# 2019 Intangible Assets Financial Statement Impact Comparison Report

## EMEA Edition

*The rise of intangible assets*

**Sponsored by Aon**

Independently conducted by Ponemon Institute LLC

Publication Date: November 2019

AON
Empower Results®

# Table of Contents

# Executive Summary

Barely a week passes without the fallout of a cyber attack on a major corporation hitting the headlines. In July 2019, the data breach at Capital One exposed the records of almost 106 million people in the United States and Canada.[1] In Europe, Norsk Hydro was forced to halt production following a cyber attack in March 2019, which is expected to cost the firm around $60-71 million.[2]

Organisations are starting to see the significant financial impact of non-compliance with data privacy and the General Data Protection Regulation (EU) 2016/679 ("GDPR"). Two recent examples are: the UK Information Commissioner's Office (ICO)'s notification of intention to impose an £183 million fine on British Airways in July 2019,[3] and the US Federal Trade Commission (FTC)'s $5 billion civil penalty against Facebook for violations of an earlier FTC order, announced in the same month, is "record-breaking and history-making" in July 2019.[4]

Despite such high profile losses related to cybersecurity breaches or attacks, this latest research conducted by Ponemon Institute and sponsored by Aon, reveals that across Europe, the Middle East and Africa (EMEA), there continues to be a significant difference between the amount of insurance bought for Property Plant and Equipment (PP&E), compared to insurance bought for information assets despite organisations valuing those information assets higher than they do their PP&E.

## Key findings in the report include:

- More than two thirds of companies (67 percent) expect their cyber risk exposure to increase over the next 24 months
- 41 percent reported a material or significantly disruptive cyber security incident or data breach one or more times in the past 24 months, with the average total financial impact of these incidents at $5.5 million
- Businesses think they are more likely to experience a loss in relation to their information assets, than they are in relation to their PP&E. And the value of a probable maximum loss for information assets is higher at an average of just over $1 billion compared to $686 million for PP&E
- Despite this vulnerability, an average of only 18 percent of information assets are insured compared to an average of 59 percent of PP&E assets
- Nearly a third (29 percent) of the survey's respondents experienced a material Intellectual Property (IP) event involving trade secrets (36 percent), copyright (30 percent) and patents (24 percent)

**The rise of intangible assets[5]**

With 67% of EMEA organisations expecting their cyber risk exposure to increase over the next two years, risk transfer options are continuously evolving with insurance policies coming to market to meet this demand. When businesses suffer a cybersecurity attack against their computer systems and related digital assets, there are some very real losses they face, such as: legal costs and damages from claims alleging a privacy breach or network security failure. Potentially more costly losses may result from business interruption and increased working costs. These costs can be quantified through financial modelling by professional cybersecurity risk consultants. However, losses associated with dilution of brand and reputational losses are much more difficult to quantify and ultimately to insure.

We see that in instances where pure financial gain by theft of funds or theft of customer data are not the principal aim, theft of trade secrets and other intellectual property is often the primary or secondary purpose of the attack. Businesses are only just beginning to come to terms with the true long-term costs of a cybersecurity attack beyond the immediate financial losses and focus on safeguarding their intangible assets.

[1] https://www.capitalone.com/facts2019/

[2] https://www.hydro.com/Document/Index?name=Report%20Q3%202019.pdf&id=252245

[3] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/

[4] https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history

[5] Tangible assets are Property, Plant & Equipment ("PP&E"). Intangible assets include computer systems and related digital assets, but also brand and reputation, as well as intellectual property values.

# Part 1: Introduction

The purpose of this research is to compare the relative insurance protection of certain tangible[6] versus intangible[7] assets. How do cyber asset values and potential losses compare to tangible asset values and potential losses from an organisation's other perils, such as fires and weather?

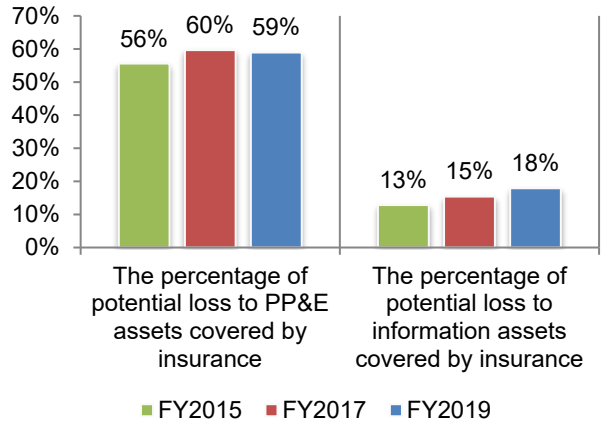
Since 2015, Aon and Ponemon Institute have studied the financial statement impact of tangible property and network risk exposures. In this year's research, we have added the cyber threats to intellectual property and what organisations are doing to manage the risk. A better understanding of the relative financial statement impact will assist organisations in allocating resources and determining the appropriate amount of risk transfer (insurance) resources to allocate to the mitigation of the financial statement impact of network risk exposures.

Network risk exposures can broadly include breach of privacy and security of personally identifiable information, stealing an organisation'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.[8]

We surveyed 563 individuals in Europe, the Middle East and Africa (EMEA) 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 (33 percent of respondents) or risk management (29 percent of respondents). Other respondents are in corporate compliance/audit (16 percent of respondents) and general management (9 percent of respondents).

As shown in Figure 1, despite the greater average potential loss to information assets ($1,006 million) compared to property, plant & equipment ("PP&E) ($686 million), the latter has much higher insurance coverage (59 percent vs. 18 percent).

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




[6] Property, Plant & Equipment ("PP&E")

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

[8] 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.

**Following are some of the key takeaways from this research:**

**Companies value information assets slightly higher than they do PP&E[9].** On average, the total value of PP&E, including all fixed assets plus SCADA and industrial control systems is approximately $1,064 million. 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 less than PP&E at $931 million.

**The value of PML[10] 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 $1,006 million.
In contrast, the value of the largest loss that could result from damage or total destruction of PP&E is approximately $686 million on average.

**There is a significant difference between the insurance coverage of PP&E and information assets**. On average, approximately 59 percent of PP&E assets are covered by insurance and approximately 30 percent of PP&E assets are self-insured (Figure 6)[11]. Only an average of 18 percent of information assets are covered by insurance. Self-insurance is higher for information assets at 63 percent.

**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 5.4 percent and 100 percent of PML at 3 percent. 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 1.8 percent and at 100 percent of PML it is 0.38 percent.

**More than one-third of respondents believe no disclosure of a material loss to information assets is required.** Forty-two 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, (24 percent of respondents). Forty-one percent say they would disclose a material loss to information assets as a footnote disclosure in the financial statements, but 34 percent of respondents do not believe disclosure is necessary.

**The majority of companies had a material[12] or significantly disruptive security exploit or data breach one or more times in the past 24 months.** Forty-one percent of respondents report their company had such a security incident. The average total financial impact of these incidents was $5.5 million.[13] Sixty-nine percent of these respondents say the incident increased their company's concerns over cyber liability.

**Companies' exposure to cyber risk is expected to increase**. However, 41 percent of respondents say there is no plan to purchase cyber insurance. Sixty-seven percent of respondents believe their company's exposure to cyber risk will increase and 22 percent of respondents say it will stay the same. Only 11 percent of respondents expect it to actually decrease.

---

[9] Respondents were asked to assume, with respect to PP&E assets, the root causes of loss (a.k.a. perils) include fire, flooding, weather events, earthquakes and other natural or man-made disasters.
[10] 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).
[11] 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.
[12] 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.
[13] 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.

**Despite the extent of cyber risk, which exceeds that of PP&E risk, only 30 percent of respondents say their companies currently have cyber insurance coverage with an average limit of $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 IP risks rank in the top 10 of all business risks facing companies**. Ninety percent of respondents consider a cyber risk as the number one or two business risk (21 percent of respondents), in the top five (40 percent of respondents) and in the top 10 (29 percent of respondents). Similarly, 80 percent of respondents rate the risk to their company's intellectual property (IP) in the top 10 of all business risks.

**In the past two years, 29 percent of respondents say their company experienced a material IP event.** Most of these incidents involved trade secrets (36 percent of respondents). Fewer events involved copyrights and patents (30 percent and 24 percent of respondents, respectively).

**Most companies' insurance policy does not cover all the consequences of an IP event.** Fifty-one percent of respondent say the policy covers third-party infringement of their company's IP assets and 45 percent of respondents say it covers a challenge to their company's IP assets. Thirty-eight percent of respondents say their existing policy does not cover IP events.

**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 25 percent of respondents say they have a trade secret theft insurance policy and 33 percent of respondents say their company has an intellectual property liability policy.

# Part 2: Key findings

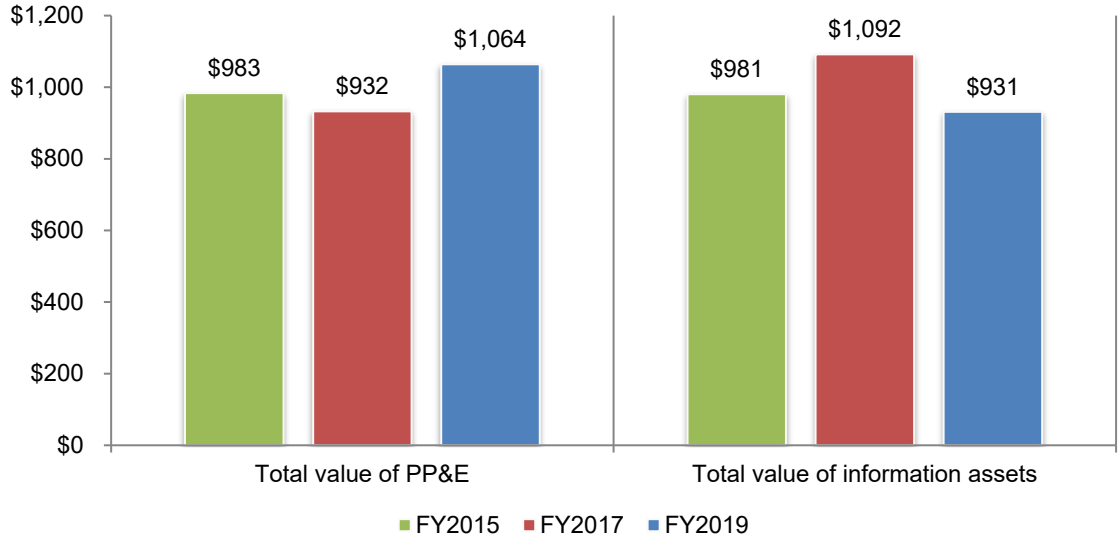
This report features the EMEA[14] findings since the study was conducted in 2015. All respondents are familiar with the cyber risks facing their company. In the context of this research, cyber risk means any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems.[15] The complete audited findings are presented in the Appendix of this report. We have organised 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
- Cyber risks 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.** According to Figure 2, on average, the total value of PP&E, including all fixed assets plus SCADA and industrial control systems is approximately $1,064 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 less than PP&E at $931 million.

**Figure 2. The total value of PP&E and information assets**
Extrapolated value ($ millions)

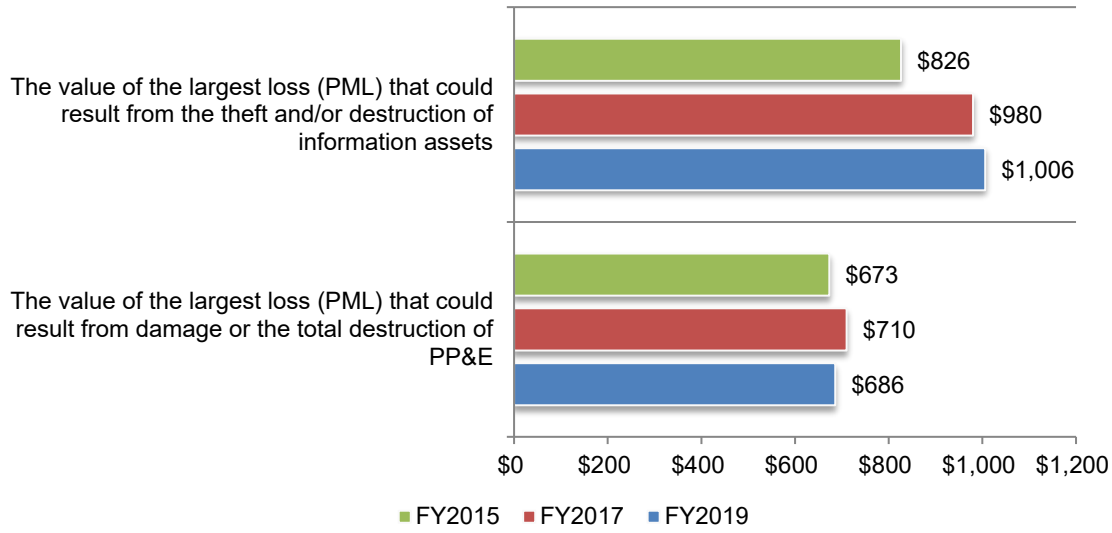



[14] The *2019 Global Cyber Risk Transfer Report* presents the consolidated findings for the following regions: NA, EMEA, APJ and LATAM (2,348 respondents).
[15] Source: Institute of Risk Management

**The value of PML 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 $1,006 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.

