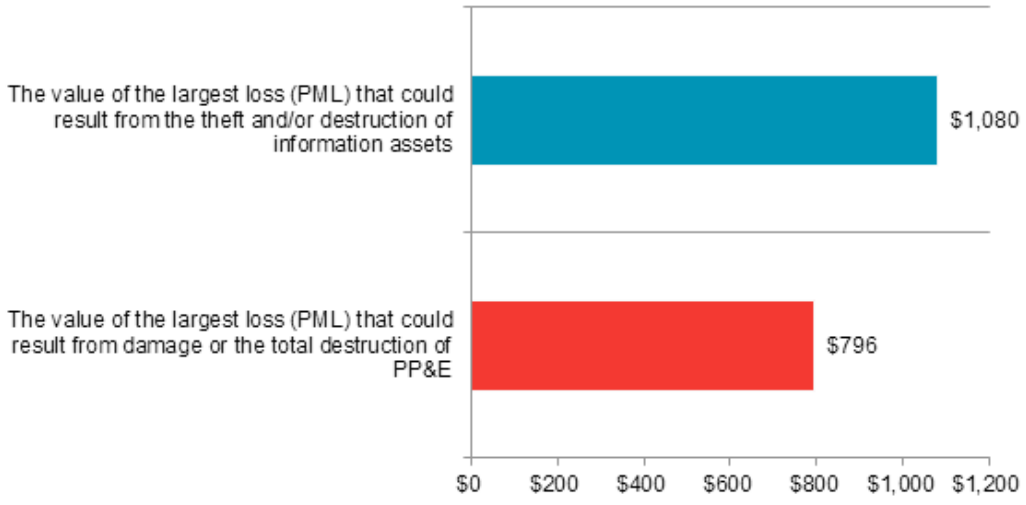
38 Source: Institute of Risk Management.

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

40 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 (e.g., firewalls, nonflammable materials, etc.) and proper functioning of most (perhaps not all) active suppression systems (e.g, sprinklers).

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

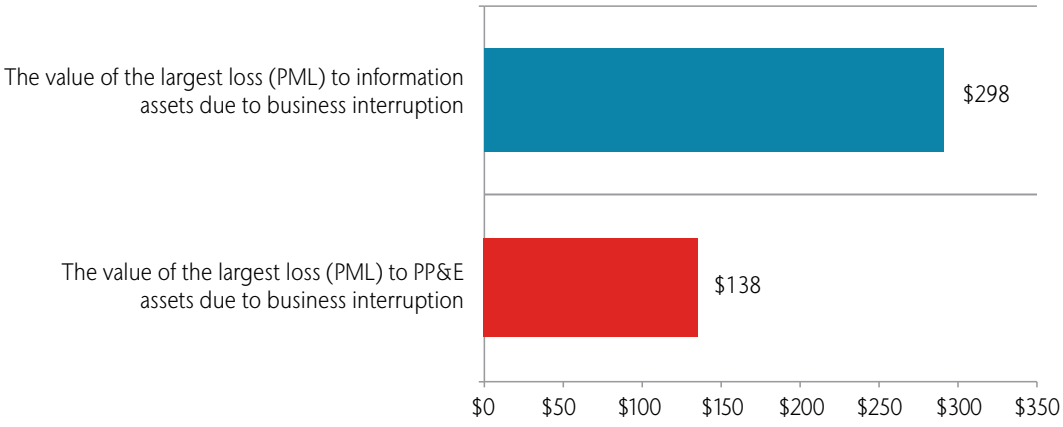
Extrapolated value ($ millions)



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 ($299 million)[41] than on PP&E ($138 million).

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

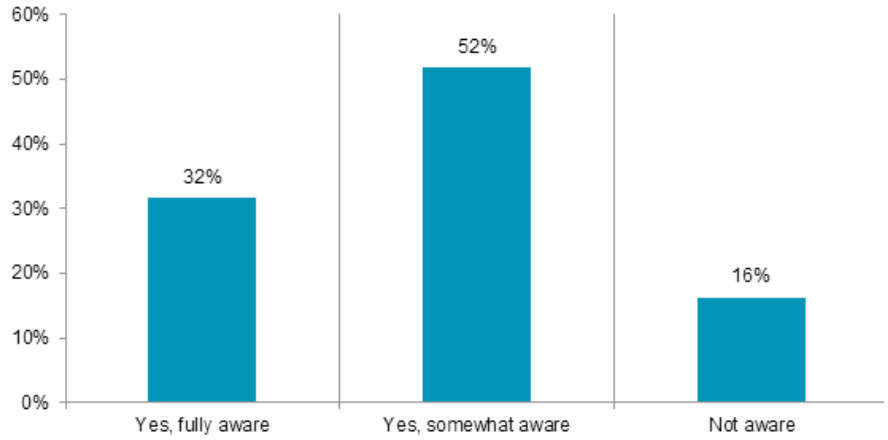
Extrapolated value ($ millions)



41 While the survey results suggest probable 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.

Awareness of the economic and legal consequences from an international data breach or security exploit is low. As revealed in Figure 5, only 32 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 16 percent say they are not aware of the consequences.

Figure 5. Awareness of the economic and legal consequences from an international data breach or security exploit

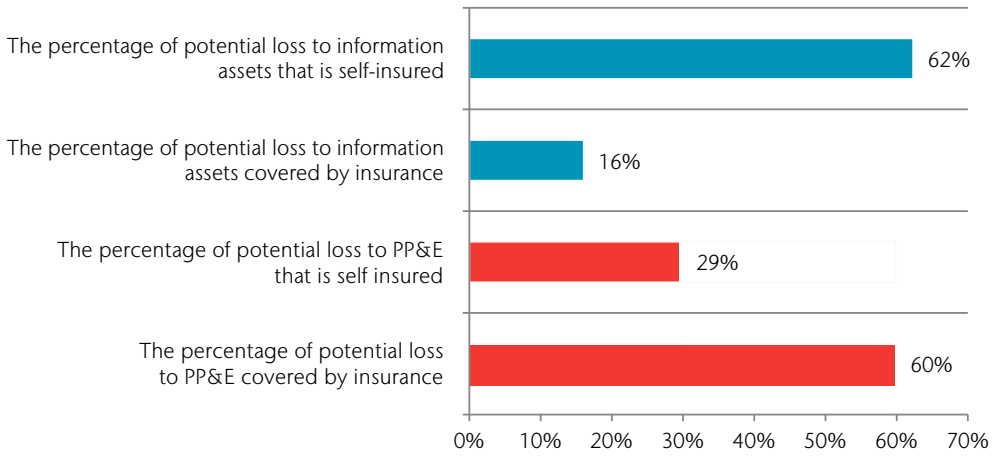


There is a significant difference between the insurance coverage of PP&E and information assets. On average, approximately 60 percent of PP&E assets are covered by insurance and approximately 29 percent of PP&E assets are self-insured (Figure 6).[42] An average of only 16 percent of information assets are covered by insurance. Self-insurance is higher for information assets at 62 percent.

42 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.

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

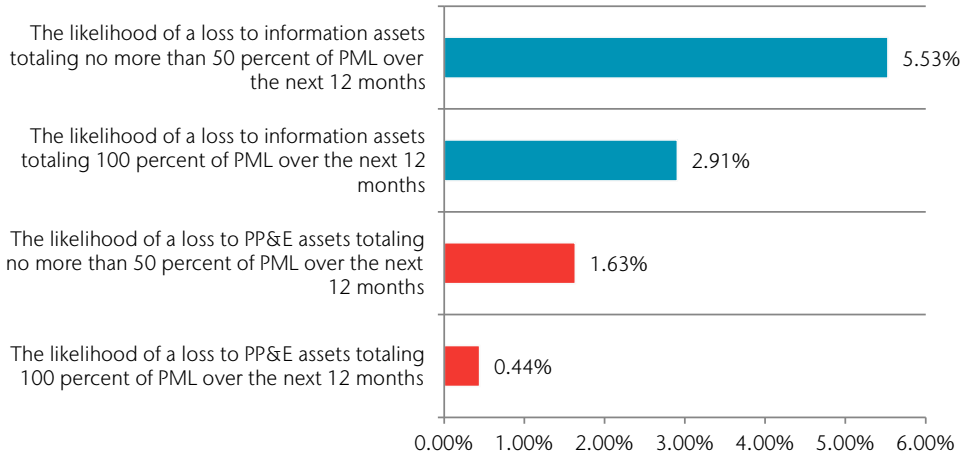
Extrapolated percentage



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 5.5 percent and 100 percent of PML at 2.9 percent, as shown in Figure 7. 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 1.6 percent and at 100 percent of PML it is 0.44 percent.

