2024 Intangible Versus Tangible Risks Comparison Report: De-risking AI, IP, and Cyber

Global Edition

Sponsored by Aon
Independently conducted by Ponemon Institute LLC

Contents

1. **Introduction**

   Artificial Intelligence Affects Cyber and IP Value and Risk

   A High-level Overview of the Consolidated Global Findings

2. **Key Findings**

   The Valuation of Property, Plant and Equipment (PP&E) Information Assets and Probable Maximum Loss

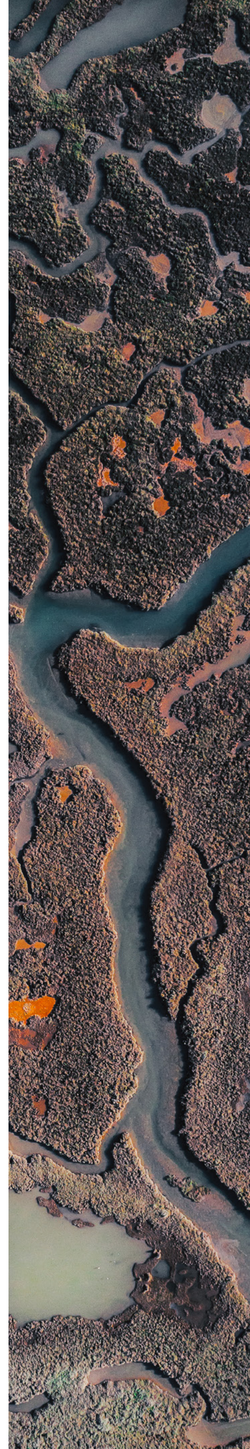
   Cyber Risk Exposure Increases

   The Use of Cyber Insurance to Mitigate the Financial Consequences of Data Breaches and Security Exploits

   The Vulnerability of IP Assets

3. **Appendix 1. Methods & Caveats**

4. **Appendix 2. Detailed Survey Results**



1

Introduction

1 Artificial Intelligence Affects Cyber and IP Value and Risk

A. Evolution of Intangible Risks

Generative artificial intelligence and cybersecurity are the top CEO concerns according to a 2024 survey[1]. While the European Union's new artificial intelligence law[2] was designed to bridge the gap between concerned intellectual property creators and AI providers, the measure may actually embolden copyright holders to go to court.[3] Additional 2024 intangible assets-related studies suggested the following:

- Misinformation and disinformation driven by artificial intelligence ("AI") pose the most severe global risks in the next two years.[4]
  - Providers of AI products/solutions range from some of the largest technology leaders in the world[5] to innovative AI assistant start-ups[6]
  - We are at the very early stages of a highly complex multi-decade AI transformation where the upside rewards and downside perils are uncertain[7]
  - From nonbinding guidelines to restrictions, AI regulation varies amongst nations[8]
- Intellectual Property ("IP") is one of the greatest sources of value creation in the corporate world, but it is also one of the most underutilized, which creates unintended enterprise level risks[9]
  - AI affects IP risk and uncertainty[10]
  - IP-rich UK firms uncertain/challenged by continued gap in funding[11]
  - IP infringement and legal complexities[12]
- Cyber incidents are the biggest threats facing organizations[13]
  - Businesses are 67% more likely to experience a cyber incident than a physical theft and almost five times as likely to have a cyber attack as a fire.[14]
  - Major cyberattack could cost the world $3.5 trillion: Lloyd's[15]
  - Cybercrime 'Greatest Threat' For Paris Olympics[16]

1 https://www.pwc.com/us/en/library/ceo-survey.html;

2 Key Considerations Regarding the Recently Passed EU Artificial Intelligence Act | Kramer Levin

3 Experts predict that the measure could actually encourage copyright holders to go to court EU's AI Act Disclosure Rules Could Spark Further Litigation - Law360

4 World Economic Forum Global Risks Report 2024

5 IBM led the field in applying for generative artificial intelligence patents over the last five years, filling over 500 more than runner Google and beating out household AI names such as Microsoft and OpenAI IBM Leads In AI Patent Applications Over Google, Microsoft - Law360

6 The Center for AI Policy has proposed a concrete actual bill that sets forth AI risk and safety levels and mandates AI insurance in some instances RTFB: On the New Proposed CAIP AI Bill - by Zvi Mowshowitz (substack.com)

7 Two of every three CXOs say GenAI will have existential impact: EY | News - Business Standard (business-standard.com)

8 How Nations Are Losing a Global Race to Tackle A.I.'s Harms - The New York Times (nytimes.com)

9 Intellectual Property and business value: making IP a C-suite priority | Dennemeyer.com; Corporate Governance Spotlight: Considerations for Protecting Valuable AI-Related Assets | Insights | Mayer Brown