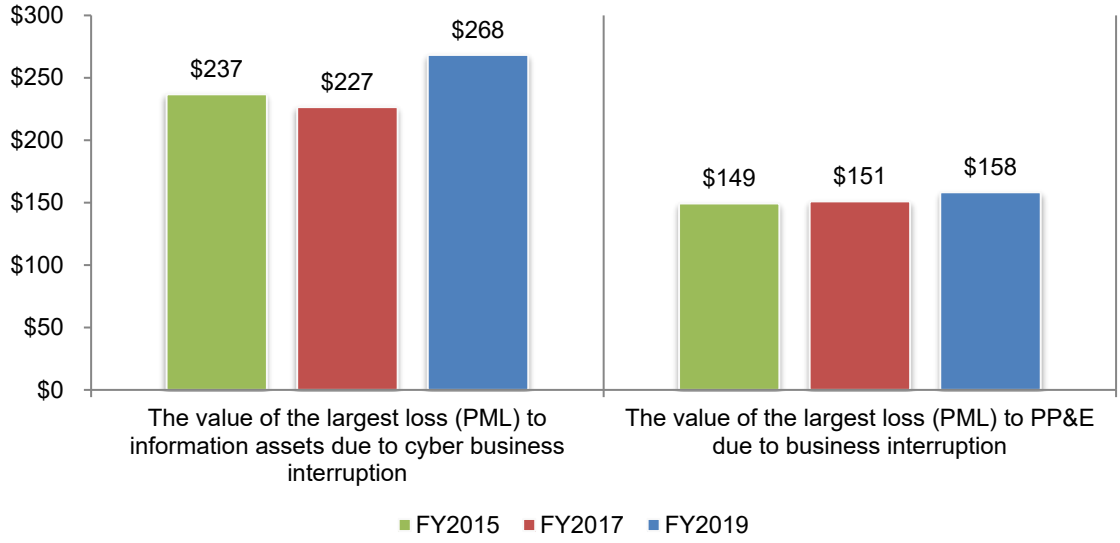
In contrast, the value of the largest loss that could result from damage or total destruction of PP&E is approximately $686 million on average. This also assumes the normal functioning of passive protective features such as firewalls, nonflammable materials, proper functioning of active suppression systems, fire sprinklers, raised flooring and more.

**Figure 3. The PML value for PP&E and information assets**
Extrapolated value ($ millions)



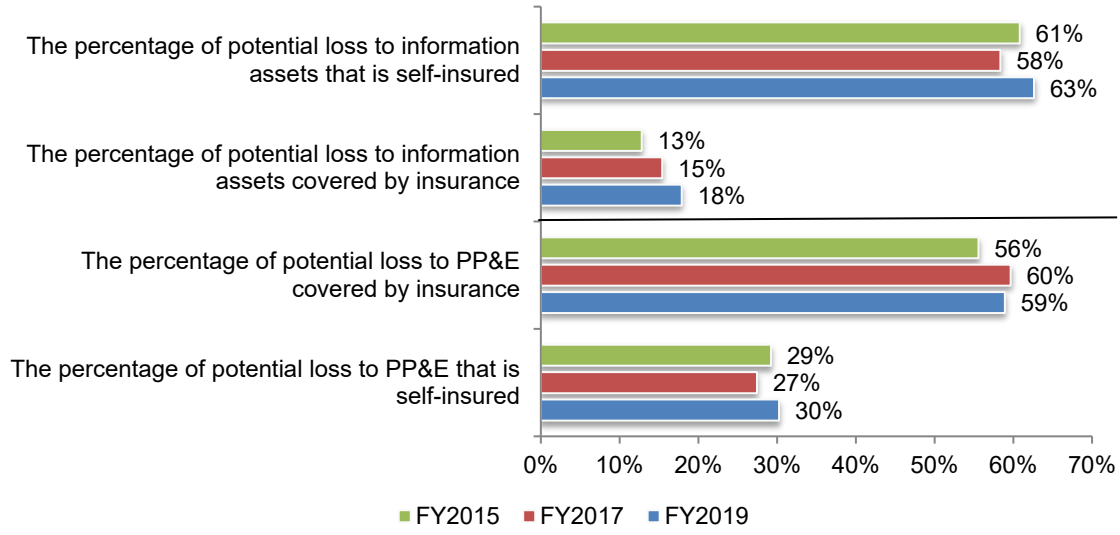
**What is the impact of business disruption to PP&E and information asset losses?** According to Figure 4, business disruption has a greater impact on information assets ($268 million)[16] than on PP&E ($158 million).

**Figure 4. The impact of business disruption to information assets and PP&E**
Extrapolated value ($ millions)




**There is a significant difference between the insurance coverage of PP&E and information assets**. On average, approximately 59 percent of PP&E assets are covered by insurance and approximately 30 percent of PP&E assets are self-insured (Figure 5). Only an average of 18 percent of information assets are covered by insurance. Self-insurance is higher for information assets at 63 percent.

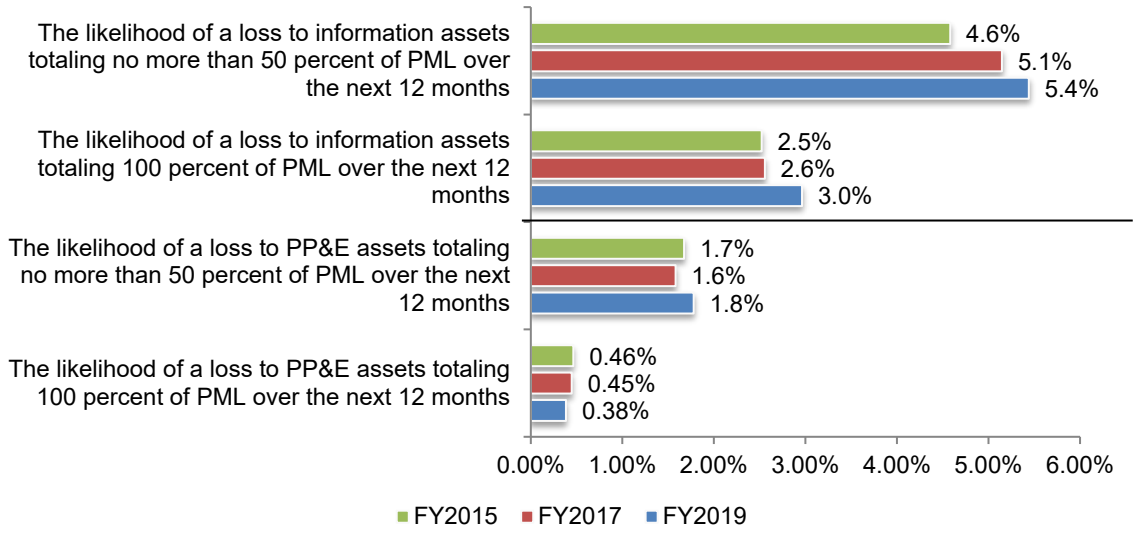
**Figure 5. Percentage of PP&E and information assets covered by insurance**
Extrapolated percentage




[16] While the survey results suggest Probable Maximum Loss in the neighborhood of $268 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.

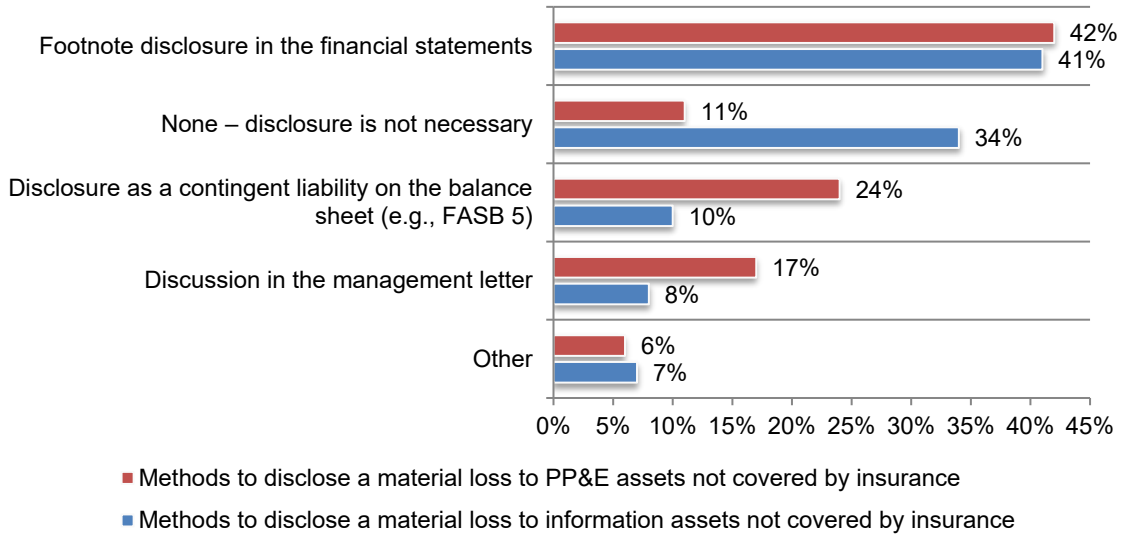
**The likelihood of a loss is higher for information assets than for PP&E.** Companies estimate the likelihood that they will sustain a loss to information assets totaling no more than 50 percent of PML over the next 12 months at 5.4 percent and 100 percent of PML at 3 percent, as shown in Figure 6. The likelihood of a loss to PP&E totaling no more than 50 percent of PML over the next 12 months is an average of 1.8 percent and at 100 percent of PML it is 0.38 percent.

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



**More than one-third of respondents believe no disclosure of a material loss to information assets is required.** Figure 7 focuses on how companies would disclose a material loss. Forty-two 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, followed by a disclosure as a contingent liability on the balance sheet, such as FASB 5, (24 percent of respondents). Forty-one percent say they would disclose a material loss to information assets as a footnote disclosure in the financial statements, but 34 percent of respondents do not believe disclosure is necessary.

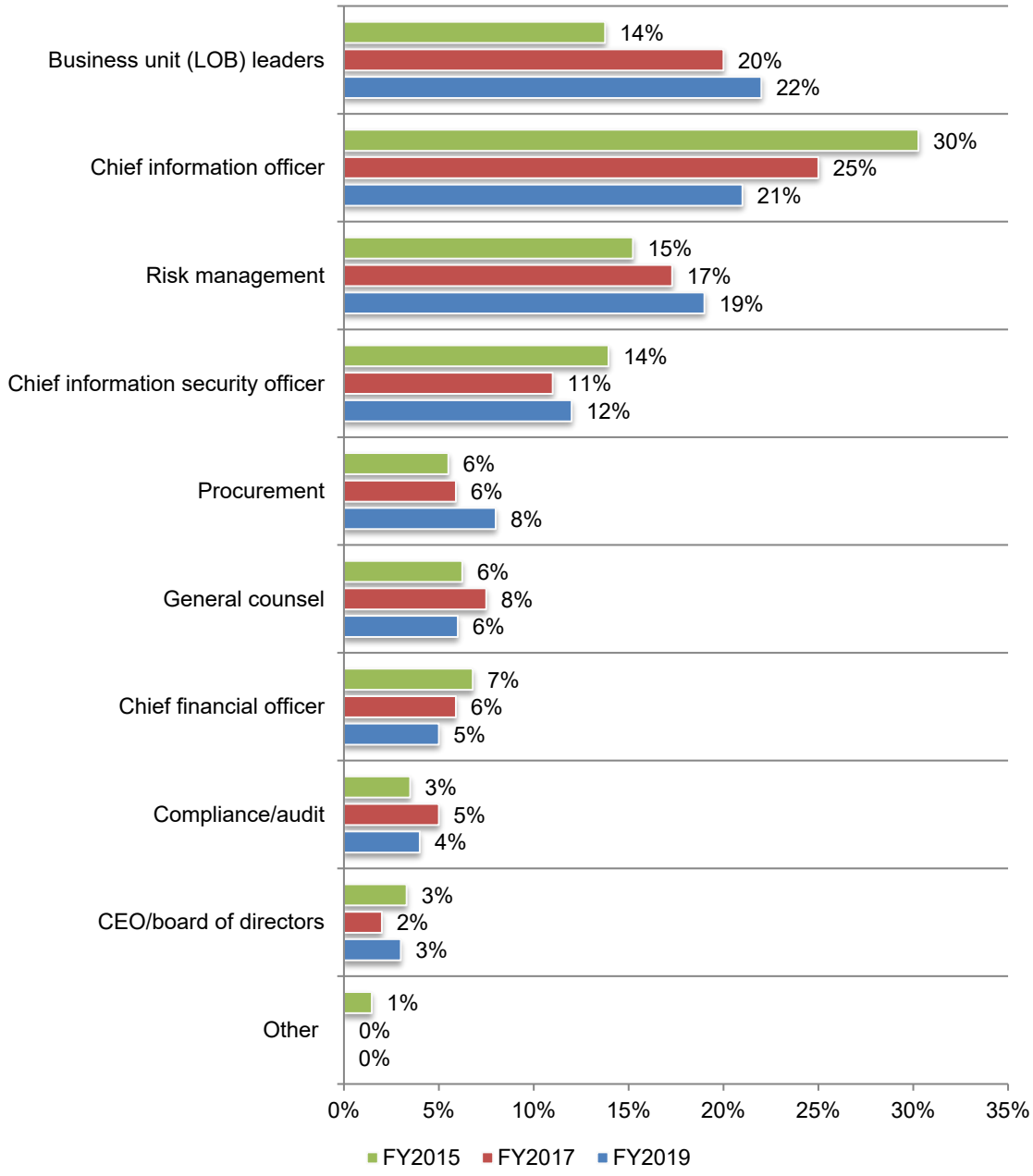
**Figure 7. How would your company disclose a material loss to PP&E and information assets?**