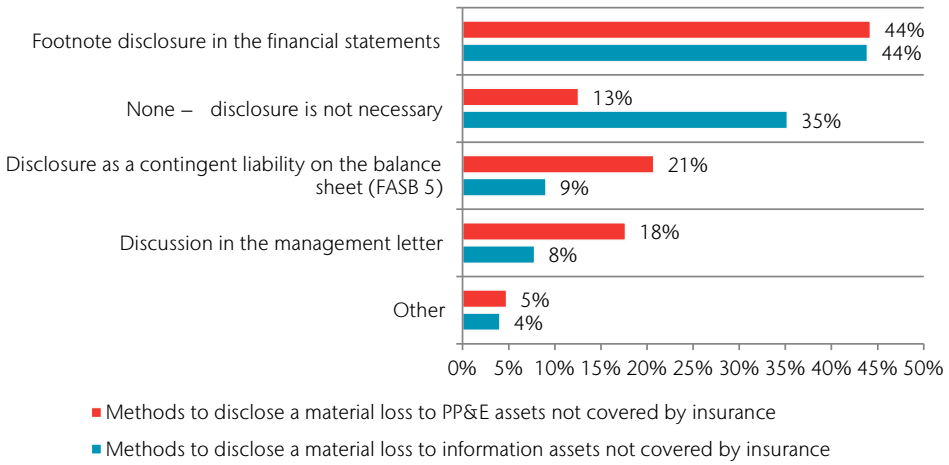
Figure 7. Likelihood of loss to PP&E and information assets totaling more than 50 percent and 100 percent of PML over the next 12 months

Extrapolated percentage



More than one-third of respondents believe no disclosure of a material loss to information assets is required. Figure 8 focuses on how companies would disclose a material loss. Forty-four 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 (21 percent of respondents). Forty-four percent say they would disclose a material loss to information assets as a footnote disclosure in the financial statements, but 35 percent of respondents do not believe disclosure is necessary.

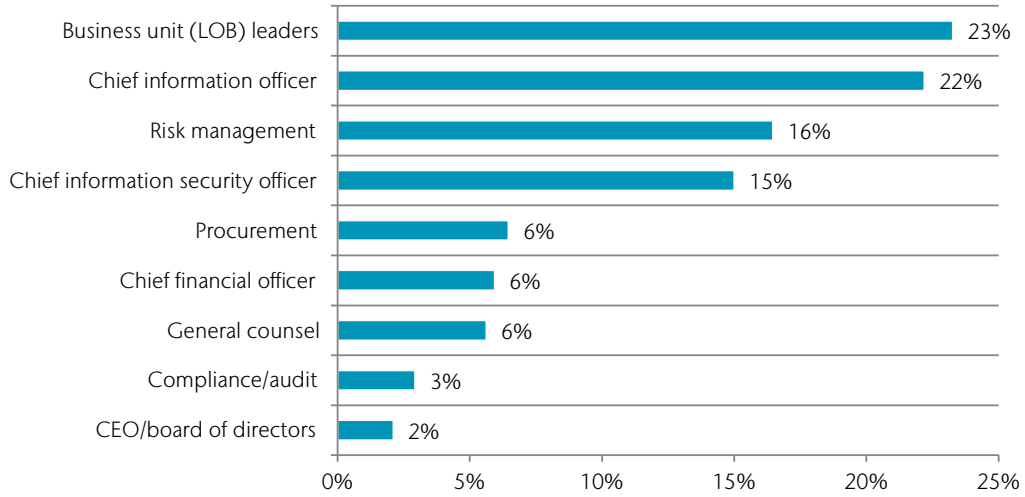
Figure 8. How would your company disclose a material loss to PP&E and information assets?



The cyber risk experience of companies

Responsibility for cyber risk management is dispersed throughout the organization. As shown in Figure 9, no one function is clearly responsible for managing cyber risks in their organizations. The top two are business unit leaders (23 percent of respondents) and the chief information officer (22 percent of respondents)

Figure 9. Who is most responsible for cyber risk management?

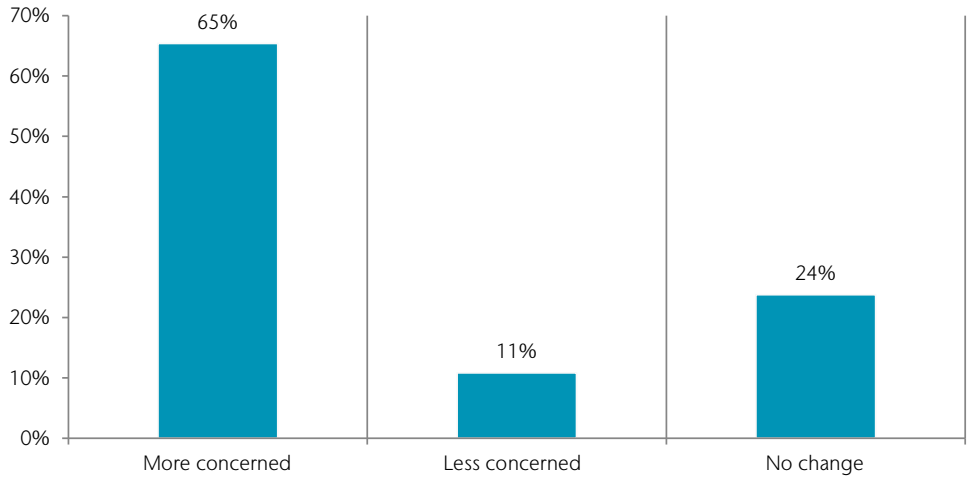


Almost half of companies had a material or significantly disruptive security exploit or data breach one or more times in the past 24 months.[43] Almost half (48 percent of respondents) report their company had such a security incident. The average total financial impact of these incidents was $4.9 million.[44] According to Figure 10, 65 percent of these respondents say the incident increased their company's concerns over cyber liability.

43 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.

44 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.

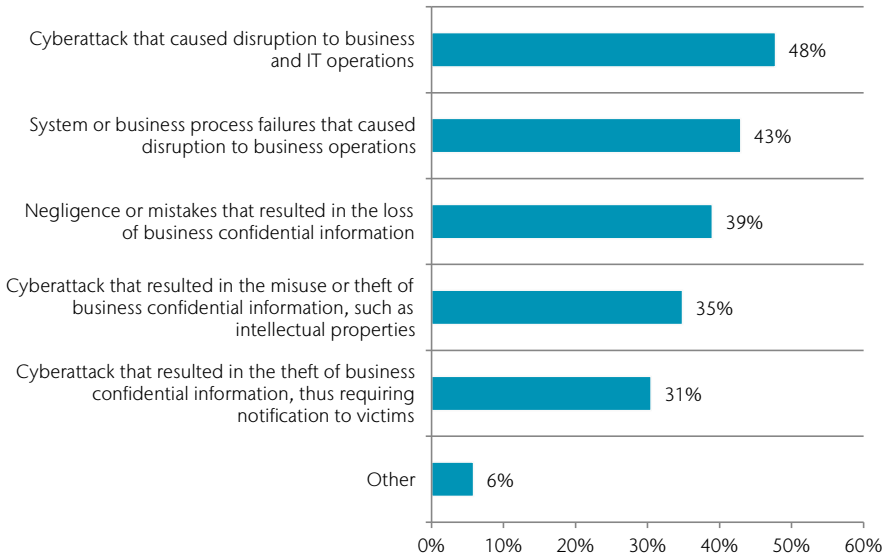
Figure 10. How did the security exploit or data breach affect your company's concerns over cyber liability?



The types of security incidents that 46 percent of the companies in this research faced are displayed in Figure 11. The most frequent type of incident was one that caused disruption to business and IT operations (48 percent of respondents) or resulted in a system or business process failure that caused disruption to business operations (43 percent of respondents). This is followed by 39 percent of respondents, who say the cyberattack 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?