10 Aon-AI and the Age of IP Risk and Uncertainty-whitepaper

11 Funding Innovation: Intellectual Property's Role in Unlocking the Potential of UK Scale-ups

12 Top Intellectual Property Issues to Think About in M&A Deals - Gibson Dunn

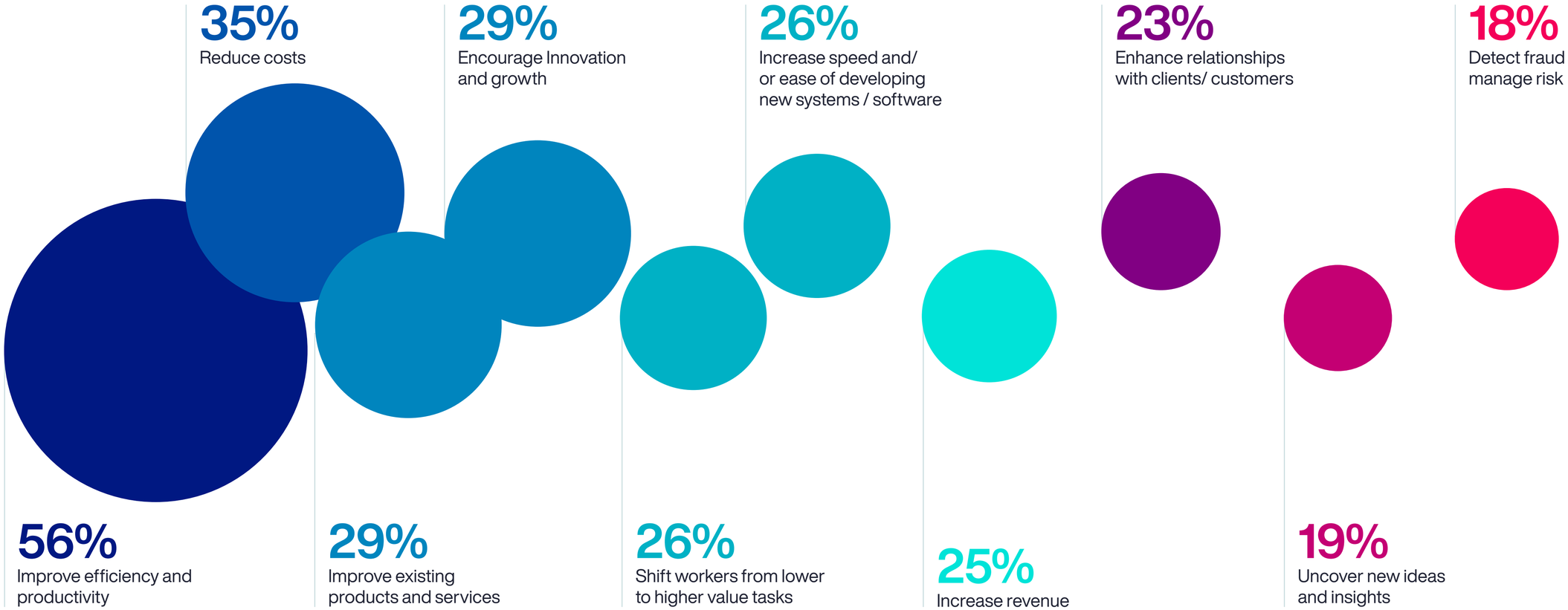
13 Global Risk Management Survey | Aon

14 One in five businesses have been victims of cyber attack in the last year - Aviva plc

15 Major cyberattack could cost the world $3.5 trillion: Lloyd's | Business Insurance; Possibility of a Billion-Dollar Systemic Cyber Event 'Is Real' (insurancejournal.com)

16 Cybercrime 'Greatest Threat' For Paris Olympics: Interpol Exec

Key benefits organizations hope to achieve with generative AI



*Q: What are the key benefits you hope to achieve through your generative AI efforts? (Oct/Dec. 2023) N (Total)=2,835

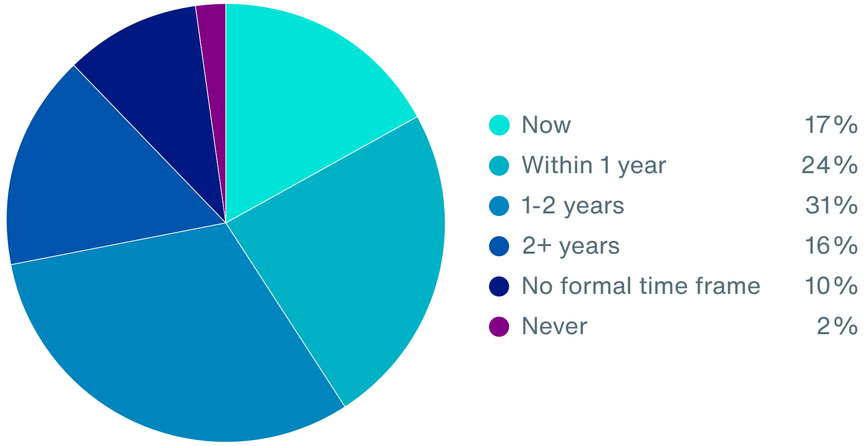
* Deloitte. "Now Decides Next: Insights from the leading edge of generative AI adoption." Deloitte, January 2024

B. Insurance helps to drive Intangible Asset Safety

Insurance mandates superior risk management practices and facilitates lower Total Cost of Risk[17] for today's evolving intangible assets. Increased safety resilience in artificial intelligence, cyber-related products/services, intellectual property and evolving technology digital assets/services might be rewarded with:

- Superior insurance coverage and lower premium options, which protects organizations' balance sheets against catastrophic losses;
- Third party, independent underwriters' review (and suggestions for improvements) of intangible asset providers' and users' risk management;
- A stamp of insurance carrier risk management verification, which differentiates organizations to meet customer contract requirements and satisfy regulatory obligations; and
- Risk capital[18] and human capital[19] service providers forced[20] to be more creative in terms of coverage,[21] sources of capital[22] and innovative solutions.[23]

Generative AI is impacting talent strategies now



**Q: When do you expect to make changes to your talent strategies because of generative AI? (Oct/Dec. 2023) N (Total)=2,835*

* Deloitte. "Now Decides Next: Insights from the leading ed ge of generative AI adoption." Deloitte, January 2024

> "In order to maximize the impact and effectiveness of our client's colleagues with the advent of AI, we use data, analytics and expertise across our Human Capital solutions to help clients make better workforce decisions aligned to business goals.
>
> **Christine Williams**
> Managing Director
> Greater New York Region
> Aon

[17] = Risk Financing + Loss Costs (Direct and Indirect) + Administrative Costs + Taxes and Fees (insurance buyers often focus too much on premium and not enough on comprehensive customized and "in-context" coverage and vetting reliable Insurers) whereby Risk Financing Costs include all insurance premiums and attendant costs; Direct Costs of Losses includes deductibles and claims that are anticipated and funded inside the organization's risk financing program (e.g., captive, deductible, or self-insurance programs); Indirect Loss Costs are a corresponding expense that is unfunded and, in some cases, unanticipated; Administrative Costs include claims management, risk control, and all other project costs such as data analytics; Taxes and fees are the various state taxes attached to insurance placements and are paid to governmental and regulatory bodies (e.g., state surplus lines or admission fees).

[18] AI Misuse Will Drive Cyber Insurance Demand, Actuary Says - Law360

[19] Artificial intelligence poses risk to HR practices | Business Insurance: Postings for AI-related roles are growing and touting higher pay: AI Talent Is in Demand as Other Tech Job Listings Decline - WSJ

[20] 37% of insurance CEOs think their organization will no longer be economically viable in 10 years, if it continues on its current course. The fundamental relevance of insurance to their customer base and also the double-edged effect of new technology pose the biggest threats. Ahead of the Curve: CEO Insights with PwC:

[21] Markets/Coverages: Aon Offers Financial Institutions Solution With Capacity of $100M (insurancejournal.com); $10 billion cyber-insurance sector fears war, AI, ransomware ahead | Fortune

[22] Revolutionizing risk transfer: the emergence of 144A cat bonds in captive | Captive International

[23] Aon teams with Rubrik to help companies maintain cyber resiliency - Reinsurance News; Multiple lines of insurance collaboration + superior risk management practices throughout the organization is recommended (Why Now is the Right Time to Customize Cyber and E&O Contracts

C. Better Decisions for Intangible Asset Investment and Protection

The most valuable organizations make risk management cost-benefit decisions predicated upon quantifiable, objective, fact-based data. The return on intangible assets investment is unclear[24]. The estimated ROI magnitude range is enormous[25]. A February 2024 report states that OpenAI CEO Sam Altman seeks to raise up to $7 trillion, which had many tech-industry observers raising eyebrows. The amount easily exceeds the market cap of any company—including Microsoft, which recently hit $3.1 trillion and surged past Apple as America's most valuable company.[26]

Similarly, the range of estimates regarding frequency and severity of potential losses from intangible assets is enormous[27]. The insurance industry typically builds actuarial loss models based on decades of data.[28]

However, due to the dynamic and fluid nature of intangible assets, we will never have decades worth of static intangible assets and risks data. Therefore, "retain risk" versus "transfer risk" decisions require fresh thinking.[29] Compliance with accepted industry standards should be the minimum baseline.[30]

In this report, we compare the relative:

- Value of certain tangible[31] compared to certain intangible assets[32]
- Quantification of potential losses from tangible compared to intangible assets
- Insurance protection of tangible compared to intangible assets

> "Large, complex, global organizations that execute a data and analytics-based enterprise risk management process are better positioned to maximize value and mitigate risks from their intangible assets.
>
> **Lori Goltermann**
> Chief Client Officer & CEO Global Enterprise Clients
> Aon

[24] After OpenAI launched Sora — a text-to-video AI model that converts text into a high-quality video up to a minute long -- a video of Meta Chief AI Scientist Yann LeCun went viral in which he said at Davos 2024 that he believes: "The future of AI is not generative."