## The cyber risk experience of companies

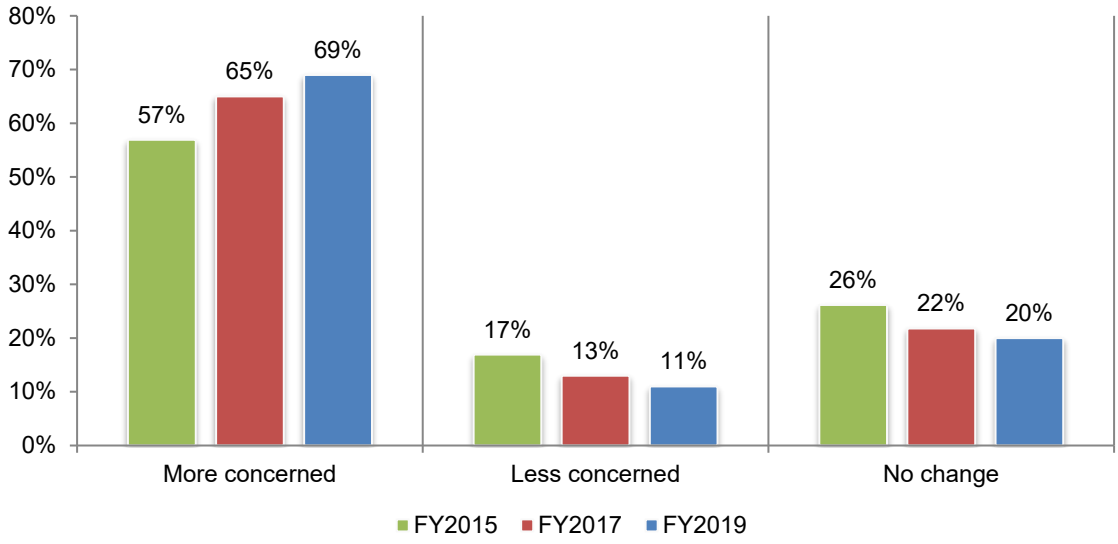
**Responsibility for cyber risk management is dispersed throughout the organisation.** As shown in Figure 8, no one function is clearly responsible for managing cyber risks in their organisations. The top two are business unit leaders (22 percent of respondents) and the chief information officer (21 percent of respondents). Since 2015, business unit leaders have increased their responsibility while the responsibility of CIOs has decreased.

**Figure 8. Who is most responsible for cyber risk management?**



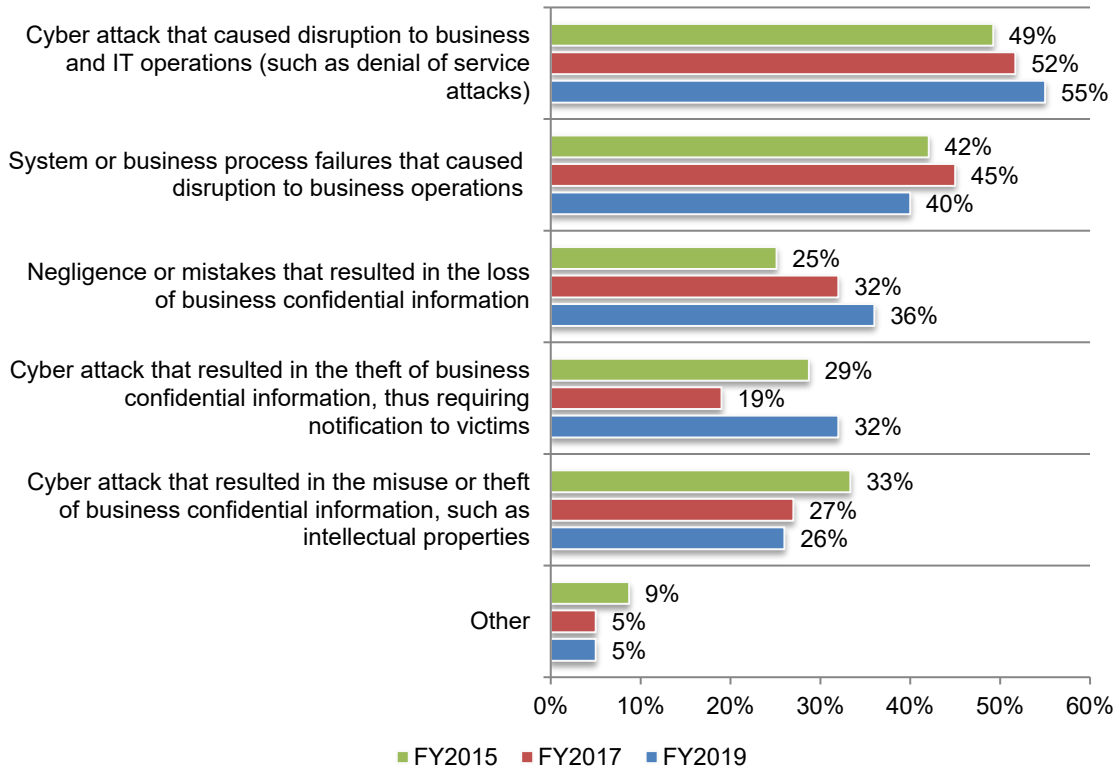
**Many companies had a material or significantly disruptive security exploit or data breach one or more times in the past 24 months.** Forty-one percent of respondents report their company had such a security incident. The average total financial impact of these incidents was $5.5 million. According to Figure 9, 69 percent of these respondents say the incident increased their company's concerns over cyber liability.

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



The types of security incidents that 41 percent of the companies in this research faced are displayed in Figure 10. The most frequent type of incident was one that caused disruption to business and IT operations (55 percent of respondents) or resulted in a system or business process failure that caused disruption to business operations (40 percent of respondents). This is followed by 36 percent of respondents who say the cyber attack was caused by negligence or mistakes that resulted in the loss of business confidential information.

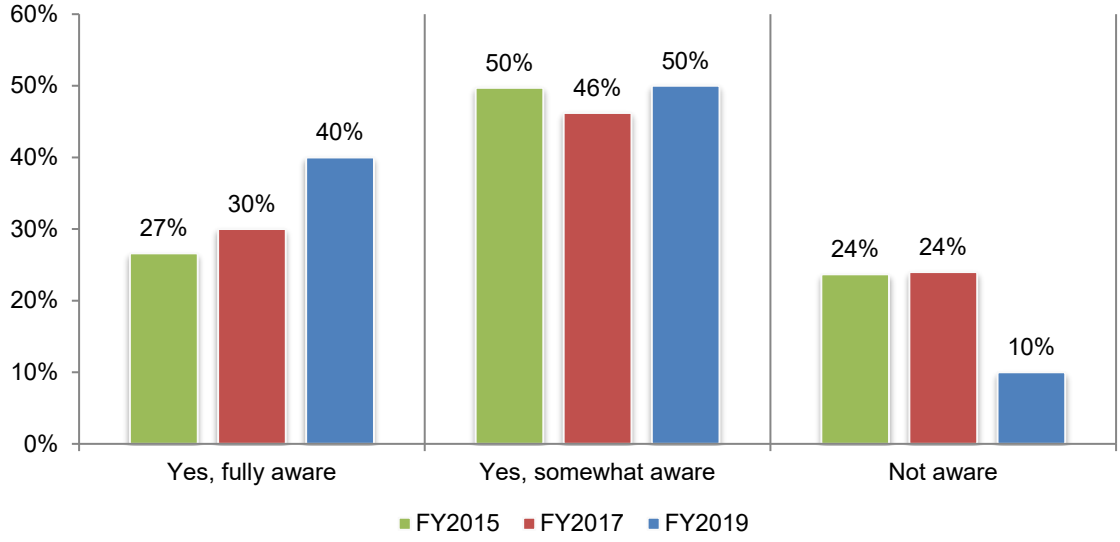
**Figure 10. What type of data breach or security exploit did your company experience?**
More than one response permitted



## Perceptions about the financial impact of cyber exposures

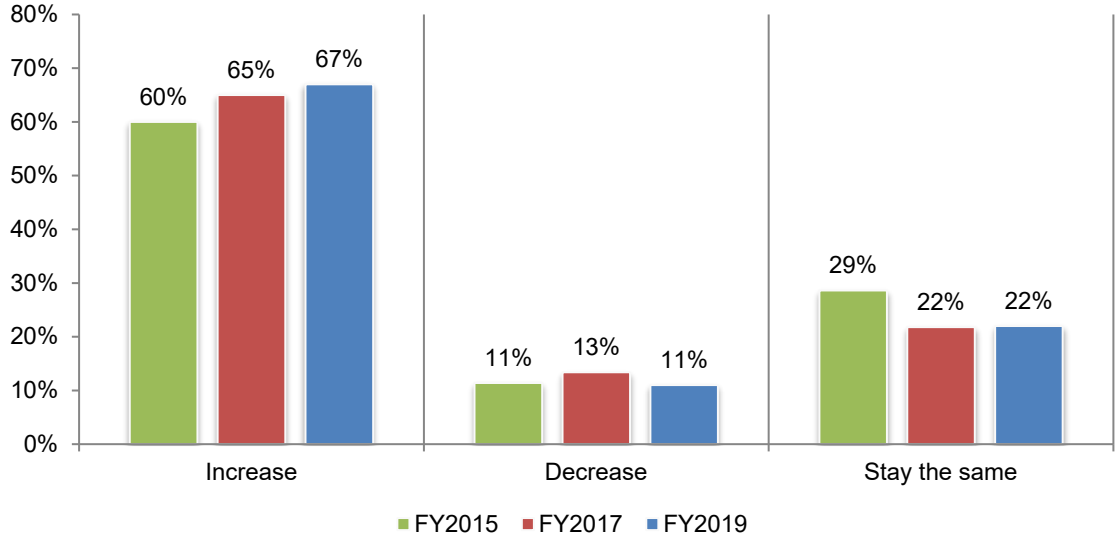
**Awareness of the economic and legal consequences from an international data breach or security exploit is low.** As revealed in Figure 11, only 40 percent of respondents are fully aware of the consequences that could result from a data breach or security exploit in other countries in which their company operates and 10 percent say they are not aware of the consequences.

**Figure 11. Awareness of the economic and legal consequences from an international data breach or security exploit**



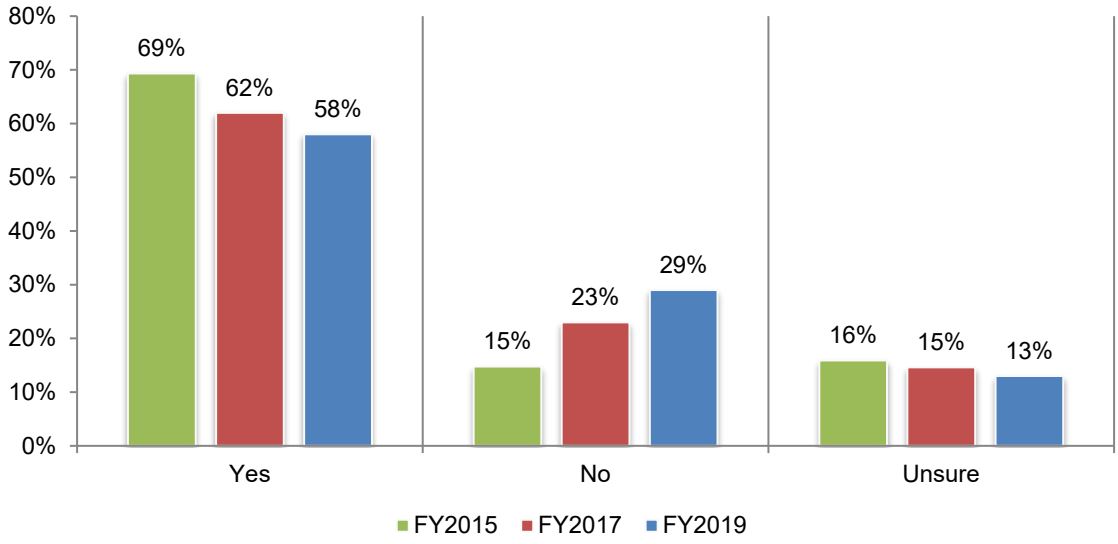

**Companies' exposure to cyber risk is expected to increase.** However, 41 percent of respondents say there is no plan to purchase cyber insurance. As the data in Figure 12 show, 67 percent of respondents believe their company's exposure to cyber risk will increase and 22 percent of respondents say it will stay the same. Only 11 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 24 months?**



**Despite the extent of cyber risk, which exceeds that of PP&E risk, only 30 percent of respondents say their companies currently have cyber insurance coverage with an average limit of $17 million.** As Figure 13 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, a significant decrease since 2015.