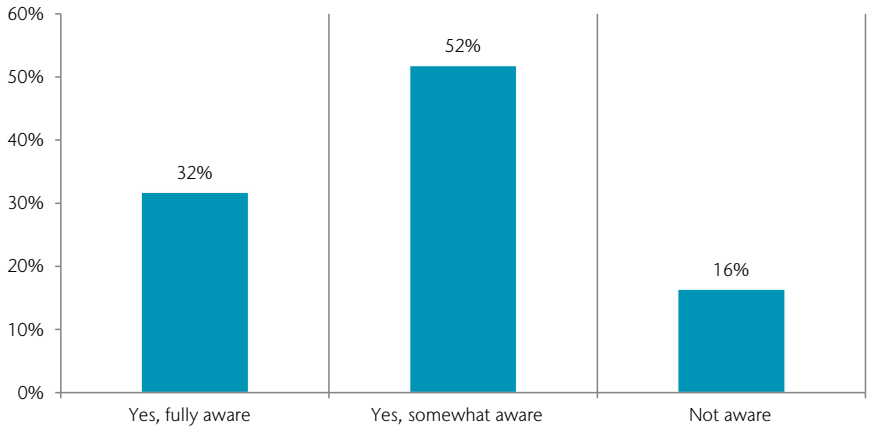
More than one response permitted



Perceptions about the financial impact of cyber exposures

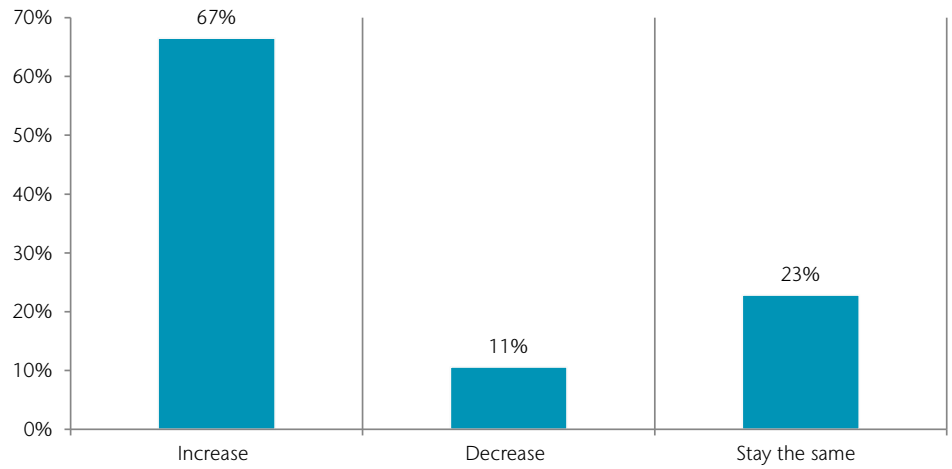
Awareness of the economic and legal consequences from an international data breach or security exploit is low. As revealed in Figure 12, only 32 percent of respondents are fully aware of the consequences that could result from a data breach or security exploit in other countries in which their company operates and 16 percent say they are not aware of the consequences.

Figure 12. Awareness of the economic and legal consequences from an international data breach or security exploit



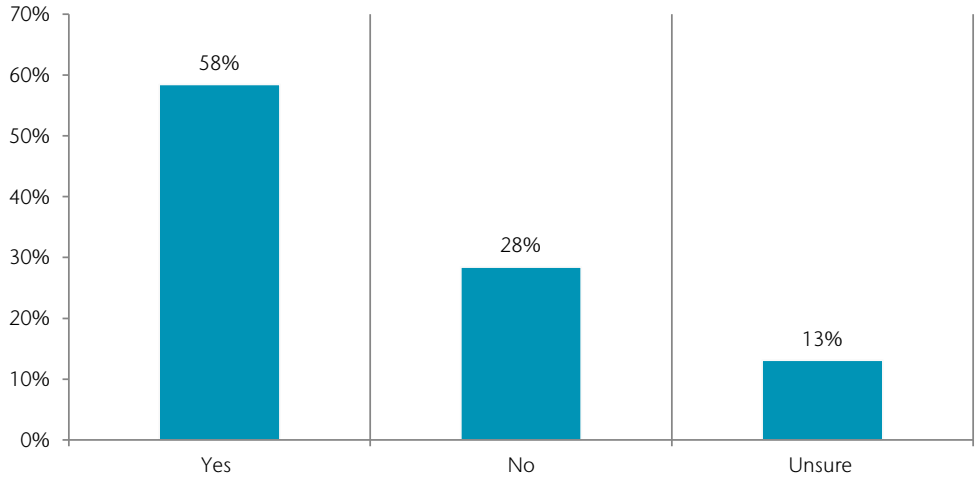
Companies' exposure to cyber risk is expected to increase. However, 38 percent of respondents say there is no plan to purchase cyber insurance. As the data in Figure 13 show, 67 percent of respondents believe their company's exposure to cyber risk will increase and 23 percent of respondents say it will stay the same. Only 11 percent of respondents expect it to actually decrease.

Figure 13. 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 28 percent of respondents say their companies currently have cyber insurance coverage with an average limit of $17 million. As Figure 14 reveals, 58 percent of these respondents believe this insurance is sufficient with respect to coverage terms and conditions, exclusions, retentions, limits and insurance carrier financial security.

Figure 14. Is your company's cyber insurance coverage sufficient?



According to Figure 15, the adequacy of coverage is determined mainly by a formal risk assessment by third party (24 percent of respondents) or policy terms and conditions reviewed by a third-party specialist (20 percent of respondents). Only 14 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 15. How companies determine the adequacy of coverage

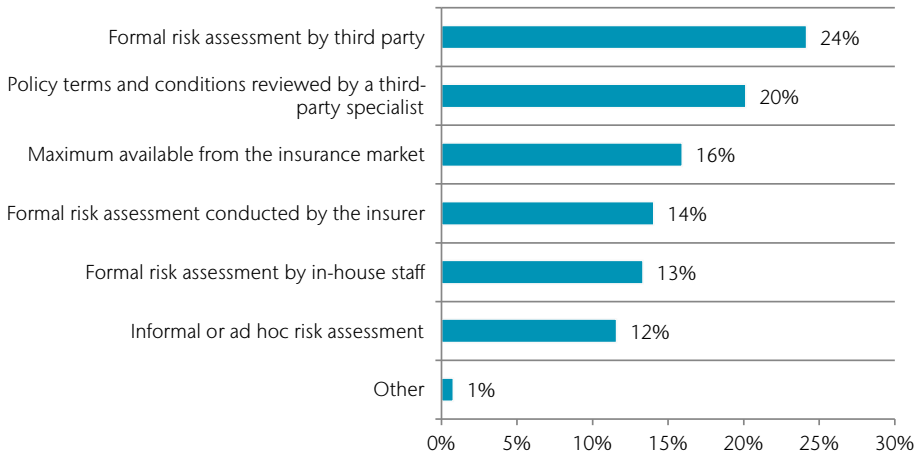
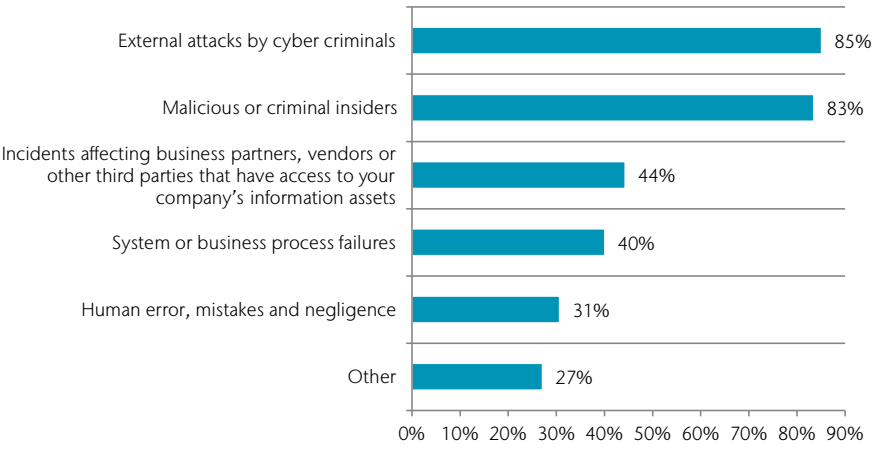


Figure 16 displays the incidents typically covered by cyber insurance. Most incidents covered involve external attacks by cybercriminals (85 percent of respondents), malicious or criminal insiders (83 percent of respondents), and incidents affecting business partners, vendors or other third parties that have access to their company's information assets (44 percent of respondents).