[25] Thousands_of_AI_authors_on_the_future_of_AI.pdf (aiimpacts.org)

[26] Sam Altman Seeks Trillions of Dollars to Reshape Business of Chips and AI:

[27] "If I were advising governments, I would say that there's a 10 per cent chance AI will wipe out humanity in the next 20 years. I think that would be a reasonable number," Geoffrey Hinton, godfather of AI "Will Digital Intelligence Replace Biological Intelligence."

[28] Will AI Destroy the World? If Not, How Will It Affect Insurance? - Today's General Counsel (todaysgeneralcounsel.com)

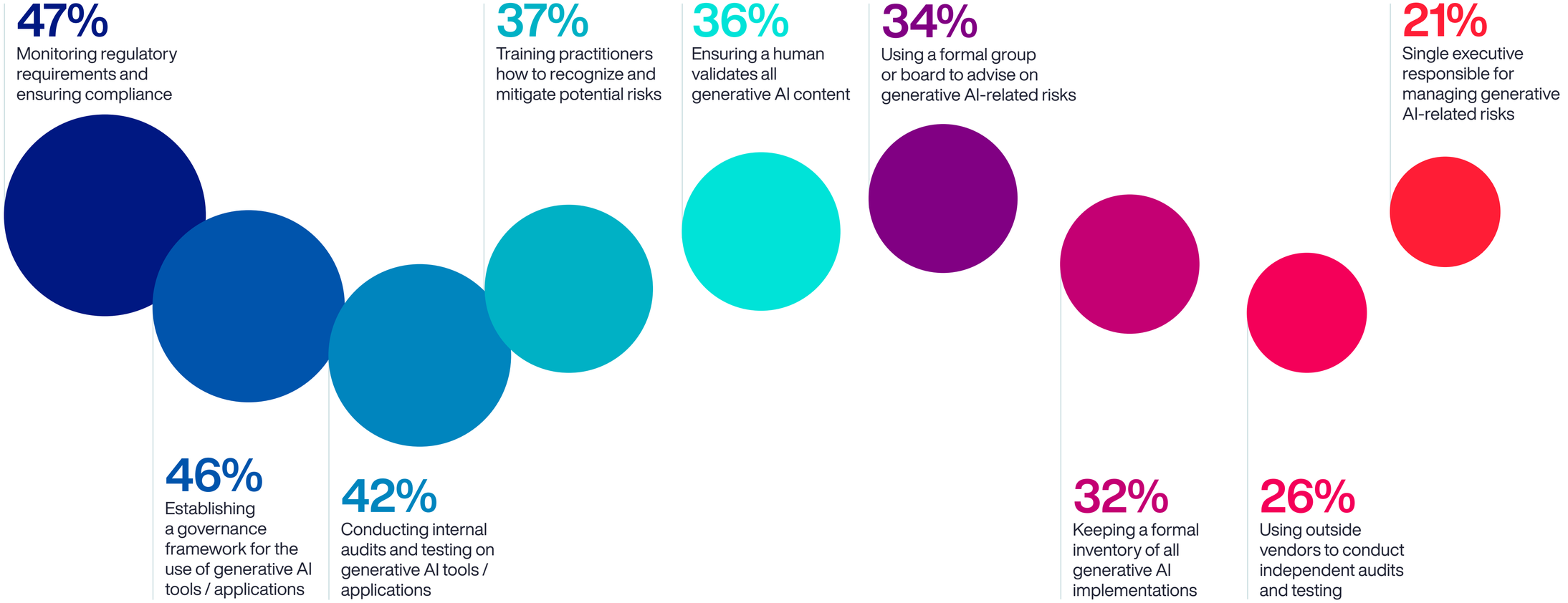
[29] The most calamitous failures of prediction usually have a lot in common. We focus on those signals that tell a story about the world as we would like it to be, not how it really is. We ignore the risks that are hardest to measure, even when they pose the greatest threats to our well-being. We make approximations and assumptions about the world that are much cruder than we realize. We abhor uncertainty, even when it is an irreducible part of the problem we are trying to solve." Silver, Nate. The Signal and the Noise: Why Most Predictions Fail – but Some Don't. United States. Penguin Group. 2012.

[30] NIST Cybersecurity Framework 2.0: 4 Steps to Get Started (darkreading.com);

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

[32] Information assets, intellectual property, and related digital technology, such as artificial intelligence. Additional intangible assets that lack physical substance are beyond the scope of this study, such as goodwill, brand equity, ESG (aon-2023-impact-report.pdf), DE & I, licensing, and (except as included within the calculation of trade secrets), customer lists and research and development. 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.