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



According to Figure 14, the adequacy of coverage is determined mainly by the maximum available from the insurance market or a formal risk assessment by a third party (both 20 percent of respondents). Only 16 percent of respondents say their companies have a formal risk assessment conducted by the insurer and only 14 percent have an assessment completed by in-house staff.

**Figure 14. How companies determine the adequacy of coverage**

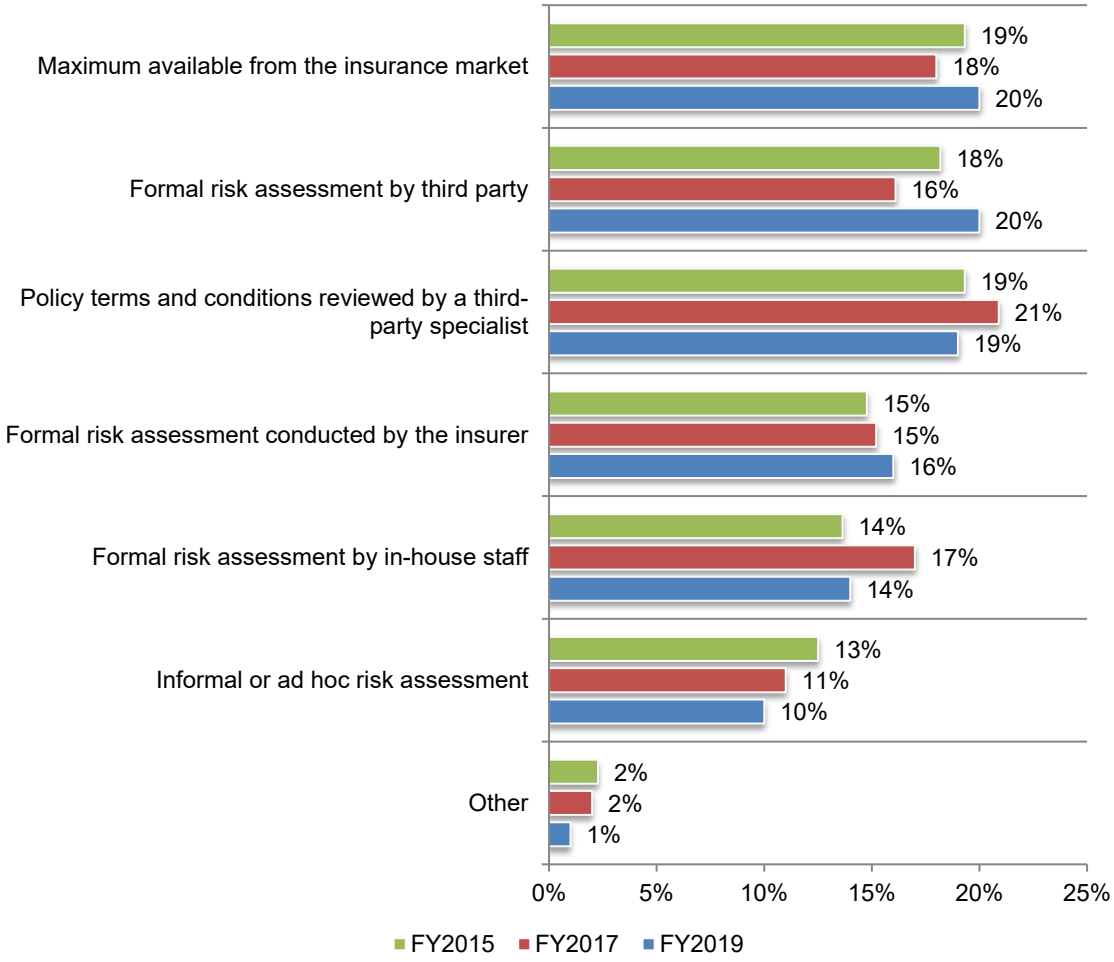
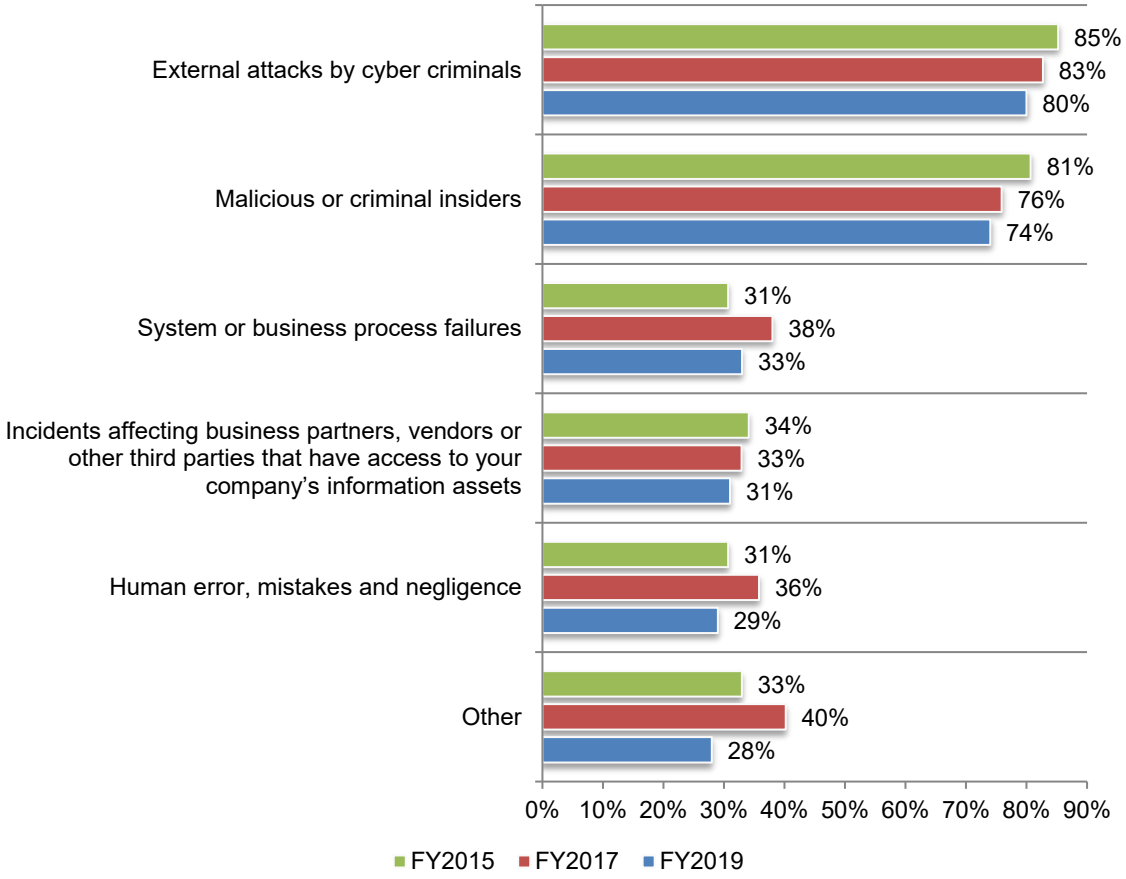


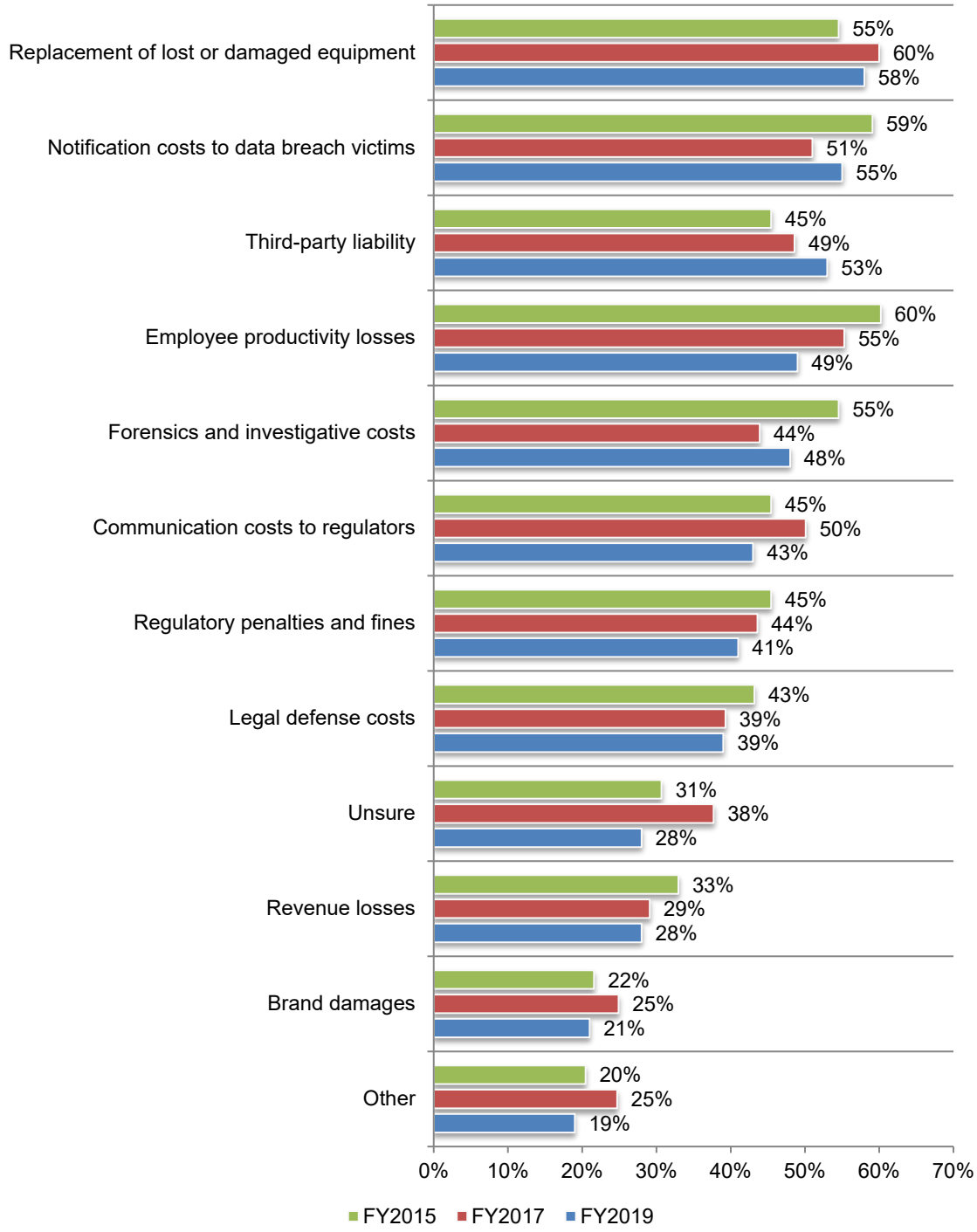
Figure 15 displays the incidents typically covered by cyber insurance. Most incidents covered are external attacks by cyber criminals (80 percent of respondents), malicious or criminal insiders (74 percent of respondents) and systems or business process failures (33 percent of respondents).

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



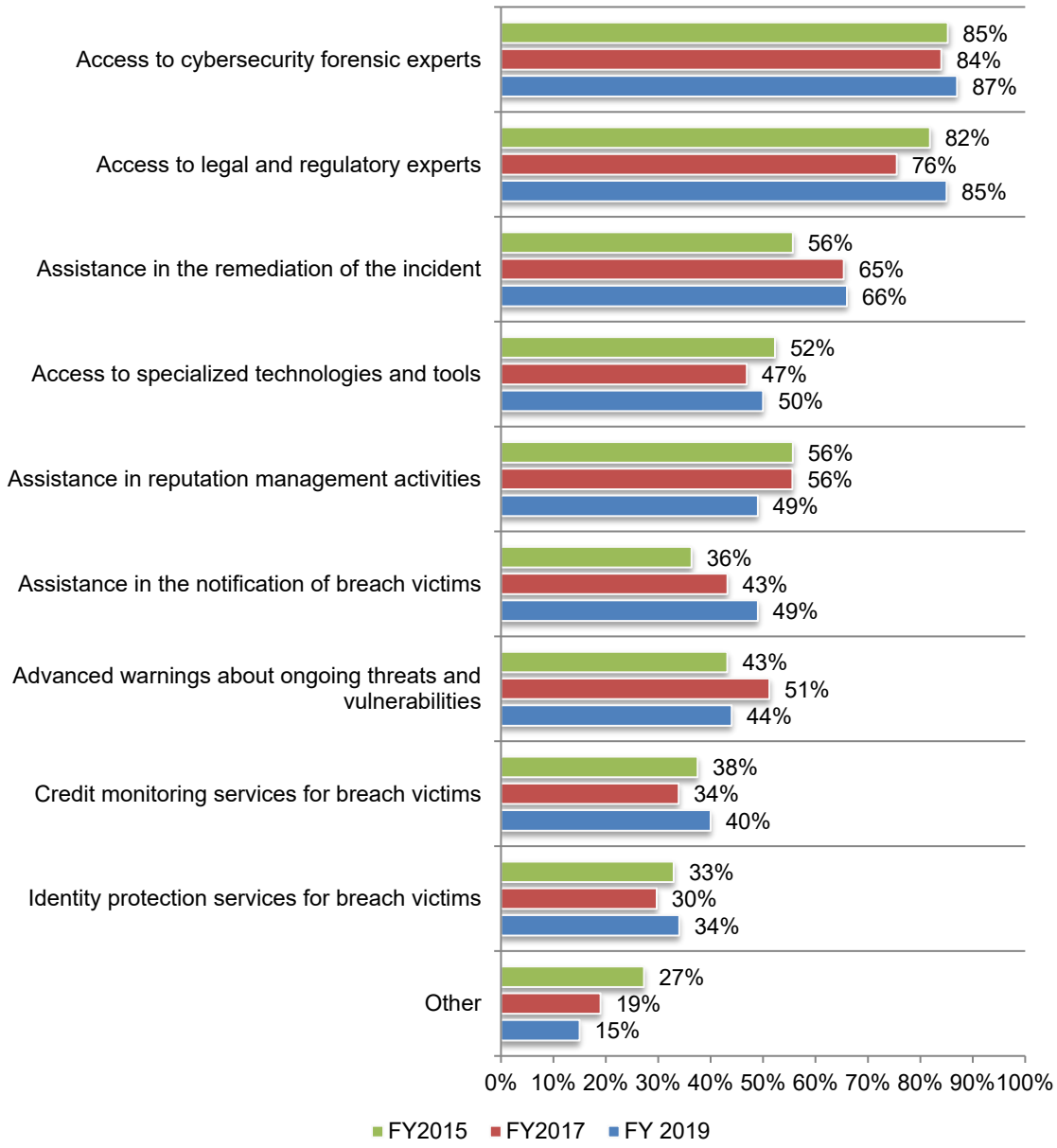
Figures 16 and 17 present the coverage and services provided by insurance companies. The top five costs covered are: replacement of lost or damaged equipment (58 percent of respondents), data breach notification costs (55 percent of respondents), third-party liability (53 percent of respondents), employee productivity losses (49 percent of respondents) and forensics and investigative costs (48 percent of respondents).