Figure 16. Types of incidents covered by cyber insurance

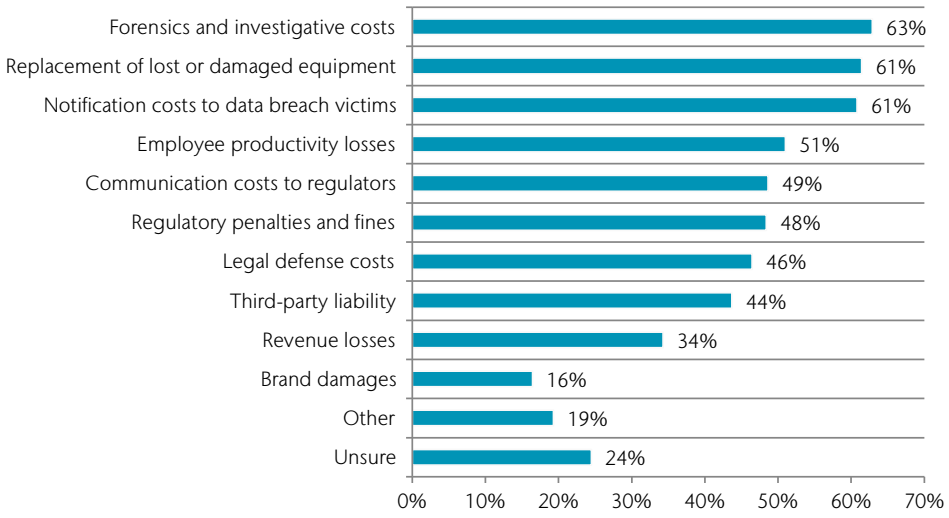
More than one response permitted



Figures 17 and 18 present the coverage and services provided by insurance companies. The top five costs covered are: forensics and investigative costs (63 percent of respondents), replacement of lost or damaged equipment (61 percent of respondents), data breach notification costs (61 percent of respondents), employee productivity losses (51 percent of respondents) and communication costs to regulators (49 percent of respondents).

Figure 17. Coverage provided by the insurance company

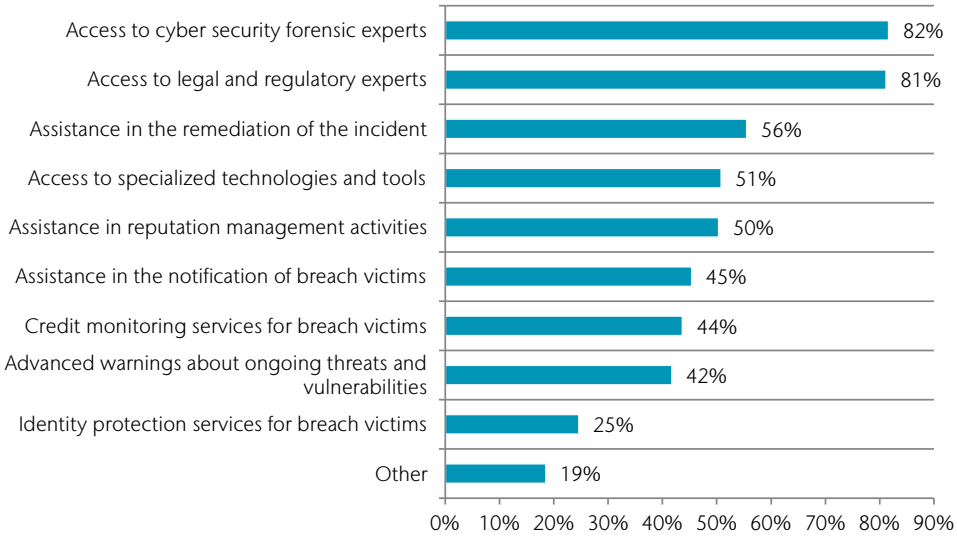
More than one response permitted



In addition to this coverage, other services provided are access to cybersecurity forensic experts (82 percent of respondents), access to legal and regulatory experts (81 percent of respondents), assistance in the remediation of the incident (56 percent of respondents), access to specialized technologies and tools (51 percent of respondents), and assistance in reputation management activities (50 percent of respondents), as shown in Figure 18.

Figure 18. Other services provided by the cyber insurer

More than one response permitted

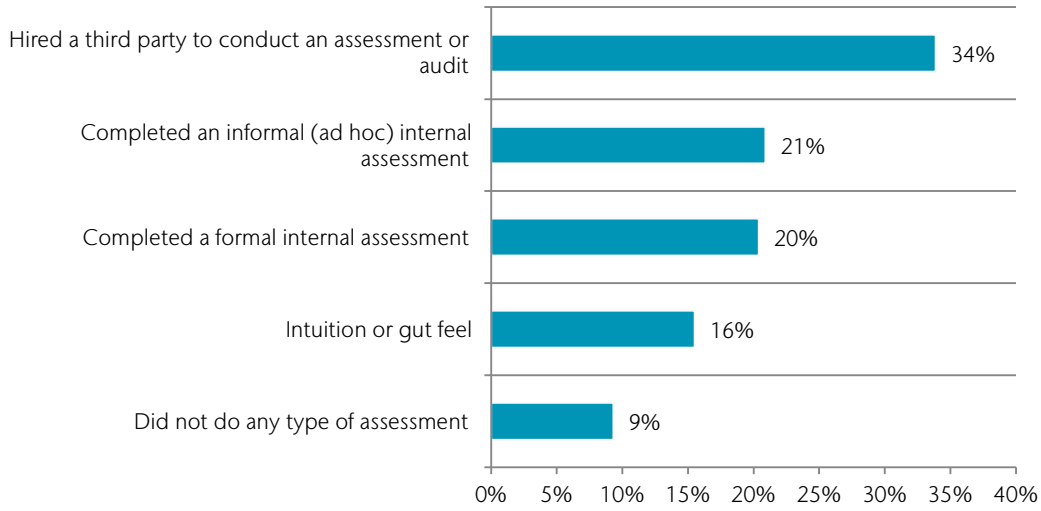


Cyber liability and IP risks rank in the top 10 of all business risks facing companies. Figure 19 demonstrates that 86 percent of respondents consider a cyber risk as the number one or two business risk (19 percent of respondents), in the top five (34 percent of respondents) or in the top 10 (33 percent of respondents). Similarly, 81 percent of respondents rate the risk to their company's intellectual property (IP) in the top 10 of all business risks.

Figure 19. How do cyber and IP risks compare to other business risks?

To determine the cyber risk to their company, 34 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 20). Only 20 percent of respondents say their company completed a formal internal assessment, but 16 percent of respondents say it was intuition or gut feel.

Figure 20. How did you determine the level of cyber risk to your company?