Managing generative AI implementation risk



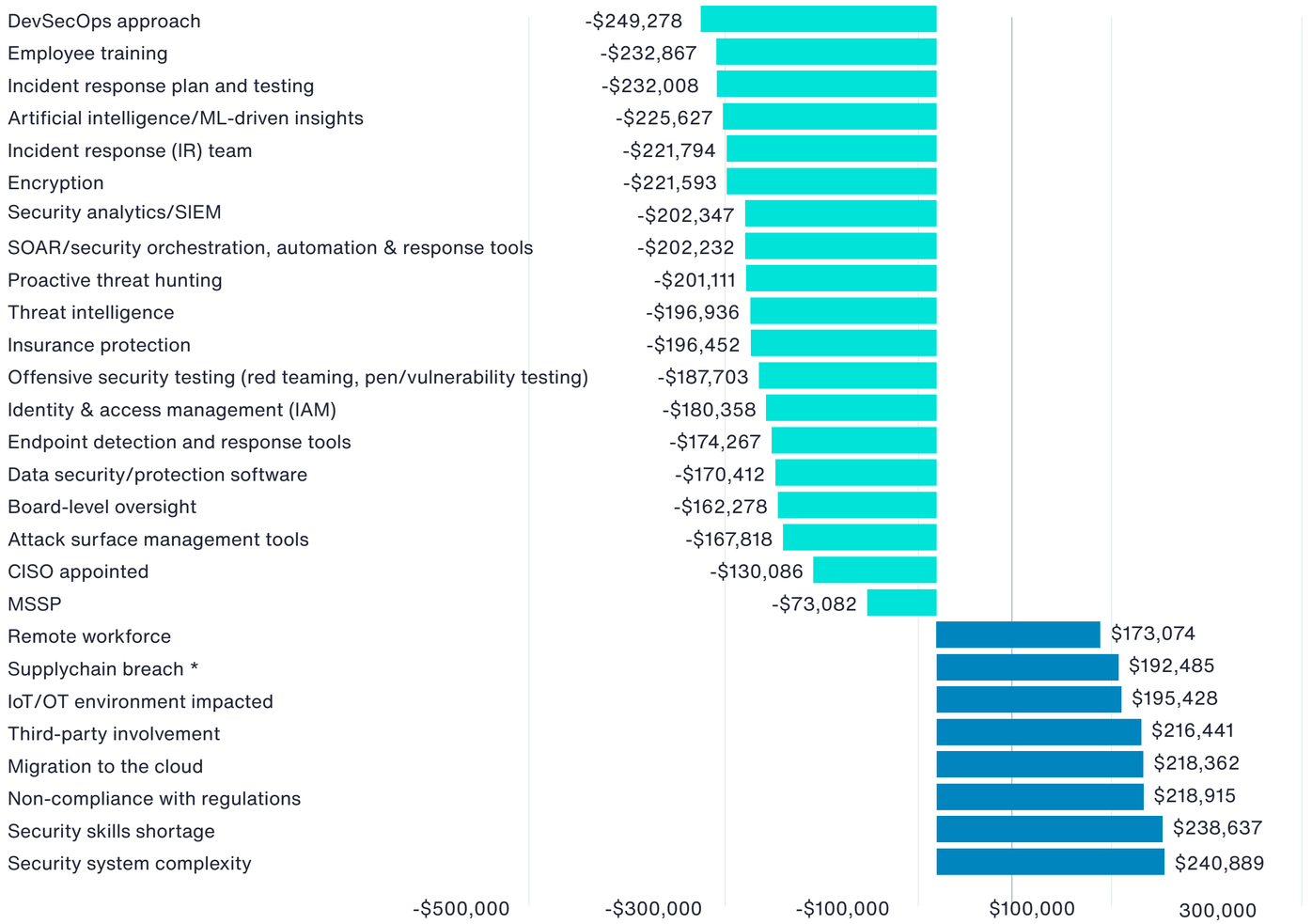
*Q: What is your organization currently doing to actively manage the risks around your generative AI implementations? (Oct/Dec. 2023) N (Total)=2,835

* Deloitte. "Now Decides Next: Insights from the leading edge of generative AI adoption." Deloitte, January 2024

How can organizations make better decisions regarding allocation of their finite resources to protect against tangible and intangible perils? At its most basic, insurance is a financial instrument — a way to manage the cost of future risk. It's pretty simple. On the one hand, you can self-insure risk, holding onto it yourself and bearing the full cost of a loss (unless you have transferred it contractually in an indemnity agreement with a counterparty). Or you can pay an insurance company a premium to take some or all of that risk from you. The biggest challenges to address intangible assets risks are identification/quantification of the exposures and then taking a different, proactive mindset to mitigate such risks.

For example, there are recent studies that set forth the relative ROI of various cyber risk management mechanisms. Allocating cyber resiliency resources based on their relative increase/decrease effect on expected losses is a better decision-making mindset. The following chart sets forth factors that decrease/increase the total cost of a data breach on an average relative basis.[33]

Factors that can decrease or amplify the cost of a data breach (measured in USD)

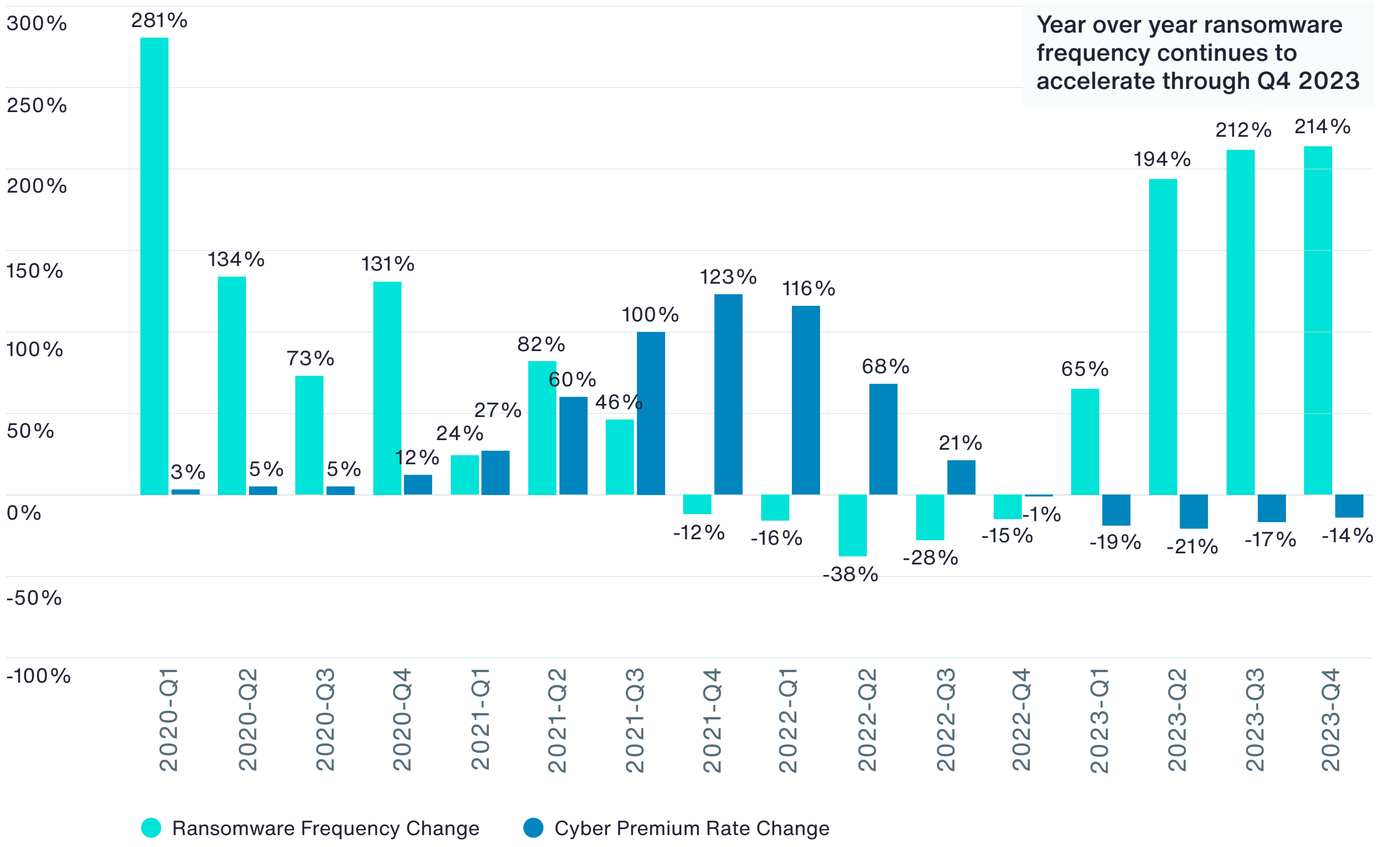


[33] https://www.ibm.com/reports/data-breach

Given the intersection of tangible and intangible assets in many instances with the advent of the Internet of Things/5G,[34] growth of AI robotics, metaverse/Web 3.0,[35] virtual reality gaming, quantum computing, blockchain,[36] etc. it is difficult to separate the actuarial modelling of intangible and tangible risks – but it is necessary and useful. For instance, the tangible assets of Property, Plant & Equipment (despite lower relative value) are insured three times greater (60 percent vs 19 percent) than information assets.[37]

Cyberattacks, especially ransomware[38] are surging[39] despite increased cyber security.[40] Yet, cyber insurance pricing continues to decrease due to insurance carrier competition. Something has got to give.