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



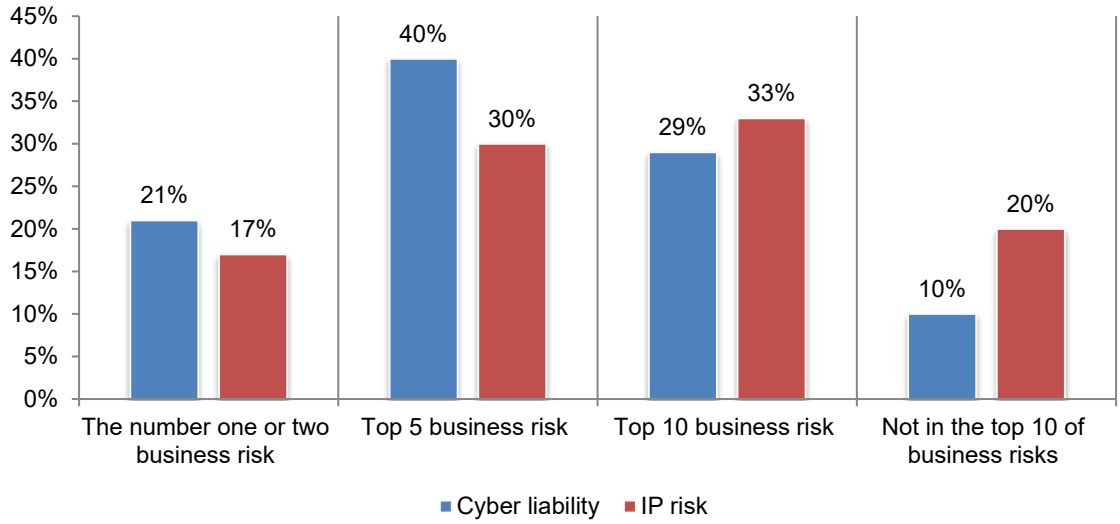

In addition to this coverage, other services provided are access to cybersecurity forensic experts (87 percent of respondents), access to legal and regulatory experts (85 percent of respondents), assistance in the remediation of the incident (66 percent of respondents) access to specialised technologies and tools (50 percent of respondents) and assistance in reputation management activities (49 percent of respondents), as shown in Figure 17.

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



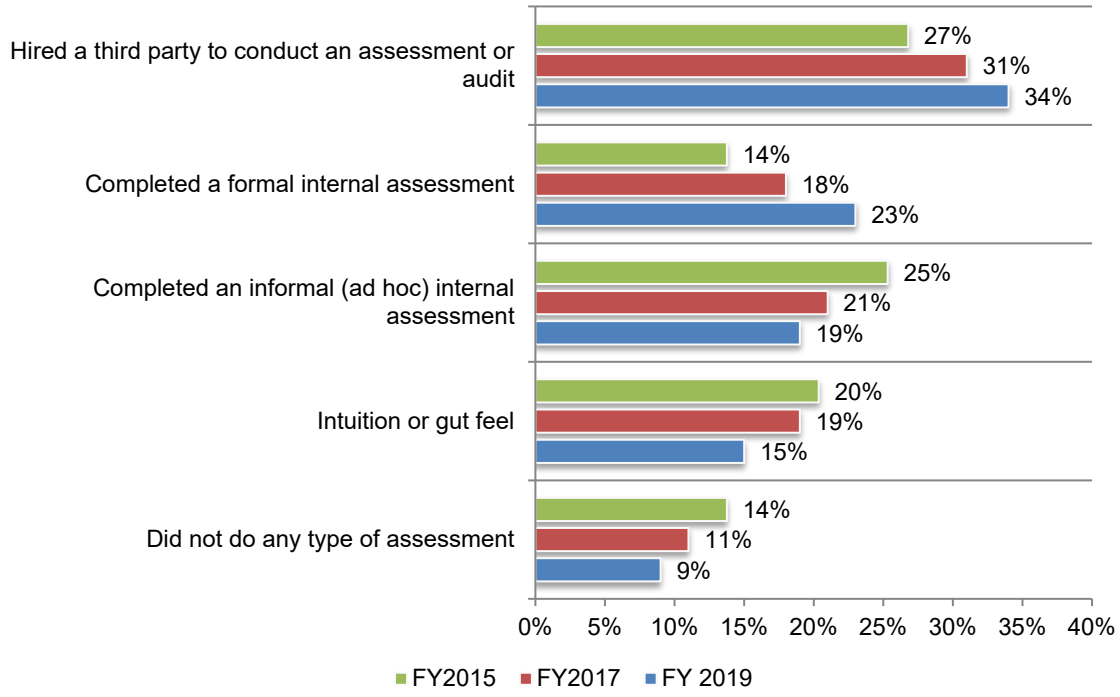
**Cyber liability and IP risks rank in the top 10 of all business risks facing companies**. Figure 18 shows that 90 percent of respondents consider a cyber risk as the number one or two business risk (21 percent of respondents), in the top five (40 percent of respondents) and in the top 10 (29 percent of respondents). Similarly, 80 percent of respondents rate the risk to their company's intellectual property (IP) in the top 10 of all business risks

**Figure 18. 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 23 percent of respondents say it was a formal internal assessment (Figure 19). Only 9 percent of respondents say their company did not do any type of assessment.

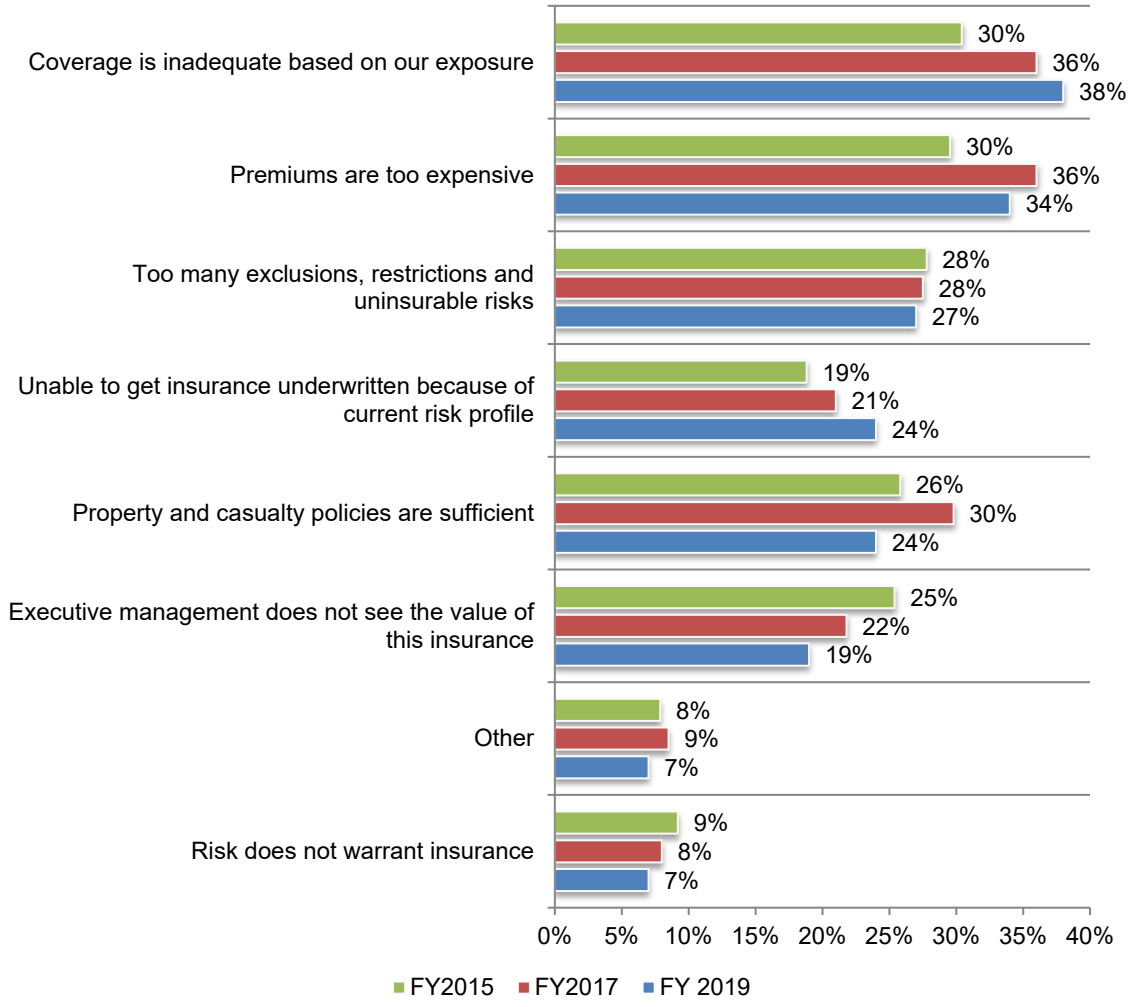
**Figure 19. How did you determine the level of cyber risk to your company?**



**Most companies are postponing the purchase of cyber insurance.** As discussed previously, 41 percent of respondents say their company has no plans to purchase cyber insurance. Only 17 of respondents say their company will purchase cyber insurance in the next 12 months. Almost half of respondents (42 percent) say they will purchase cyber insurance in the next 24 months (26 percent) or more than 24 months (16 percent).

According to Figure 20, the main reasons for not purchasing cybersecurity insurance are: coverage is inadequate based on their exposure (38 percent of respondents), premiums are too expensive (34 percent of respondents) and there are too many exclusions, restrictions and uninsurable risks (27 percent of respondents).

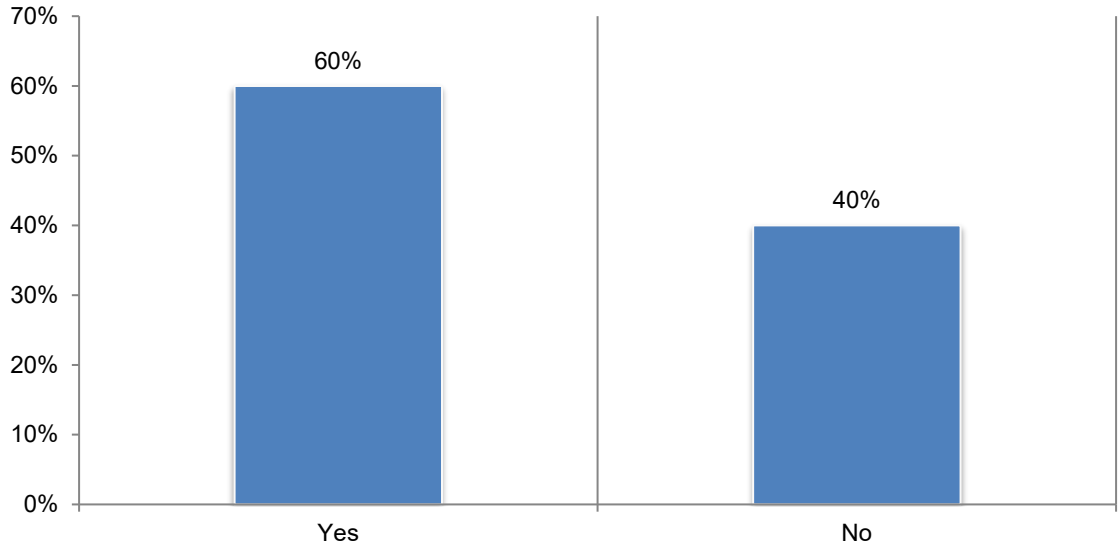
**Figure 20. What are the main reasons why your company will not purchase cyber security insurance?**
More than one response permitted