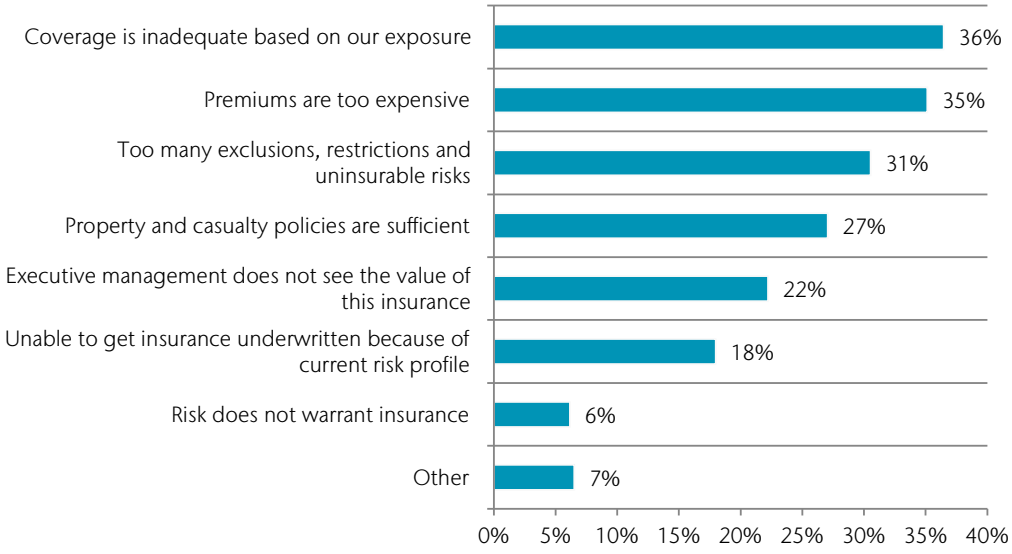


Most companies are postponing the purchase of cyber insurance. As discussed previously, 38 percent of respondents say their company has no plans to purchase cyber insurance. Only 16 of respondents say their company will purchase cyber insurance in the next 12 months. Almost half of respondents (46 percent) say they will purchase cyber insurance in the next 24 months (25 percent) or more than 24 months (21 percent).

According to Figure 21, the main reasons for not purchasing cyber security insurance are: coverage is inadequate based on their exposure (36 percent of respondents), premiums are too expensive (35 percent of respondents), and there are too many exclusions, restrictions and uninsurable risks (31 percent of respondents).

Figure 21. What are the main reasons why your company will not purchase cybersecurity insurance?

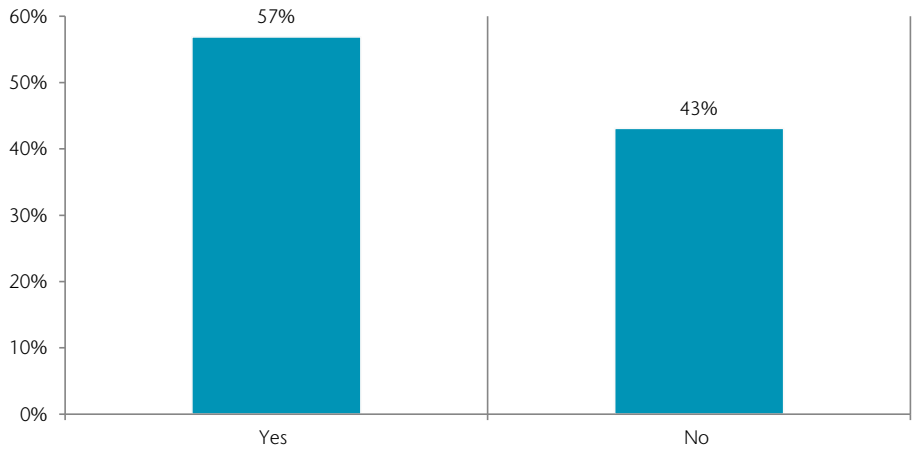
More than one response permitted



Cyber risks to intellectual property (IP)

The majority of companies have a strategy to manage risks to IP. Companies represented in this research estimate that the average total value of their IP assets, such as trademarks, patents, copyrights, trade secrets and know-how, is $473 million. As shown in Figure 22, 57 percent of respondents say their enterprise risk management activities include risks to their IP.

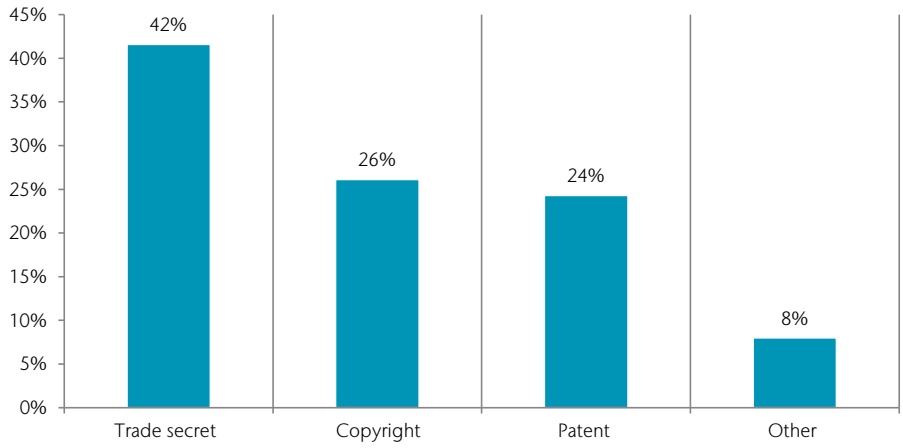
Figure 22. Do your company's enterprise risk management activities include risks to IP?



In the past two years, 28 percent of respondents say their company experienced a material IP event.

According to Figure 23, most of these incidents involved trade secrets (42 percent of respondents). Fewer events involved copyrights and patents (26 percent and 24 percent of respondents, respectively).

Figure 23. What type of IP assets were involved in a material IP event?



In this section, respondents were asked to refer to the most recent IP event that occurred over the past 24 months. According to Figure 24, the event can be described as an infringement of company rights (40 percent of respondents), allegation of company infringement of third-party rights (31 percent of respondents) or challenge to company rights (29 percent of respondents).

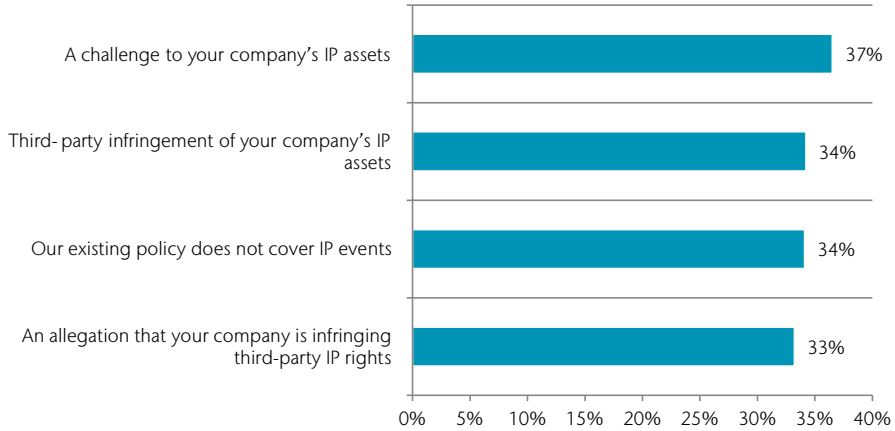
Figure 24. What best describes the event?

Only 1 response permitted

Most companies' insurance policy does not cover all the consequences of an IP event. According to Figure 25, only 37 percent of respondents say it covers a challenge to their company's IP assets. Thirty-four percent of respondents say the policy covers third-party infringement of their company's IP assets and 33 percent of respondents say it covers an allegation that their company is infringing third-party IP rights. More than one-third of respondents say the policy does not cover IP events.

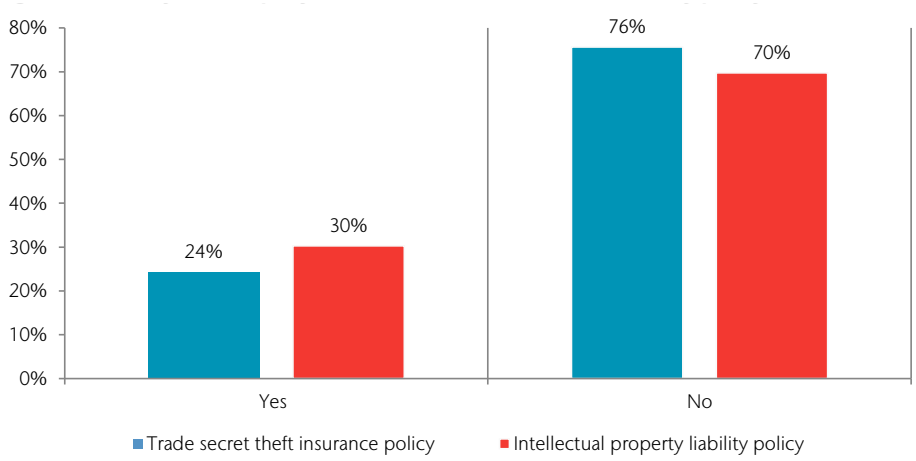
Figure 25. Does your company's existing insurance policy cover any of the following IP events?