Ransomware Frequency & Cyber Premium Rates: Yo-Y Change



Source: Risk Based Security, analysis by Aon. Data as of 1/1/2024; Claim count development may cause these percentages to change over time

[34] The Role Of The Insurance Industry In The Connected Era (forbes.com)

[35] 02520_BRG_A4_Report_The-Metaverse_06.23.2023.pdf (thinkbrg.com)

[36] Goldman Sachs digital assets chief sees 'huge appetite' for blockchain assets | Reuters

[37] See Figure 1 and Figure 5 hereinbelow: 2024 Aon/Ponemon Intangible vs. Tangible Risks Report.

[38] Ransomware landscape overview 2023 | Cybernews

[39] Data breaches reached new highs in 2023, smashing old record | PropertyCasualty360

[40] Why Data Breaches Spiked in 2023 (hbr.org)

Generative AI, which creates material such as images, music and text, results in perils such as intellectual property infringement,[41] hallucinations,[42] security/ privacy breaches[43] and bias[44] garnering most of the litigation news. However, some developing AI products, such as AI robots, face perils that are different from content misinformation, such as mistakes that can lead to bodily injury and/or tangible property damage. AI raises particular risk transfer challenges because AI exposures may implicate potential losses that do not fit neatly in to existing insurance buckets.[45] Courts may struggle to extend or limit existing tort/case, statutory and contract law with respect to AI. Where there are multiple AI providers, users, vendors, distributors, customers and others in the supply chain,[46] allocation of liability looms large.

Furthermore, most traditional insurance policies do not explicitly address AI-related risks. Insureds should clarify the scope of coverage and potential exclusions. The "silent cyber" cases, whereby historical property, crime, and general liability policies did not affirmatively "cover" or "exclude" cyber perils, resulted in extensive litigation between insurance companies and insureds.

Insurance policies address artificial intelligence perils in one of three ways:

- Affirmative coverage[47]
- Specific exclusions[48]
- Silent,[49] which creates ambiguity[50]

> "With all that's going on in the economy, whether its artificial intelligence, whether it's intellectual property, whether it's cyber dependency, or regulatory change related to intangible assets, our ability to continue to innovate, to create new products to bring new services to our clients, effectively stay one step ahead of where the economy and where these issues are going, is vital to us being able to provide advice and products to make better decisions for their businesses.
>
> **Eric Andersen**
> President, Aon

[41] Google hit with $270M fine in France as authority finds news publishers' data was used for Gemini | TechCrunch

[42] Hallucinations are "made up" output, a type of error that brings about novel perils, and novel cases, such as Mata v Avianca, Battle v Microsoft, and Walters v Op.

[43] How AI use in cyber attacks affects insurers' risk exposure (pinsentmasons.com)

[44] Insurance to drive AI reforms with the risk of increased litigation - Clyde and Co (clydeco.com)

[45] Generative AI expected to impact many different insurance lines: Aon - Reinsurance News

[46] Risk Management Magazine - Organizations Unprepared for Third Party Risks (rmmagazine.com); Aon launches Partner Risk Insights to help businesses digitize third-party risk management (mediaroom.com)

[47] https://www.munichre.com/en/solutions/for-industry-clients/insure-ai.html

[48] Beazley, for example, is proposing AI coverage restrictions for SME placements: Microsoft faces 'uninsurable' GDPR fine in Ireland | Insurance Business UK (insurancebusinessmag.com)

[49] Common Cyber Claims Insured Outside Of Cyber Policies | GB&A (gbainsurance.com)

[50] Merck And Insurers Settle $1.4B Cyberattack Coverage Case - Law360

Artificial Intelligence: Insurance Coverage Gap Analysis

	Media Liability	Tech Errors & Omissions, MPL, PI	Product Liability	General Liability	Intellectual Property	Standalone Cyber Liability	Crime	D&O	Employment
AI Peril									
Third-Party Damages Liability for Faulty Product or Service	●	●	●	●	●	●	●	●	●
Copyright, Trademark or Service Mark Infringement	●	●	●	●	●	●	●	●	●
Patent Infringement	●	●	●	●	●	●	●	●	●
Discrimination/bias	●	●	●	●	●	●	●	●	●
Defamation, Libel, Slander	●	●	●	●	●	●	●	●	●
Bodily Injury	●	●	●	●	●	●	●	●	●
Tangible Property Damage	●	●	●	●	●	●	●	●	●
Privacy and Security Breaches	●	●	●	●	●	●	●	●	●
Loss of Finanical Assets	●	●	●	●	●	●	●	●	●
Market Manipulation	●	●	●	●	●	●	●	●	●
Deepfake	●	●	●	●	●	●	●	●	●
Robotics	●	●	●	●	●	●	●	●	●
Product Recall	●	●	●	●	●	●	●	●	●
Business Interruption	●	●	●	●	●	●	●	●	●
Breach of Director's or Officers' Duties	●	●	●	●	●	●	●	●	●