## Cyber risks to intellectual property (IP)

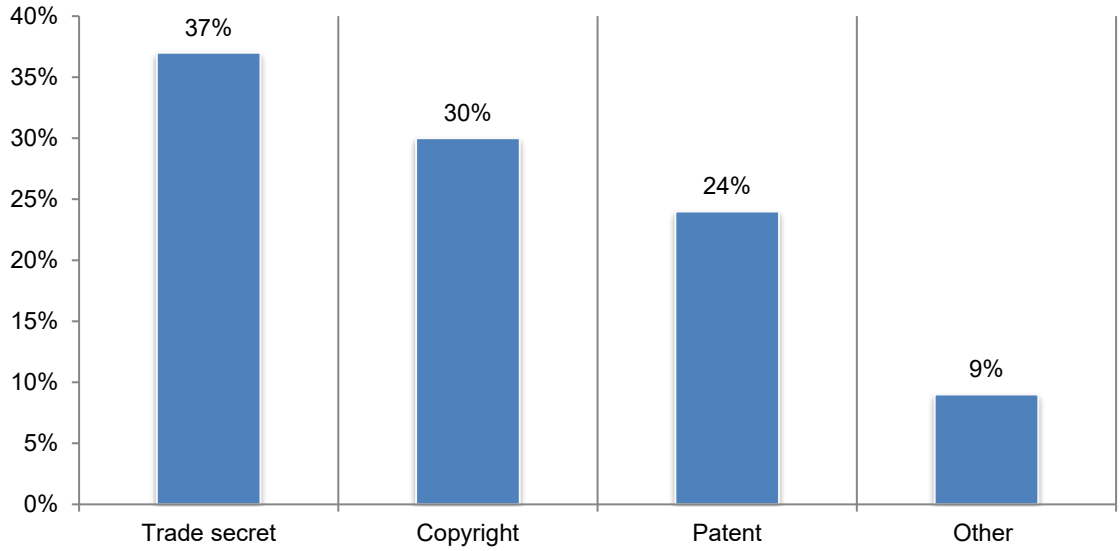
**The majority of companies have a strategy to manage risks to IP.** Companies represented in this research estimate that the average total value of their IP assets such as trademarks, patents, copyrights, trade secrets and know-how is $475 million. As shown in Figure 21, 60 percent of respondents say their enterprise risk management activities include risks to their IP.

**Figure 21. Do your company's enterprise risk management activities include risks to IP?**



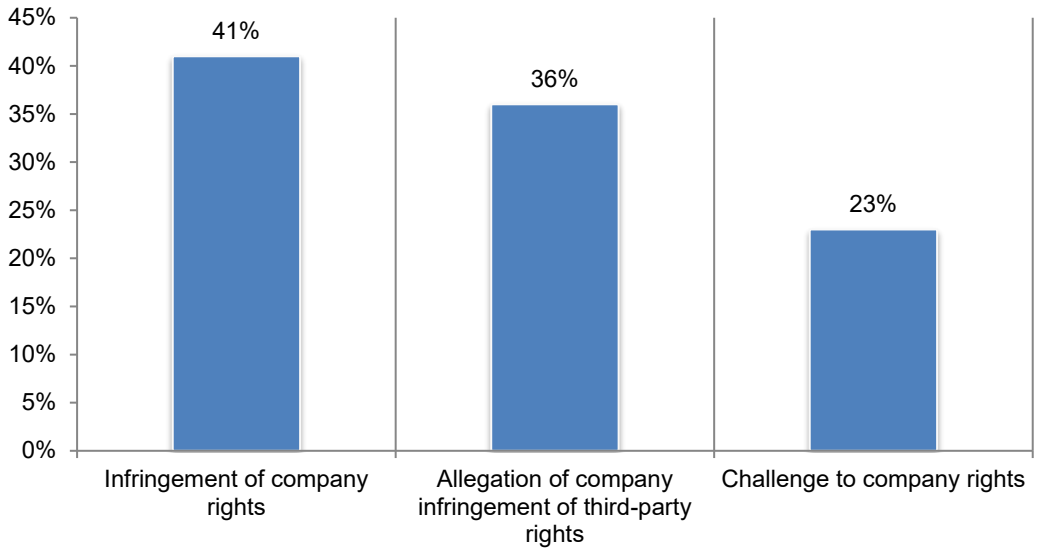

**In the past two years, 29 percent of respondents say their company experienced a material IP event.** According to Figure 22, most of these incidents involved trade secrets (37 percent of respondents). Fewer events involved copyrights and patents (30 percent and 24 percent of respondents, respectively).

**Figure 22. What type of IP assets were involved in a material IP event?**



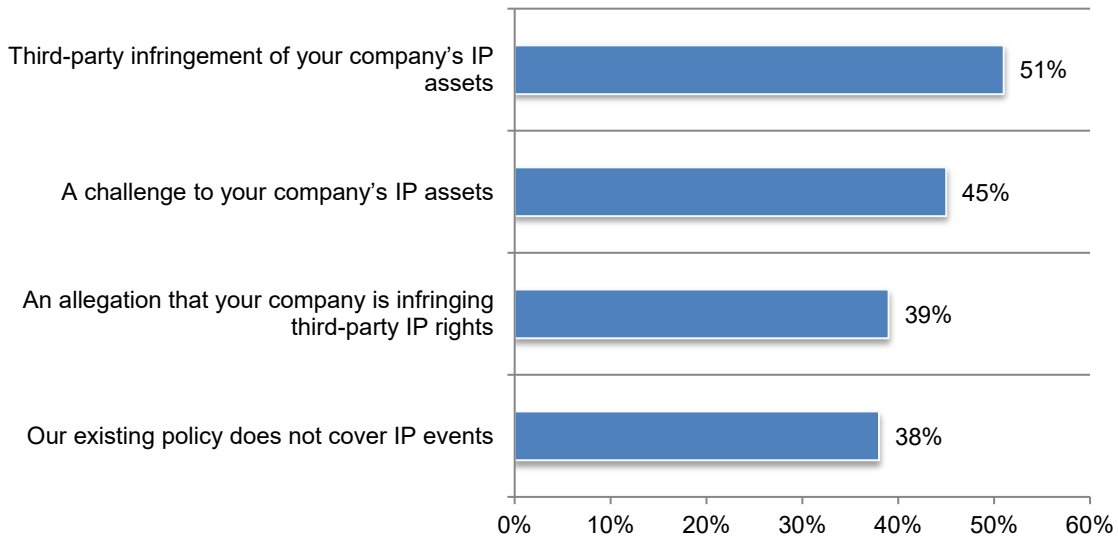
**In this section, respondents were asked to refer to the most recent IP event that occurred over the past 24 months.** According to Figure 23, the event can be described as an infringement of company rights (41 percent of respondents), allegation of company infringement of third-party rights (36 percent of respondents) or a challenge to company rights (23 percent of respondents).

**Figure 23. What best describes the event?**
Only one response permitted



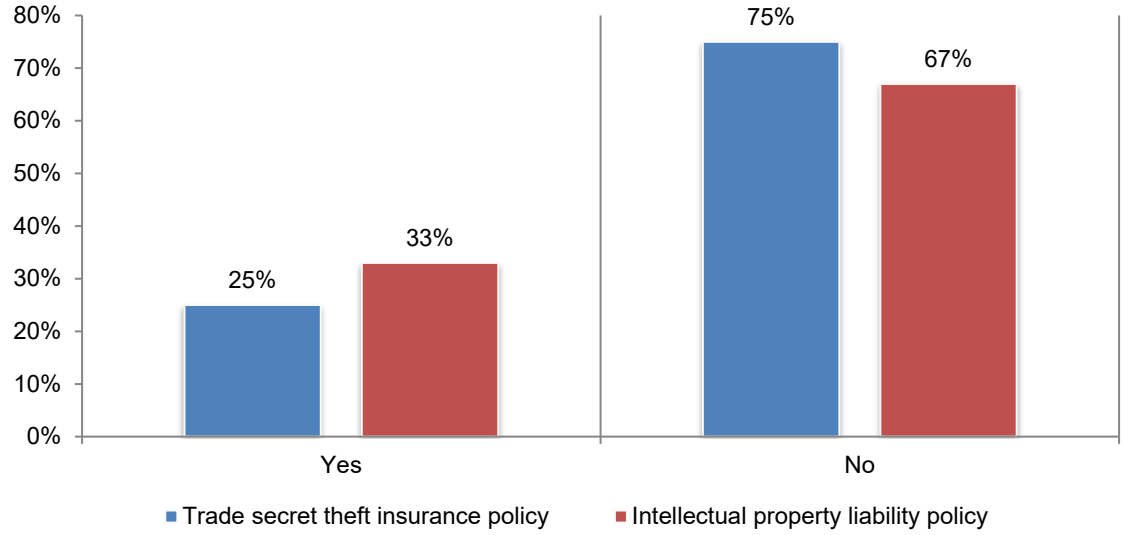

**Many companies' insurance policy does not cover all the consequences of an IP event.** According to Figure 24, 51 percent of respondent say the policy covers third-party infringement of their company's IP assets and 45 percent of respondents say it covers a challenge to their company's IP assets. Thirty-eight percent of respondents say their existing policy does not cover IP assets.

**Figure 24. Does your company's existing insurance policy cover any of the following IP events?**
More than one response permitted



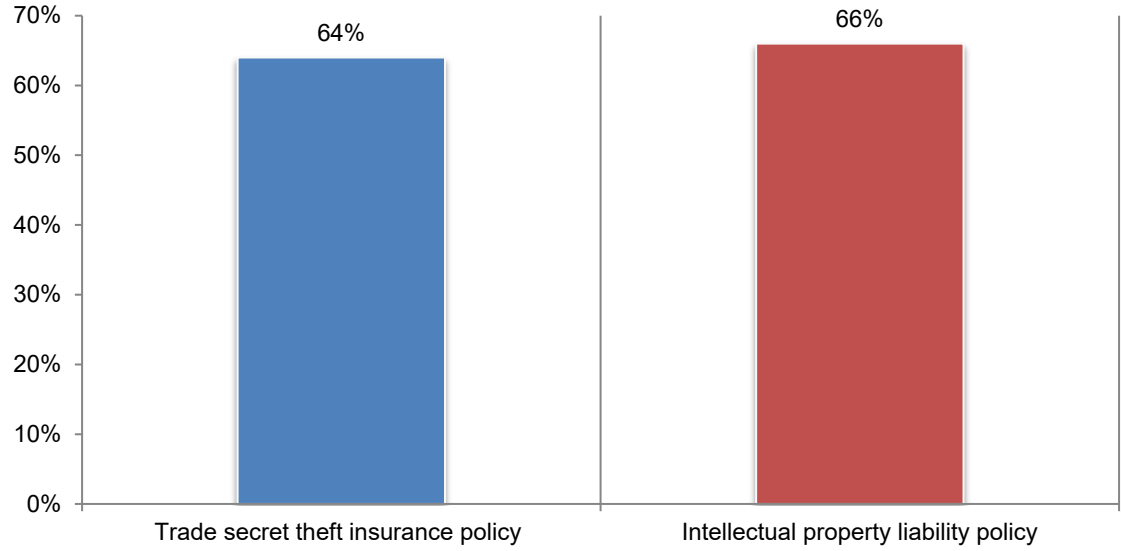
**As a complement to a cyber risk policy, few companies have a trade secret theft insurance policy and/or an intellectual property liability policy.** As shown in Figure 25, only 25 percent of respondents say they have a trade secret theft insurance policy and 33 percent of respondents say their company has an intellectual property liability policy.

**Figure 25. 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 26, 64 percent and 66 percent of respondents are very interested or interested in purchasing a trade secret and/or an IP liability policy, respectively.