More than one response permitted



As a complement to a cyber risk policy, few companies have a trade secret theft insurance policy and/or an intellectual property liability policy. As shown in Figure 26, only 24 percent of respondents say they have a trade secret theft insurance policy and a similar percentage of respondents (30 percent) have an intellectual property liability policy.

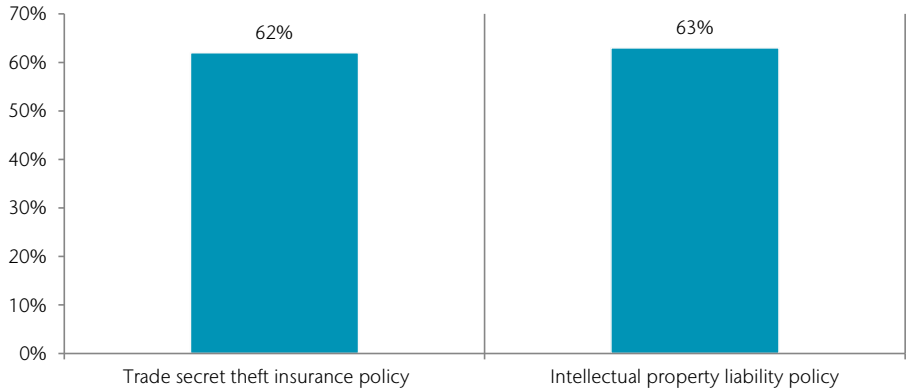
Figure 26. Does your company have a trade secret and/or IP liability policy?



While most companies do not have specific IP insurance policies, there is significant interest in purchasing them. According to Figure 27, 62 percent and 63 percent of respondents are very interested or interested in purchasing a trade secret and/or an IP liability policy, respectively.

Figure 27. If no, what is your company's level of interest in purchasing a trade secret theft insurance policy and/or an IP liability policy?

Very interested and Interested responses combined



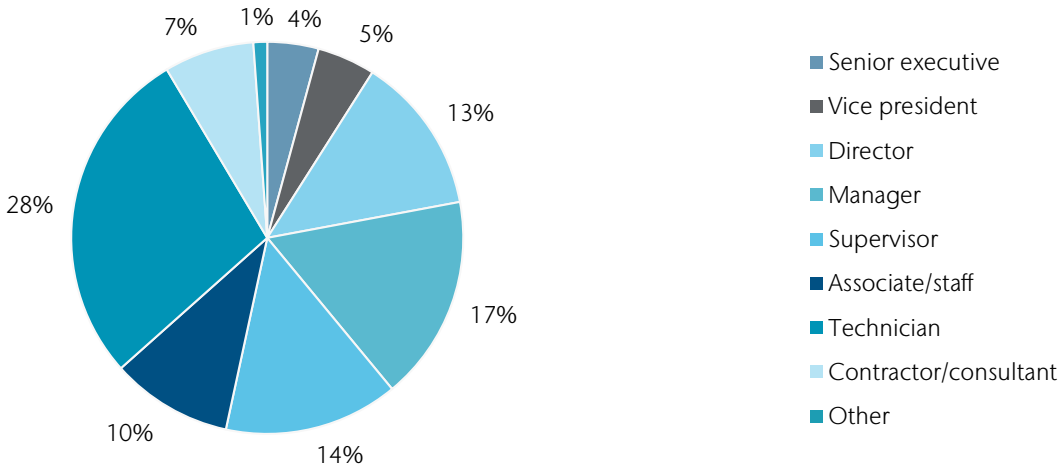
Part 3. Methods

The consolidated sampling frame is composed of 60,517 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, 2,619 respondents completed the survey, of which 271 were rejected for reliability issues. The final sample consisted of 2,348 surveys, a 3.9 percent response rate.

Table1.Sampleresponse	Frequency	Percentage
Totalsamplingframe	60,517	100.0%
Totalreturns	2,619	4.3%
Rejectedorscreenedsurveys	271	0.4%
Finalsample	2,348	3.9%

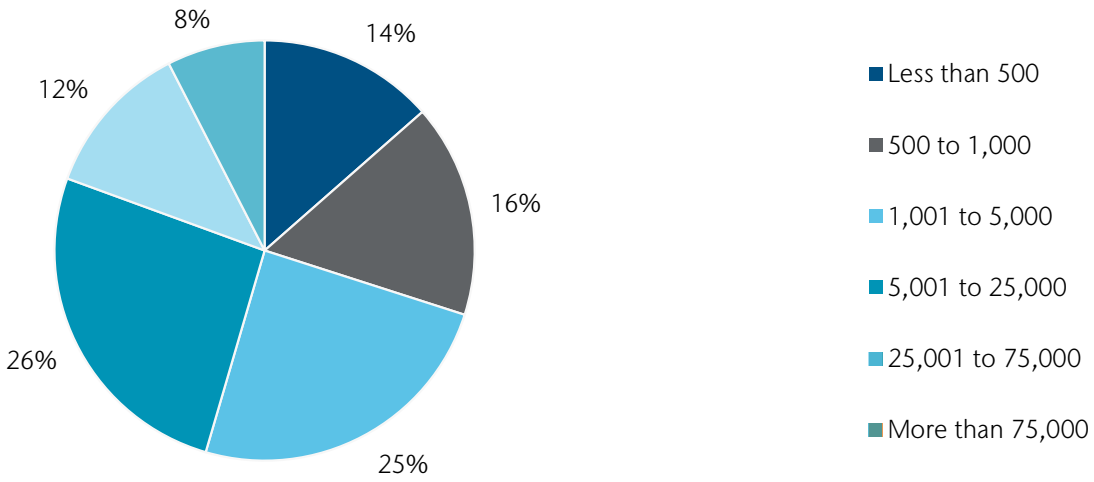
Pie Chart 1 reports the current position or organizational level of the respondents. Approximately half of the respondents (53 percent) reported their current position as supervisory level or above and 28 percent of respondents reported their current position level as technician.

Pie Chart 1. Current position or organizational level



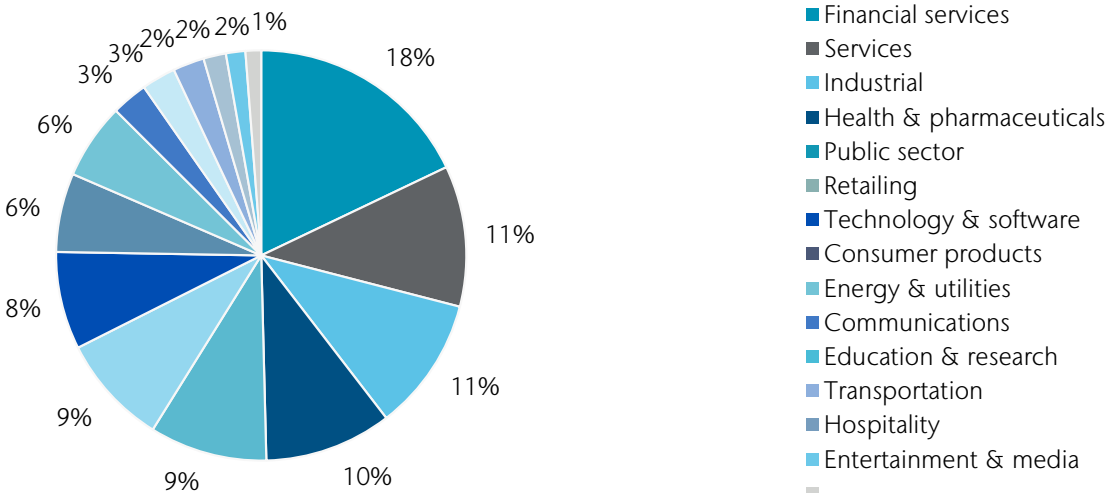
As Pie Chart 2 reveals, 70 percent of the respondents are from organizations with a global head count of more than 1,000 employees.

Pie Chart 2. Worldwide head count of the organization



Pie Chart 3 reports the primary industry classification of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by services (11 percent of respondents), industrial (11 percent of respondents), and health and pharmaceuticals (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.