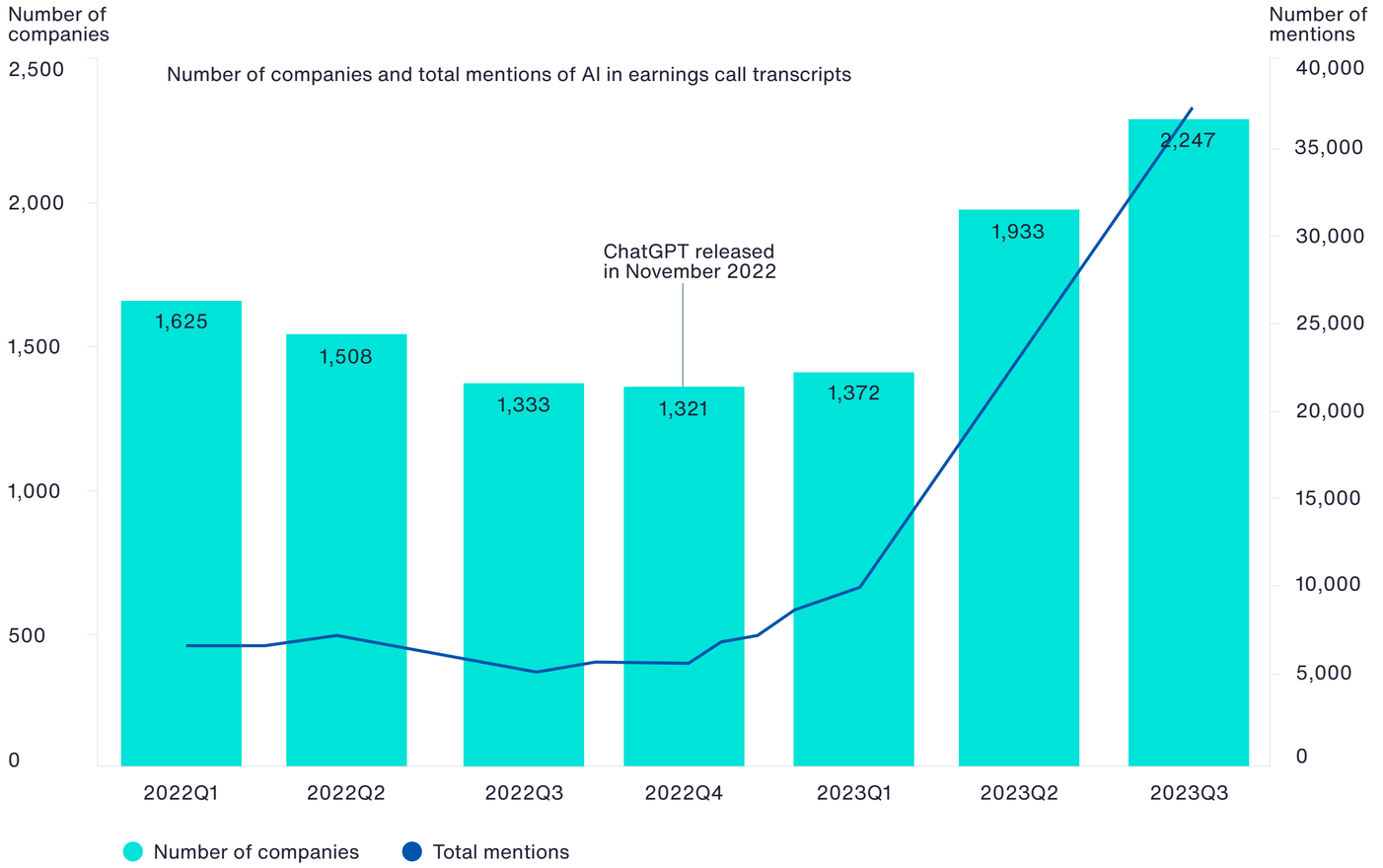
● Generally Available ● Limited ● Excluded, unless customized contingent liability added

Risk management typically considers frequency and severity of perils. With respect to intangible assets (especially artificial intelligence and cyber), we should add velocity of evolving risk profiles. Organizations must proactively address intangible risks through tailored insurance policies that align with their unique circumstances.[51] As the intangible assets landscape continues to evolve, a collaborative effort between stakeholders,[52] led by legal counsel, risk management, finance/treasury, business units, information technology, and compliance - and mandated by management - is crucial to help ensure that the potential perils of intangible assets are effectively managed and mitigated.

Interestingly, the S&P companies that cited “AI” on Q4 2023 earnings calls have seen a better average stock price performance over the past 12 months compared to the S&P 500 companies that did not.[53]

Can AI Have Your Attention?

AI mentions in earnings call transcripts increased **6x** since release of ChatGPT in Nov.2022.



Source: Accenture “Technology Vision 2024: Human by Design: How AI Unleashes the Next Level of Human Potential.” Accenture, 2024

[51] Note that procuring a robust cyber insurance program could be a consideration in determining whether a cyber incident is “material” for purposes of the new SEC four day mandatory disclosure rule (Aon | Financial Services Group - SEC Sharpens Focus on Cybersecurity with New Disclosure Rule). For instance, assume that two organizations in the same industry, geography and revenue band suffer an identical cyber incident = $25 million in potential losses each. Company “A” has a $50 million limits cyber insurance program and Company “B” declined to purchase cyber insurance due to budget cuts (and Company “B” does not have any other insurance policy that addresses the loss). There is an argument that Company “A” may not be required to disclose the cyber incident as “material” (because it is protected against the loss by its cyber insurance policy) while Company “B” not only has to disclose the incident within 4 days, but will also suffer the uninsured $25 million hit to its balance sheet. (Why Private Companies Should Pay Attention to the SEC’s New Cybersecurity Disclosure Rules (cosecure.com)

[52] For Cyber Readiness, the CISO and CRO Join Forces (aon.com)3

[53] The Growing Use of Artificial Intelligence: D&O Risks and Potential Coverage Solutions - Aon Financial Services Group; Fact Set Earnings Insight Report

1 A High-level Overview of the Consolidated Global Findings

Most organizations (67 percent of respondents) use or intend to use (19 percent) artificial intelligence (AI) products or services. There is growing interest in adopting AI to strengthen their organizations' security posture. According to a recent Ponemon Institute study, AI improves IT security staff's productivity and the ability to detect previously undetectable threats.[54] **Sixty-four percent** of respondents say their organizations use or plan to use (21 percent) cryptocurrency or non-fungible token assets.

The Valuation of PP&E, Information Assets and Probable Maximum Loss (PML)

The value of Information Assets Probable Maximum Loss ("PML")[55] is higher than PP&E. Organizations estimate the average PML resulting from stolen or destroyed information at approximately $1,155 million. In contrast, the average value of the largest loss that could result from damage or total destruction of PP&E is approximately $846 million. Business disruption has a greater impact on information assets ($324 million)[56] than on PP&E ($144 million).

The value of information assets is higher than tangible asset values. The average total value of information assets is $1,239 million, which is slightly higher thanthe average total value of PP&E, which is approximately $1,088 million for the organizations represented in this research.

The likelihood of a loss is higher for information assets than for PP&E. Organizations estimate the likelihood that they will sustain a loss relating to information assets totaling no more than 50 percent of PML over the next 12 months at 5 percent and 100 percent of PML at 3 percent. The likelihood of a loss relating to PP&E totaling no more than 50 percent of PML over the next 12 months is an average of 2 percent and at 100 percent of PML it is 0.55 percent.

Insurance coverage is higher for tangible assets (PP&E) than for intangible assets (information assets). On average, approximately 60 percent of PP&E assets are covered by insurance and approximately 32 percent of PP&E are self-insured. While the likelihood of a loss is higher for information assets than for PP&E, only an average of 19 percent of information assets are covered by insurance, while self-insurance is higher for information assets at 58 percent.

Thirty percent of respondents believe no disclosure of a material loss to information assets not covered by insurance is required. This is a stunning data point given that the U.S. Securities and Exchange Commission's new Form 8-K rules for reporting material cybersecurity incidents took effect (other than for smaller reporting companies) December 18, 2024.[57] In contrast, only 14 percent of respondents believe no disclosure of a material loss to PP&E assets not covered by insurance is required.