**Figure 26. 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



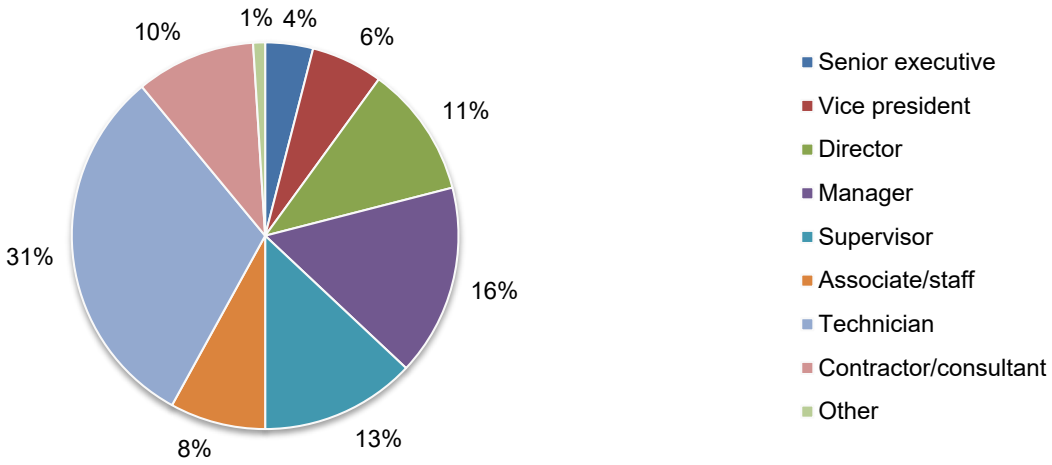
# Part 3: Methods

The EMEA sampling frame is composed of 14,842 individuals that are involved in their company's cyber risk and enterprise risk management activities. As Table 1 shows, 625 respondents completed the survey, of which 62 were rejected for reliability issues. The final sample consisted of 563 surveys, a 3.8 percent response rate.

| Table 1. Sample response | Freq | Pct% |
|---|---|---|
| Total sampling frame | 14,842 | 100.0% |
| Total returns | 625 | 4.2% |
| Rejected or screened surveys | 62 | 0.4% |
| Final sample | 563 | 3.8% |

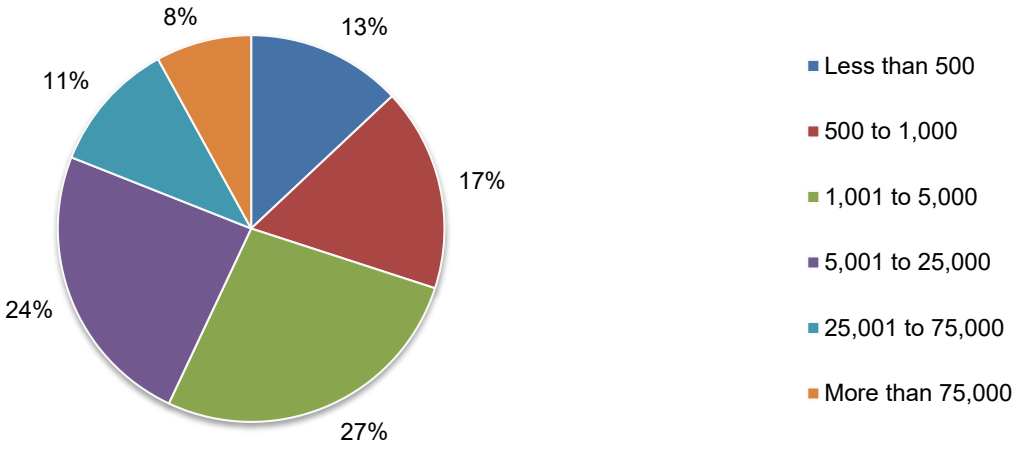
Pie Chart 1 reports the current position or organisational level of the respondents. Half of the respondents (50 percent) reported their current position as supervisory level or above and 31 percent of respondents reported their current position level as technician.

**Pie Chart 1. Current position or organisational level**



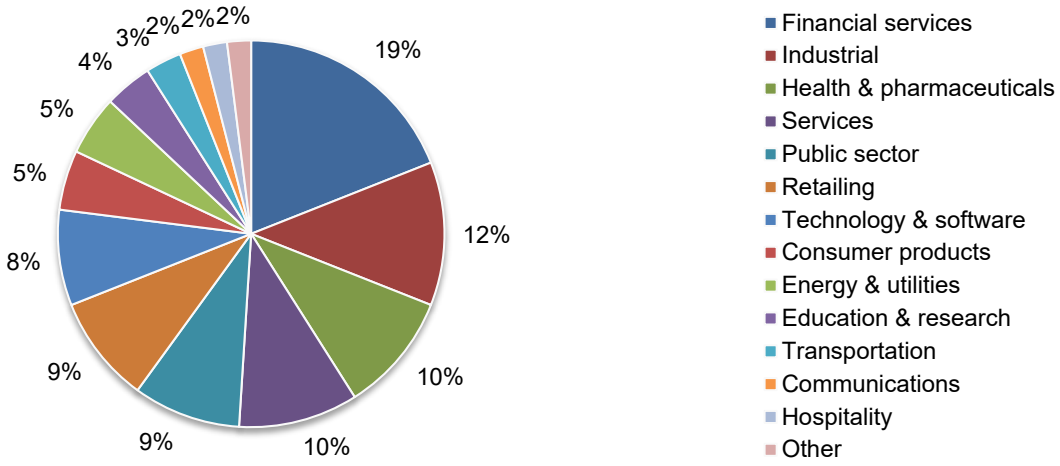
As Pie Chart 2 reveals, 70 percent of the respondents are from organisations with a global headcount of more than 1,000 employees.

**Pie Chart 2. Worldwide headcount of the organisation**




Pie Chart 3 reports the primary industry classification of respondents' organisations. This chart identifies financial services (19 percent of respondents) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by industrial sector (12 percent of respondents), health and pharmaceuticals (10 percent of respondents), services (10 percent of respondents), public sector (9 percent of respondents) and retailing (9 percent of respondents).

**Pie Chart 3. Primary industry focus**



# Part 4: Caveats

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

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

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

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

# Appendix: Detailed Survey Results

The following EMEA 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** | EMEA 2019 |
|---|---|
| Sampling frame | 14,842 |
| Total returns | 625 |
| Rejected surveys | 62 |
| Final sample | 563 |
| Response rate | 3.8% |

Screening questions

| S1. How familiar are you with cyber risks facing your company today? | EMEA 2019 |
|---|---|
| Very familiar | 25% |
| Familiar | 33% |
| Somewhat familiar | 42% |
| Not familiar (stop) | 0% |
| Total | 100% |

| S2. Are you involved in your company's cyber risk management activities? | EMEA 2019 |
|---|---|
| Yes, significant involvement | 34% |
| Yes, some involvement | 66% |
| No involvement (stop) | 0% |
| Total | 100% |

| S3. What best defines your role? | EMEA 2019 |
|---|---|
| Risk management | 29% |
| Finance, treasury & accounting | 33% |
| Corporate compliance/audit | 16% |
| Security/information security | 6% |
| General management | 9% |
| Legal (OGC) | 7% |
| None of the above (stop) | 0% |
| Total | 100% |

| S4. Are you involved in your company's enterprise risk management activities? | EMEA 2019 |
|---|---|
| Yes, significant involvement | 31% |
| Yes, some involvement | 69% |
| 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). | EMEA 2019 |
|---|---|
| Less than $1 million | 2% |
| $1 to 10 million | 10% |
| $11 to 50 million | 14% |
| $51 to 100 million | 23% |
| $101 to 500 million | 24% |
| $501 to 1 billion | 16% |
| $1 to 10 billion | 6% |
| More than $10 billion | 5% |
| Total | 100% |
| Extrapolated value | 1,063.97 |

| 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. | EMEA 2019 |
|---|---|
| Less than $1 million | 5% |
| $1 to 10 million | 14% |
| $11 to 50 million | 16% |
| $51 to 100 million | 23% |
| $101 to 500 million | 21% |
| $501 to 1 billion | 12% |
| $1 to 10 billion | 8% |
| More than $10 billion | 1% |
| Total | 100% |
| Extrapolated value | 685.80 |

| Q2b. What is the value of your largest loss (PML) to PP&E 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. | EMEA 2019 |
|---|---|
| Less than $1 million | 13% |
| $1 to 10 million | 23% |
| $11 to 50 million | 22% |
| $51 to 100 million | 20% |
| $101 to 500 million | 16% |
| $501 to 1 billion | 5% |
| $1 to 10 billion | 1% |
| More than $10 billion | 0% |
| Total | 100% |
| Extrapolated value | 158.37 |

| Q3. What percentage of this potential loss to PP&E assets is covered by insurance, including captives reinsured but not including captives not reinsured? | EMEA 2019 |
|---|---|
| Less than 5% | 0% |
| 5% to 10% | 1% |
| 11%to 20% | 5% |

| | |
|---|---|
| 21% to 30% | 6% |
| 31% to 40% | 9% |
| 41% to 50% | 12% |
| 51% to 60% | 19% |
| 61% to 70% | 15% |
| 71% to 80% | 12% |
| 81% to 90% | 11% |
| 91% to 100% | 10% |
| Total | 100% |
| Extrapolated value | 59% |

| Q4. What percentage of this potential loss to PP&E assets is self-insured, including captives not reinsured? | EMEA 2019 |
|---|---|
| Less than 5% | 9% |
| 5% to 10% | 14% |
| 11% to 20% | 15% |
| 21% to 30% | 17% |
| 31% to 40% | 12% |
| 41% to 50% | 14% |
| 51% to 60% | 8% |
| 61% to 70% | 9% |
| 71% to 80% | 1% |
| 81% to 90% | 1% |
| 91% to 100% | 0% |
| Total | 100% |
| Extrapolated value | 30% |

| 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? | EMEA 2019 |
|---|---|
| Less than 0.1% | 23% |
| 0.1% to 0.5% | 15% |
| 0.6% to 1.0% | 14% |
| 1.1% to 2.0% | 9% |
| 2.1% to 3.0% | 20% |
| 3.1% to 4.0% | 8% |
| 4.1% to 5.0% | 7% |
| 5.1% to 10.0% | 2% |
| More than 10.0% | 2% |
| Total | 100% |
| Extrapolated value | 1.8% |

| 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? | EMEA 2019 |
|---|---|
| Less than 0.1% | 69% |
| 0.1% to 0.5% | 15% |
| 0.6% to 1.0% | 10% |
| 1.1% to 2.0% | 2% |
| 2.1% to 3.0% | 2% |
| 3.1% to 4.0% | 1% |
| 4.1% to 5.0% | 0% |
| 5.1% to 10.0% | 1% |

| | |
|---|---|
| More than 10.0% | 0% |
| Total | 100% |
| Extrapolated value | 0.38% |

| 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? | EMEA 2019 |
|---|---|
| Disclosure as a contingent liability on the balance sheet (e.g., FASB 5) | 24% |
| Footnote disclosure in the financial statements | 42% |
| Discussion in the management letter | 17% |
| None – disclosure is not necessary | 11% |
| Other | 6% |
| 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. | EMEA 2019 |
|---|---|
| Less than $1 million | 5% |
| $1 to 10 million | 9% |
| $11 to 50 million | 14% |
| $51 to 100 million | 21% |
| $101 to 500 million | 17% |
| $501 to 1 billion | 16% |
| $1 to 10 billion | 6% |
| More than $10 billion | 4% |
| Total | 92% |
| Extrapolated value | 931.45 |

| 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. | EMEA 2019 |
|---|---|
| Less than $1 million | 8% |
| $1 to 10 million | 13% |
| $11 to 50 million | 15% |
| $51 to 100 million | 20% |
| $101 to 500 million | 17% |
| $501 to 1 billion | 14% |
| $1 to 10 billion | 10% |
| More than $10 billion | 3% |
| Total | 100% |
| Extrapolated value | 1,006.22 |

| Q9b. What is the value of your largest loss (PML) to information assets 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. | EMEA 2019 |
|---|---|
| Less than $1 million | 20% |
| $1 to 10 million | 23% |
| $11 to 50 million | 20% |
| $51 to 100 million | 12% |
| $101 to 500 million | 14% |
| $501 to 1 billion | 8% |
| $1 to 10 billion | 3% |
| More than $10 billion | 0% |
| Total | 100% |
| Extrapolated value | 268.33 |

| Q10. What percentage of this potential loss to information assets is covered by insurance, including captives reinsured but not including captives not reinsured? | EMEA 2019 |
|---|---|
| Less than 5% | 18% |
| 5% to 10% | 35% |
| 11% to 20% | 18% |
| 21% to 30% | 11% |
| 31% to 40% | 6% |
| 41% to 50% | 4% |
| 51% to 60% | 4% |
| 61% to 70% | 1% |
| 71% to 80% | 2% |
| 81% to 90% | 1% |
| 91% to 100% | 0% |
| Total | 100% |
| Extrapolated value | 18% |

| Q11. What percentage of this potential loss to information assets is self-insured, including captives not reinsured? | EMEA 2019 |
|---|---|
| Less than 5% | 0% |
| 5% to 10% | 1% |
| 11% to 20% | 4% |
| 21% to 30% | 3% |
| 31% to 40% | 4% |
| 41% to 50% | 10% |
| 51% to 60% | 17% |
| 61% to 70% | 21% |
| 71% to 80% | 22% |
| 81% to 90% | 13% |
| 91% to 100% | 5% |
| Total | 100% |
| Extrapolated value | 63% |

| 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? | EMEA 2019 |
|---|---|
| Less than 0.1% | 1% |
| 0.1% to 0.5% | 3% |
| 0.6% to 1.0% | 7% |
| 1.1% to 2.0% | 10% |
| 2.1% to 3.0% | 9% |
| 3.1% to 4.0% | 12% |
| 4.1% to 5.0% | 18% |
| 5.1% to 10.0% | 18% |
| More than 10.0% | 22% |
| Total | 100% |
| Extrapolated value | 5.4% |

| Q13. What is the likelihood your company will sustain a loss to information assets totaling 100 percent of PML over the next 12 months? | EMEA 2019 |
|---|---|
| Less than 0.1% | 8% |
| 0.1% to 0.5% | 11% |
| 0.6% to 1.0% | 9% |
| 1.1% to 2.0% | 14% |
| 2.1% to 3.0% | 13% |
| 3.1% to 4.0% | 14% |
| 4.1% to 5.0% | 19% |
| 5.1% to 10.0% | 10% |
| More than 10.0% | 2% |
| Total | 100% |
| Extrapolated value | 3.0% |