Nonresponse 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 nonresponse 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 December 2018.

Survey response	FY2019
Sampling frame	60,517
Total returns	2,619
Rejected surveys	271
Final sample	2,348
Response rate	3.9%

Screening questions

S1. How familiar are you with cyber risks facing your company today?	FY 2019
Very familiar	23%
Familiar	36%
Somewhat familiar	42%
Not familiar [stop]	0%
Total	100%

S2. Are you involved in your company's cyber risk management activities?	FY 2019
Yes, significant involvement	33%
Yes, some involvement	67%
No involvement [stop]	0%
Total	100%

S3. What best defines your role?	FY 2019
Risk management	28%
Finance, treasury & accounting	31%
Corporate compliance/audit	14%
Security/information security	10%
General management	11%
Legal (OGC)	7%
None of the above [stop]	0%
Total	100%

S4. Are you involved in your company's enterprise risk management activities?	FY 2019
Yes, significant involvement	39%
Yes, some involvement	61%
No involvement [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).	FY2019
Less than $1 million	3%
$1 to 10 million	10%
$11 to 50 million	13%
$51 to 100 million	23%
$101 to 500 million	26%
$501 to 1 billion	14%
$1 to 10 billion	7%
More than $10 billion	4%
Total	100%
Extrapolated value (US$ millions)	1,031.68

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.	FY2019
Lessthan$1million	5%
$1to10million	11%
$11to50million	16%
$51to100million	25%
$101to500million	23%
$501to1billion	11%
$1to10billion	7%
Morethan$10billion	2%
Total	100%
Extrapolatedvalue(US$millions)	795.56

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.	FY 2019
Less than $1 million	12%
$1 to 10 million	25%
$11 to 50 million	26%
$51 to 100 million	21%
$101 to 500 million	11%
$501 to 1 billion	3%
$1 to 10 billion	1%
More than $10 billion	0%
Total	100%
Extrapolated value (US$ millions)	138.19

Q3. What percentage of this potential loss to PP&E assets is covered by insurance, including captives reinsured but not including captives not reinsured?	FY 2019
Less than 5%	0%
5% to 10%	2%
11%to 20%	3%
21% to 30%	7%
31% to 40%	8%
41% to 50%	11%
51% to 60%	18%
61% to 70%	16%
71% to 80%	14%
81% to 90%	12%
91% to 100%	10%
Total	100%
Extrapolated value	60%

Q4. What percentage of this potential loss to PP&E assets is self-insured, including captives not reinsured?	FY 2019
Less than 5%	11%
5% to 10%	14%
11% to 20%	14%
21% to 30%	17%
31% to 40%	14%
41% to 50%	14%
51% to 60%	6%
61% to 70%	7%
71% to 80%	2%
81% to 90%	1%
91% to 100%	0%
Total	100%
Extrapolated value	29%

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?	FY 2019
Less than 0.1%	22%
0.1% to 0.5%	17%
0.6% to 1.0%	15%
1.1% to 2.0%	14%
2.1% to 3.0%	16%
3.1% to 4.0%	8%
4.1% to 5.0%	5%
5.1% to 10.0%	1%
More than 10.0%	2%
Total	100%
Extrapolated value	1.6%

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?	FY 2019
Less than 0.1%	71%
0.1% to 0.5%	14%
0.6% to 1.0%	8%
1.1% to 2.0%	2%
2.1% to 3.0%	2%
3.1% to 4.0%	1%
4.1% to 5.0%	1%
5.1% to 10.0%	1%
More than 10.0%	0%
Total	100%
Extrapolated value	0.44%

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?	FY 2019
Disclosure as a contingent liability on the balance sheet (e.g., FASB 5)	21%
Footnote disclosure in the financial statements	44%
Discussion in the management letter	18%
None – disclosure is not necessary	13%
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.	FY 2019
Less than $1 million	6%
$1 to 10 million	7%
$11 to 50 million	12%
$51 to 100 million	24%
$101 to 500 million	23%
$501 to 1 billion	14%
$1 to 10 billion	7%
More than $10 billion	6%
Total	98%
Extrapolated value (US$ millions)	1,154.73

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.	FY 2019
Less than $1 million	8%
$1 to 10 million	12%
$11 to 50 million	14%
$51 to 100 million	23%
$101 to 500 million	18%
$501 to 1 billion	12%
$1 to 10 billion	8%
More than $10 billion	5%
Total	100%
Extrapolated value (US$ millions)	1,080.04

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.	FY 2019
Less than $1 million	17%
$1 to 10 million	24%
$11 to 50 million	20%
$51 to 100 million	14%
$101 to 500 million	11%
$501 to 1 billion	7%
$1 to 10 billion	4%
More than $10 billion	0%
Total	97%
Extrapolated value (US$ millions)	298.61

Q10. What percentage of this potential loss to information assets is covered by insurance, including captives reinsured but not including captives not reinsured?	FY 2019
Less than 5%	30%
5% to 10%	32%
11% to 20%	14%
21% to 30%	6%
31% to 40%	6%
41% to 50%	4%
51% to 60%	3%
61% to 70%	2%
71% to 80%	2%
81% to 90%	1%
91% to 100%	0%
Total	100%
Extrapolated value	16%

Q11. What percentage of this potential loss to information assets is self-insured, including captives not reinsured?	FY 2019
Less than 5%	0%
5% to 10%	2%
11% to 20%	2%
21% to 30%	2%
31% to 40%	6%
41% to 50%	11%
51% to 60%	18%
61% to 70%	22%
71% to 80%	21%
81% to 90%	11%
91% to 100%	6%
Total	100%
Extrapolated value	62%

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?	FY 2019
Less than 0.1%	2%
0.1% to 0.5%	2%
0.6% to 1.0%	5%
1.1% to 2.0%	8%
2.1% to 3.0%	10%
3.1% to 4.0%	15%
4.1% to 5.0%	17%
5.1% to 10.0%	21%
More than 10.0%	21%
Total	100%
Extrapolated value	5.5%

Q13. What is the likelihood your company will sustain a loss to information assets totaling 100 percent of PML over the next 12 months?	FY 2019
Less than 0.1%	10%
0.1% to 0.5%	9%
0.6% to 1.0%	11%
1.1% to 2.0%	13%
2.1% to 3.0%	16%
3.1% to 4.0%	15%
4.1% to 5.0%	15%
5.1% to 10.0%	9%
More than 10.0%	3%
Total	100%
Extrapolated value	2.9%

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?	FY 2019
Disclosure as a contingent liability on the balance sheet (FASB 5)	9%
Footnote disclosure in the financial statements	44%
Discussion in the management letter	8%
None – disclosure is not necessary	35%
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, 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?	FY 2019
Yes, fully aware	32%
Yes, somewhat aware	52%
Not aware	16%
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.	FY 2019
Yes	48%
No [skip to Q17]	52%
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.	FY 2019
Cyberattack that caused disruption to business and IT operations (such as denial of service attacks)	48%
Cyberattack that resulted in the theft of business confidential information, thus requiring notification to victims	31%
Cyberattack that resulted in the misuse or theft of business confidential information, such as intellectual properties	35%
Negligence or mistakes that resulted in the loss of business confidential information	39%
System or business process failures that caused disruption to business operations (e.g., software updates)	43%
Other	6%
Total	201%

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.	FY 2019
Zero	0%
Less than $10,000	8%
$10,001 to $100,000	8%
$100,001 to $250,000	17%
$250,001 to $500,000	22%
$500,001 to $1,000,000	16%
$1,000,001 to $5,000,000	11%
$5,000,001 to $10,000,000	9%
$10,000,001 to $25,000,000	5%
$25,000,001 to $50,000,000	3%
$50,00,001 to $100,000,000	2%
More than $100,000,000	0%
Total	100%
Extrapolated value	4,861,079

Q16d. If yes, how has the above security exploit or data breach changed your company's concerns about cyber liability?	FY 2019
More concerned	65%
Less concerned	11%
No change	24%
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?	FY 2019
Increase	67%
Decrease	11%
Stay the same	23%
Total	100%

Q18a. From a business risk perspective, how do cyber risks compare to other business risks? Please select one best choice.	FY 2019
Cyber liability is the number 1 or 2 business risk for my company	19%
Cyber liability is a top 5 business risk for my company	34%
Cyber liability is a top 10 business risk for my company	33%
Cyber liability is not in the top 10 of business risks for my company	14%
Total	100%