Forty-two percent of respondents say their organizations would disclose a material loss to information assets and PP&E in a footnote in the financial statements. Twenty-one percent of respondents would disclose a material loss to PP&E as a contingent liability on the balance sheet (FASB 5) and only 13 percent would disclose a material loss to information assets as a contingent liability on the balance sheet.

[54] The 2024 Study on the State of AI in Cybersecurity, conducted by Ponemon Institute, sponsored by MixMode, February 2024.

[55] 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).

[56] While the survey results suggest Probable Maximum Loss at approximately $324 million, a growing number of organizations are using Risk Decision Platform Analysis and Cyber Modeling to suggest potential losses in excess of $500 million to over $1 billion and are seeking cyber insurance limit premium quotes and policy terms for such amounts.

[57] Aon | Financial Services Group - SEC Sharpens Focus on Cybersecurity with New Disclosure Rule

Cyber Risk Exposure Increases

Fifty-six percent of organizations had a material[58] or significantly disruptive security exploit or data breach one or more times in the past 24 months. The average total financial impact of these incidents was $5 million.[59] Sixty-six percent of these respondents say the incident increased their company's concerns over cyber liability.

Data breaches and security exploitations caused by negligence or mistakes increases significantly. The most frequent type of incident was one that was caused by negligence or mistakes that resulted in the loss of business confidential information (53 percent of respondents). Fifty percent of respondents say it was a cyberattack that caused a disruption to business and IT operations. Forty-seven percent of respondents say a system or business process failure caused disruption to business operations.

More organizations are becoming aware of the economic and legal consequences from an international data breach or security exploit. Eighty-nine percent of respondents are either fully (41 percent) or somewhat aware (48 percent) of the consequences that could result from a data breach or security exploit in other countries in which their company operates. Only 11 percent of respondents say they are not aware of the consequences, a significant decline from 20 percent in 2017.[60]

The use of third parties to assess cyber risk has declined. To determine the cyber risk to their company, 27 percent of respondents say the company hired a third party to conduct an assessment or audit, a decrease from 33 percent. However, formal internal assessments are slowly increasing (from 15 percent in 2015 to 25 percent of respondents this year). Twenty-two percent of respondents say their organizations did an informal (ad hoc) internal assessment. Only 18 percent of respondents say it was based on intuition or gut feel.

Organizations' exposure to cyber risk is increasing. While organizations are predicting that their cyber risk exposure will increase, 32 percent of respondents say there is no plan to purchase standalone cyber insurance. Sixty-nine percent of respondents believe their company's exposure to cyber risk will increase and 21 percent of respondents say it will stay the same. Only 10 percent of respondents expect it to actually decrease.

Only 44 percent of respondents are prepared for a cyber or IP "black swan". A black swan is an event that is an "outlier" as it lies outside the realm of regular expectations. According to the research, 44 percent of respondents say ab external cyber and/or intellectual property incident can become a Black Swan for the firm.[61]

[58] 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.

[59] 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 reputational damages.

[60] The Price of Data Security: A guide to the insurability of GDPR fines across Europe (3rd Edition, May 25, 2020).

[61] Grey Swans on the Horizon; AI, Cyber, Pandemics, and ET Scenarios (forbes.com)

The Use of Cyber Insurance to Mitigate the Financial Consequences of Data Breaches and Security Exploits.[62]

Cyber liability is a top 10 business risk. However, 70 percent of respondents say their organizations are still not purchasing standalone cyber insurance coverage. The average limit for those organizations purchasing cyber insurance is $17 million.

More than half of respondents (53 percent) say it was error and negligence that was the root cause of their data breach or security exploit, yet only 33 percent of respondents say their insurance covers these types of incidents. Seventy-eight percent of respondents say it covers external attacks by cyber criminals and 76 percent of respondents say it was malicious or criminal insiders.

Few cyber insurance policies cover ransomware payments and costs to recover from the attack. The top three costs are forensics and investigative costs, replacement of lost or damaged equipment and notification costs to data breach victims, 68 percent, 62 percent and 59 percent of respondents respectively). Only 34 percent of respondents say their insurance reimburse costs related to ransomware.

> “New digital platforms can serve as a simple command center for risk managers, procurement officers and general counsels to manage third-party network risk, including suppliers, vendors, and commercial tenants.
>
> **Jillian Slyfield**
> Chief Innovation Officer
> Aon

[62] Insurance should complement cybersecurity, ‘not the other way around’ (siliconrepublic.com)

Vulnerability of IP Assets

As a complement to a cyber risk policy, few organizations have a trade secret theft insurance policy and/or an intellectual property liability policy. Only 35 percent of respondents say they have a trade secret theft insurance policy and a similar percentage of respondents (34 percent) have an intellectual property liability policy.

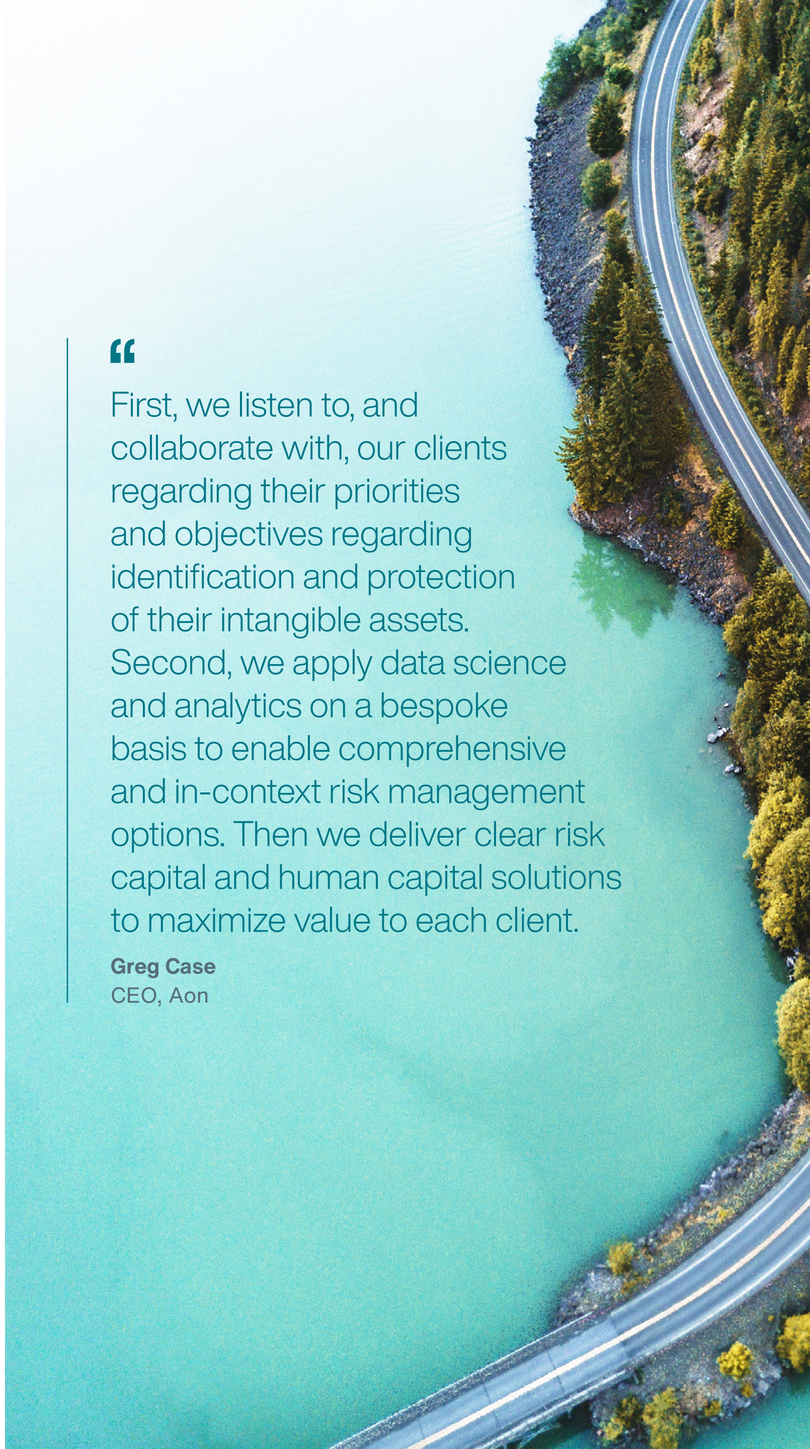
Most organizations' insurance does not cover all consequences of an IP event. Only 32 percent of respondents say it covers an allegation that their company is infringing third-party IP rights. Thirty-six percent of respondents report that their policy covers a challenge to their company's IP assets while 33 percent of respondents say it covers third-party infringement of their company's IP assets. One-third of respondents (33 percent) say the policy does not cover IP events.[63]