| 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? | EMEA 2019 |
|---|---|
| Disclosure as a contingent liability on the balance sheet (FASB 5) | 10% |
| Footnote disclosure in the financial statements | 41% |
| Discussion in the management letter | 8% |
| None – disclosure is not necessary | 34% |
| Other | 7% |
| 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 4 percent of an organisation's worldwide revenue? | EMEA 2019 |
|---|---|
| Yes, fully aware | 40% |
| Yes, somewhat aware | 50% |
| Not aware | 10% |
| 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. | EMEA 2019 |
|---|---|
| Yes | 41% |
| No [skip to Q17] | 59% |
| 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. | EMEA 2019 |
|---|---|
| Cyber attack that caused disruption to business and IT operations (such as denial of service attacks) | 55% |
| Cyber attack that resulted in the theft of business confidential information, thus requiring notification to victims | 32% |
| Cyber attack that resulted in the misuse or theft of business confidential information, such as intellectual properties | 26% |
| Negligence or mistakes that resulted in the loss of business confidential information | 36% |
| System or business process failures that caused disruption to business operations (e.g. software updates) | 40% |
| Other | 5% |
| Total | 194% |

| 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. | EMEA 2019 |
|---|---|
| Zero | 0% |
| Less than $10,000 | 8% |
| $10,001 to $100,000 | 7% |
| $100,001 to $250,000 | 19% |
| $250,001 to $500,000 | 24% |
| $500,001 to $1,000,000 | 13% |
| $1,000,001 to $5,000,000 | 8% |
| $5,000,001 to $10,000,000 | 9% |
| $10,000,001 to $25,000,000 | 6% |
| $25,000,001 to $50,000,000 | 3% |
| $50,00,001 to $100,000,000 | 3% |
| More than $100,000,000 | 0% |
| Total | 100% |
| Extrapolated value | 5,525,320 |

| Q16d. If yes, how has the above security exploit or data breach changed your company's concerns about cyber liability? | EMEA 2019 |
|---|---|
| More concerned | 69% |
| Less concerned | 11% |
| No change | 20% |
| 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? | EMEA 2019 |
|---|---|
| Increase | 67% |
| Decrease | 11% |
| Stay the same | 22% |
| Total | 100% |

| Q18a. From a business risk perspective, how do cyber risks compare to other business risks. Please select one best choice. | EMEA 2019 |
|---|---|
| Cyber liability is the number one or two business risk for my company | 21% |
| Cyber liability is a top 5 business risk for my company | 40% |
| 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 | 10% |
| Total | 100% |

| Q18b. How did you determine the level of cyber risk to your company? | EMEA 2019 |
|---|---|
| Completed a formal internal assessment | 23% |
| Completed an informal (ad hoc) internal assessment | 19% |
| Hired a third party to conduct an assessment or audit | 34% |
| Intuition or gut feel | 15% |
| 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? | EMEA 2019 |
|---|---|
| Yes | 30% |
| No [skip to Q20a] | 70% |
| Total | 100% |

| Q19b. If yes, what limits do you purchase | EMEA 2019 |
|---|---|
| Less than $1 million | 7% |
| $1 million to $5 million | 23% |
| $6 million to $20 million | 60% |
| $21 million to $100 million | 6% |
| More than $100 million | 4% |
| Total | 100% |
| Extrapolated value | 16.95 |

| Q19c. Is your company's cyber insurance coverage sufficient with respect to coverage terms and conditions, exclusions, retentions, limits and insurance carrier financial security? | EMEA 2019 |
|---|---|
| Yes | 58% |
| No | 29% |
| Unsure | 13% |
| Total | 100% |

| Q19d. How does your company determine the level of coverage it deems adequate? | EMEA 2019 |
|---|---|
| Formal risk assessment by in-house staff | 14% |
| Formal risk assessment conducted by the insurer | 16% |
| Formal risk assessment by a third party | 20% |
| Informal or ad hoc risk assessment | 10% |
| Policy terms and conditions reviewed by a third-party specialist | 19% |
| Maximum available from the insurance market | 20% |
| Other | 1% |
| Total | 100% |

| Q19e. What types of incidents does your organisation's cyber insurance cover? Please select all that apply. | EMEA 2019 |
|---|---|
| External attacks by cyber criminals | 80% |
| Malicious or criminal insiders | 74% |
| System or business process failures | 33% |
| Human error, mistakes and negligence | 29% |
| Incidents affecting business partners, vendors or other third parties that have access to your company's information assets | 31% |
| Other | 28% |
| Total | 275% |

| Q19f. What coverage does this insurance offer your company? Please select all that apply. | EMEA 2019 |
|---|---|
| Forensics and investigative costs | 48% |
| Notification costs to data breach victims | 55% |
| Communication costs to regulators | 43% |
| Employee productivity losses | 49% |
| Replacement of lost or damaged equipment | 58% |
| Revenue losses | 28% |
| Legal defense costs | 39% |
| Regulatory penalties and fines | 41% |
| Third-party liability | 53% |
| Brand damages | 21% |
| Other | 19% |
| Unsure | 28% |
| Total | 482% |

| 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. | EMEA 2019 |
|---|---|
| Access to cyber security forensic experts | 87% |
| Access to legal and regulatory experts | 85% |
| Access to specialised technologies and tools | 50% |
| Advanced warnings about ongoing threats and vulnerabilities | 44% |
| Assistance in the remediation of the incident | 66% |
| Assistance in the notification of breach victims | 49% |
| Identity protection services for breach victims | 34% |
| Credit monitoring services for breach victims | 40% |
| Assistance in reputation management activities | 49% |
| Other | 15% |
| Total | 519% |

| Q20a. Does your company plan to purchase standalone cyber insurance? | EMEA 2019 |
|---|---|
| Yes, in the next 12 months | 17% |
| Yes, in the next 24 months | 26% |
| Yes, in more than 24 months | 16% |
| No | 41% |
| Total | 100% |

| Q20b. If no, what are the two main reasons why your company is not planning to purchase standalone cyber security insurance? | EMEA 2019 |
|---|---|
| Premiums are too expensive | 34% |

| | |
|---|---|
| Coverage is inadequate based on our exposure | 38% |
| Too many exclusions, restrictions and uninsurable risks | 27% |
| Risk does not warrant insurance | 7% |
| Property and casualty policies are sufficient | 24% |
| Executive management does not see the value of this insurance | 19% |
| Unable to get insurance underwritten because of current risk profile | 24% |
| Other | 7% |
| Total | 180% |

| Q21. Who in your company is **most responsible** for cyber risk management? Please select your two top choices. | EMEA 2019 |
|---|---|
| CEO/board of directors | 3% |
| Chief financial officer | 5% |
| Business unit (LOB) leaders | 22% |
| Chief information officer | 21% |
| Chief information security officer | 12% |
| Risk management | 19% |
| Procurement | 8% |
| General counsel | 6% |
| Compliance/audit | 4% |
| 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? | EMEA 2019 |
|---|---|
| Yes | 60% |
| No (Please skip to Part 4) | 40% |
| Total | 100% |

| Q23. What is the total value of your company's IP assets such as trademarks, patents, copyrights, trade secrets and know-how? | EMEA 2019 |
|---|---|
| Less than $1 million | 0% |
| $1 to 10 million | 9% |
| $11 to 50 million | 18% |
| $51 to 100 million | 27% |
| $101 to 500 million | 28% |
| $501 to 1 billion | 14% |
| $1 to 10 billion | 3% |
| More than $10 billion | 1% |
| Total | 100% |
| Extrapolated value | 475.10 |

| Q24a. Did your company experience a material IP event in the past 24 months? | EMEA 2019 |
|---|---|
| Yes | 29% |
| No | 71% |
| 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 asset was involved in the event? | EMEA 2019 |
|---|---|
| Patent | 24% |
| Trade secret | 37% |
| Copyright | 30% |
| Other | 9% |
| Total | 100% |

| Q24c. If yes, what best describes the event? | EMEA 2019 |
|---|---|
| Challenge to company rights | 23% |
| Infringement of company rights | 41% |
| Allegation of company infringement of third-party rights | 36% |
| Total | 100% |

| Q25. How do IP risks compare to other business risks? | EMEA 2019 |
|---|---|
| IP risk is the number one or two business risk for my company | 17% |
| IP risk is a top 5 business risk for my company | 30% |
| IP risk is a top 10 business risk for my company | 33% |
| IP risk is not in the top 10 of business risks for my company | 20% |
| Total | 100% |

| Q26. Does your company's existing insurance policy (e.g., property, general liability or crime) cover any of the following IP events? | EMEA 2019 |
|---|---|
| A challenge to your company's IP assets, | 45% |
| Third-party infringement of your company's IP assets | 51% |
| An allegation that your company is infringing third-party IP rights | 39% |
| Our existing policy does not cover IP events | 38% |
| Total | 173% |

| Q27a. Does your company have a trade secret theft insurance policy as a complement to a cyber risk policy? | EMEA 2019 |
|---|---|
| Yes | 25% |
| No | 75% |
| 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? | EMEA 2019 |
|---|---|
| Very interested | 28% |
| Interested | 36% |
| Somewhat interested | 21% |
| Not interested | 15% |
| Total | 100% |

| Q28a. Does your company have an intellectual property liability policy? | EMEA 2019 |
|---|---|
| Yes | 33% |
| No | 67% |
| Total | 100% |

| Q28b. If no, what is your company's level of interest in purchasing an intellectual property liability policy? | EMEA 2019 |
|---|---|
| Very interested | 31% |
| Interested | 35% |
| Somewhat interested | 24% |
| Not interested | 10% |
| Total | 100% |

**Part 4. Role & Organisational Characteristics**

| D1. What level best describes your current position? | EMEA 2019 |
|---|---|
| Senior executive | 4% |
| Vice president | 6% |
| Director | 11% |
| Manager | 16% |
| Supervisor | 13% |
| Associate/staff | 8% |
| Technician | 31% |
| Contractor/consultant | 10% |
| Other | 1% |
| Total | 100% |

| D2. What is the worldwide employee headcount of your company? | EMEA 2019 |
|---|---|
| Less than 500 | 13% |
| 500 to 1,000 | 17% |
| 1,001 to 5,000 | 27% |
| 5,001 to 25,000 | 24% |
| 25,001 to 75,000 | 11% |
| More than 75,000 | 8% |
| Total | 100% |

| D3. What best describes your company's industry focus? | EMEA 2019 |
|---|---|
| Communications | 2% |
| Consumer products | 5% |
| Defense & aerospace | 1% |
| Education & research | 4% |
| Energy & utilities | 5% |
| Entertainment & media | 1% |
| Financial services | 19% |
| Health & pharmaceuticals | 10% |
| Hospitality | 2% |
| Industrial | 12% |
| Public sector | 9% |
| Retailing | 9% |
| Services | 10% |
| Technology & software | 8% |
| Transportation | 3% |
| Other | 0% |
| Total | 100% |

**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 organisations.

As a member of the **Council of American Survey Research Organisations (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.

# Contacts

## Aon's Cyber Solutions EMEA

**Onno Janssen**
Chief Executive Officer
Risk Consulting and Cyber Solutions EMEA
+49 (0) 40 3605 3608
onno.janssen@aon.de

**Vanessa Leemans**
Chief Commercial Officer
Cyber Solutions EMEA
+44 (0) 20 7086 4465
vanessa.leemans@aon.co.uk

**Spencer Lynch**
Managing Director, Cyber Security
Cyber Solutions EMEA
+44 (0)20 7061 2304
spencer.lynch@aon.co.uk

**David Molony**
Director, Cyber Risk
Cyber Solutions EMEA
+44 (0)7775 227 008
david.molony@aon.co.uk

**Shannan Fort**
Cyber Insurance Leader
Global Broking Centre
+44 (0)20 7086 7135
shannan.fort@aon.com

**Alistair Clarke**
Cyber Insurance Leader
Global Broking Centre
+44 (0)207 086 7357
alistair.clarke@aon.co.uk

## Aon's Intellectual Property Solutions EMEA

**Christian Gordon-Pullar**
Head of Intellectual Property
Intellectual Property Solutions EMEA
+442070861426
christian.gordon-pullar@aon.com

**Will Kier**
Director Intellectual Property
Intellectual Property Solutions EMEA
+442070860852
will.kier@aon.co.uk

# Contacts

## Cyber Country Leaders


**Mark Brannigan**
Cyber Leader
Cyber Solutions UK
mark.brannigan@aon.co.uk
+44 207 086 5847

**Johannes Behrends**
Cyber Leader
Cyber Solutions Germany
+4920870062250
Johannes.Behrends@aon.de

**Søren Carl Stryger**
Cyber Leader
Cyber Solutions Nordics
+45 32697168
soren.stryger@aon.dk

**Maarten van Wieren**
Cyber Leader
Cyber Solutions Netherlands
+31 6 82019225
maarten.van.wieren@aon.nl

**Timothee Crespe**
Cyber Leader
Cyber Solutions France
+33147830975
timothee.crespe@aon.com

**Vincenzo Aliotta**
Cyber Leader
Cyber Solutions Italy
+390245434316
Vincenzo.Aliotta@aon.it

**Claudia Beatriz Gomez**
Cyber Leader
Cyber Solutions Spain
+34913405645
claudiabeatriz.gomez@aon.es

**Karl Curran**
Cyber Leader
Cyber Solutions Ireland
+35312666424
Karl.Curran@aon.ie

# About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

For further information on our capabilities and to learn how we empower results for clients, please visit: aon.com



Empower Results®