Q18b. How did you determine the level of cyber risk to your company?	FY 2019
Completed a formal internal assessment	20%
Completed an informal (ad hoc) internal assessment	21%
Hired a third party to conduct an assessment or audit	34%
Intuition or gut feel	16%
Did not do any type of assessment	9%
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?	FY 2019
Yes	28%
No [skip to Q20a]	72%
Total	100%

Q19b. If yes, what limits do you purchase?	FY 2019
Less than $1 million	8%
$1 million to $5 million	33%
$6 million to $20 million	48%
$21 million to $100 million	8%
More than $100 million	4%
Total	100%
Extrapolated value (US$ millions)	16.96

Q19c. Is your company's cyber insurance coverage sufficient with respect to coverage terms and conditions, exclusions, retentions, limits and insurance carrier financial security?	FY 2019
Yes	58%
No	28%
Unsure	13%
Total	100%

Q19d. How does your company determine the level of coverage it deems adequate?	FY 2019
Formal risk assessment by in-house staff	13%
Formal risk assessment conducted by the insurer	14%
Formal risk assessment by third party	24%
Informal or ad hoc risk assessment	12%
Policy terms and conditions reviewed by a third-party specialist	20%
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.	FY 2019
External attacks by cybercriminals	85%
Malicious or criminal insiders	83%
System or business process failures	40%
Human error, mistakes and negligence	31%
Incidents affecting business partners, vendors or other third parties that have access to your company's information assets	44%
Other	27%
Total	311%
Total	100%

Q19f. What coverage does this insurance offer your company? Please select all that apply.	FY 2019
Forensics and investigative costs	63%
Notification costs to data breach victims	61%
Communication costs to regulators	49%
Employee productivity losses	51%
Replacement of lost or damaged equipment	61%
Revenue losses	34%
Legal defense costs	46%
Regulatory penalties and fines	48%
Third-party liability	44%
Brand damages	16%
Other	19%
Unsure	24%
Total	518%

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.	FY 2019
Access to cybersecurity forensic experts	82%
Access to legal and regulatory experts	81%
Access to specialized technologies and tools	51%
Advanced warnings about ongoing threats and vulnerabilities	42%
Assistance in the remediation of the incident	56%
Assistance in the notification of breach victims	45%
Identity protection services for breach victims	25%
Credit monitoring services for breach victims	44%
Assistance in reputation management activities	50%
Other	19%
Total	494%

Q20a. Does your company plan to purchase stand-alone cyber insurance?	FY 2019
Yes, in the next 12 months	16%
Yes, in the next 24 months	25%
Yes, in more than 24 months	21%
No	38%
Total	100%

Q20b. If no, what are the **two** main reasons why your company is not planning to purchase stand-alone cybersecurity insurance?	FY 2019
Premiums are too expensive	35%
Coverage is inadequate based on our exposure	36%
Too many exclusions, restrictions and uninsurable risks	31%
Risk does not warrant insurance	6%
Property and casualty policies are sufficient	27%
Executive management does not see the value of this insurance	22%
Unable to get insurance underwritten because of current risk profile	18%
Other	7%
Total	182%

Q21. Who in your company is **most responsible** for cyber risk management? Please select your two top choices.	FY 2019
CEO/board of directors	2%
Chief financial officer	6%
Business unit (LOB) leaders	23%
Chief information officer	22%
Chief information security officer	15%
Risk management	16%
Procurement	6%
General counsel	6%
Compliance/audit	3%
Other	0%
Total	100%

Part 3. IP risks

Q22. Does your company's enterprise risk management activities include risks to IP such as trademarks and brand, patents, copyrights and trade secrets as well as liability risks relating to third-party IP?	FY 2019
Yes	57%
No [skip to Part 4]	43%
Total	100%

Q23. What is the total value of your company's IP assets, such as trademarks, patents, copyrights, trade secrets and know-how?	FY 2019
Less than $1 million	0%
$1 to 10 million	9%
$11 to 50 million	20%
$51 to 100 million	25%
$101 to 500 million	27%
$501 to 1 billion	15%
$1 to 10 billion	4%
More than $10 billion	1%
Total	100%
Extrapolated value	472.94

Q24a. Did your company experience a material IP event in the past 24 months?	FY 2019
Yes	28%
No	72%
Total	100%

If your company experienced more than one material IP event, please refer to the most recent event that occurred over the past 24 months.

Q24b. If yes, what type of IP assets were involved in the event? Please select all that apply.	FY 2019
Patent	24%
Trade secret	42%
Copyright	26%
Other	8%
Total	100%

Q24c. If yes, what best describes the event?	FY 2019
Challenge to company rights	29%
Infringement of company rights	40%
Allegation of company infringement of third-party rights	31%
Total	100%

Q25. How do IP risks compare to other business risks?	FY 2019
IP risk is the number 1 or 2 business risk for my company	17%
IP risk is a top 5 business risk for my company	32%
IP risk is a top 10 business risk for my company	32%
IP risk is not in the top 10 of business risks for my company	19%
Total	100%

Q26. Does your company's existing insurance policy (e.g., property, general liability or crime) cover any of the following IP events?	FY 2019
A challenge to your company's IP assets	37%
Third-party infringement of your company's IP assets	34%
An allegation that your company is infringing third-party IP rights	33%
Our existing policy does not cover IP events	34%
Total	138%

Q27a. Does your company have a trade secret theft insurance policy as a complement to a cyber risk policy?	FY 2019
Yes	24%
No	76%
Total	100%

Q27b. If no, what is your company's level of interest in purchasing a trade secret theft insurance policy as a complement to a cyber risk policy?	FY 2019
Very interested	29%
Interested	33%
Somewhat interested	24%
Not interested	14%
Total	100%

Q28a. Does your company have an intellectual property liability policy?	FY 2019
Yes	30%
No	70%
Total	100%

Q28b. If no, what is your company's level of interest in purchasing an intellectual property liability policy?	FY 2019
Very interested	29%
Interested	34%
Somewhat interested	26%
Not interested	11%
Total	100%

Part 4. Role & Organizational Characteristics

D1. What level best describes your current position?	FY 2019
Senior executive	4%
Vice president	5%
Director	13%
Manager	17%
Supervisor	14%
Associate/staff	10%
Technician	28%
Contractor/consultant	7%
Other	1%
Total	100%

D2. What is the worldwide employee head count of your company?	FY 2019
Less than 500	14%
500 to 1,000	16%
1,001 to 5,000	25%
5,001 to 25,000	26%
25,001 to 75,000	12%
More than 75,000	8%
Total	100%

D3. What best describes your company's industry focus?	FY 2019
Communications	3%
Consumer products	6%
Defense & aerospace	1%
Education & research	3%
Energy & utilities	6%
Entertainment & media	2%
Financial services	18%
Health & pharmaceuticals	10%
Hospitality	2%
Industrial	11%
Public sector	9%
Retailing	9%
Services	11%
Technology & software	8%
Transportation	2%
Other	0%
Total	100%

Acknowledgements

The 2019 Intangible Assets Financial Statement Comparison Report is the third of three intangible assets/cyber risk transfer research papers that examine the comparative values, probable maximum loss and allocation of resources to protect certain tangible assets compared with intangible assets. We thank the following Aon colleagues and industry leaders who assisted Larry Ponemon, Ph.D., founder and chairman, Ponemon Institute, and Susan Jayson, executive director and co-founder, Ponemon Institute, and contributed to these efforts:

- Jesus Gonzalez, Deputy Global Practice Leader, Intangible Assets, Aon
- Carrie Yang, Asia Intangible Assets leader, Aon's Cyber Solutions
- Vanessa Leemans, EMEA Chief Commercial Officer, Aon's Cyber Solutions
- Dan Crouse, Consulting Leader, Aon's Intellectual Property Solutions
- Nick Chmielewski, Chief Broking Officer, Aon's Intellectual Property Solutions
- Neerav Patel, Manager, Aon Inpoint
- Kevin Kalinich, Esq., Global Practice Leader, Intangible Assets, Aon
- Paul Kim, Head of Strategy and Product Development, Aon

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