The percentage of respondents who say their organizations have a strategy to manage IP risks increases. Sixty-one percent of respondents say their enterprise risk management activities include risks to their IP, a significant increase from 53 percent of respondents in 2022.

IP security exploits involving patents has increased significantly. In the past two years, 50 percent of respondents say their company experienced a material IP event.[64] The IP material event can be best described as an infringement of company rights (37 percent of respondents), challenge to company rights (33 percent of respondents) or an allegation of an organization's infringement of third-party rights (30 percent of respondents).

Most of these incidents involved trade secrets (36 percent of respondents). However, exploits involving patent rights increased from 25 percent of respondents to 32 percent of respondents. Organizations 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 $600 million. An average of 47 percent of organizations' total assets are IP assets.

While most organizations do not have specific IP insurance policies, there is significant interest in purchasing them. Sixty-four percent of respondents are very interested or interested in purchasing a trade secret insurance policy and 62 percent say their organizations would purchase an intellectual property liability policy.



> "First, we listen to, and collaborate with, our clients regarding their priorities and objectives regarding identification and protection of their intangible assets. Second, we apply data science and analytics on a bespoke basis to enable comprehensive and in-context risk management options. Then we deliver clear risk capital and human capital solutions to maximize value to each client.
>
> **Greg Case**
> CEO, Aon

[63] A detailed review of insurance policies indicates that IP coverage is much lower than survey responses reflect – especially for patent infringement and trade secrets theft, which detailed reviews show less than 5% of organizations have insurance coverage for trade secrets or patents.

[64] "IP event" includes "challenge to company rights," "infringement of company rights," and "allegation of company infringement of third-party rights" pursuant to Question 25c in the Appendix hereto.

Risks to Intellectual Property (IP)[65]

Intellectual Property Insurance: Scope and Gaps. *As AI liability issues evolve, insurance is innovating to address risks to AI providers and users.

Exposures	Intellectual Property Liability	General Liability	E&O/ Professional Liability	Cyber Liability	Media Liability	Kidnap and Ransom	Reps and Warranties (Transaction Based)
IP Liability Risks							
Patent Infringement	Cover available	Excluded	Excluded	Excluded	Excluded	Excluded	Cover for the Rep on past issues, no go-forward
Trade Secret Misappropriation	Cover available, outside the scope of some core policies	Excluded	Excluded	Excluded	Excluded	Excluded	Cover for the Rep on past issues, no go-forward
Trademark/Trade Dress/ Trade Name Infringement	Cover available (AI coverage available*)	Limited to Advertising Injury, Products and Services Excluded	Limited to Advertising Injury tied to the Performance of Professional Services	Content disseminated through the website or internet	Limited to Content	Excluded	Cover for the Rep on past issues, no go-forward
Copyright Infringement	Cover available (AI coverage available)	Limited to Advertising Injury, Products and Services Excluded	Limited to Advertising Injury tied to Professional Services	Content disseminated through the website or internet	Limited to Content	Excluded	Cover for the Rep on past issues, no go-forward
Third Party IP disclosure/ release (breach of NDA/ confidentiality agreement)	Cover can be endorsed for unintentional acts	Excluded	Limited to Professional Services for unintentional acts	Cover for unintentional breach of NDA, under Security & Privacy Liability	Unintentional disclosure of private facts	Excluded	Cover for the Rep on past issues, no go-forward
Contractual Indemnities of IP Risk	Cover available for IP Infringement of Insured's Product	Excluded	Limited to Advertising Injury tied to Professional Services	Limited to Content disseminated through website or internet	Limited to Content	Excluded	Cover for the Rep on past issues, no go-forward
Breach of IP license agreement	Can be endorsed, limited availability	Excluded	Excluded	Excluded	Unintentional breach of a license	Excluded	Cover for the Rep on past issues, no go-forward
IP Ownership Risks							
IP ownership representations	Cover available	Excluded	Excluded	Excluded	Excluded	Excluded	Cover for the Rep on past issues, no go-forward
Loss of IP value due to theft/ misappropriation/other loss	Solutions being built	Excluded	Excluded	Excluded	Excluded	Excluded	Cover for the Rep on past issues, no go-forward
IP Enforcement costs	Limited availability, only outside of the U.S.	Excluded	Excluded	Excluded	Excluded	Excluded	Cover for the Rep on past issues, no go-forward
Loss of IP due to legal challenge/Loss of Revenue	Limited availability	Excluded	Excluded	Excluded	Excluded	Excluded	Cover for the Rep on past issues, no go-forward

[65] Only 19% of companies report that their patent portfolios are the right size – one of four key findings discovered in the Cipher report Cipher

2

Key Findings

2 The Valuation of Property, Plant and Equipment (PP&E) Information Assets and Probable Maximum Loss

This report features the consolidated findings of all regions in this research. Separate reports will be created for the North America, EMEA, Asia-Pac and LATAM regions. The complete global consolidated audited findings are presented in the Appendix of this report.

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.[66] We have organized the report according to the following topics:

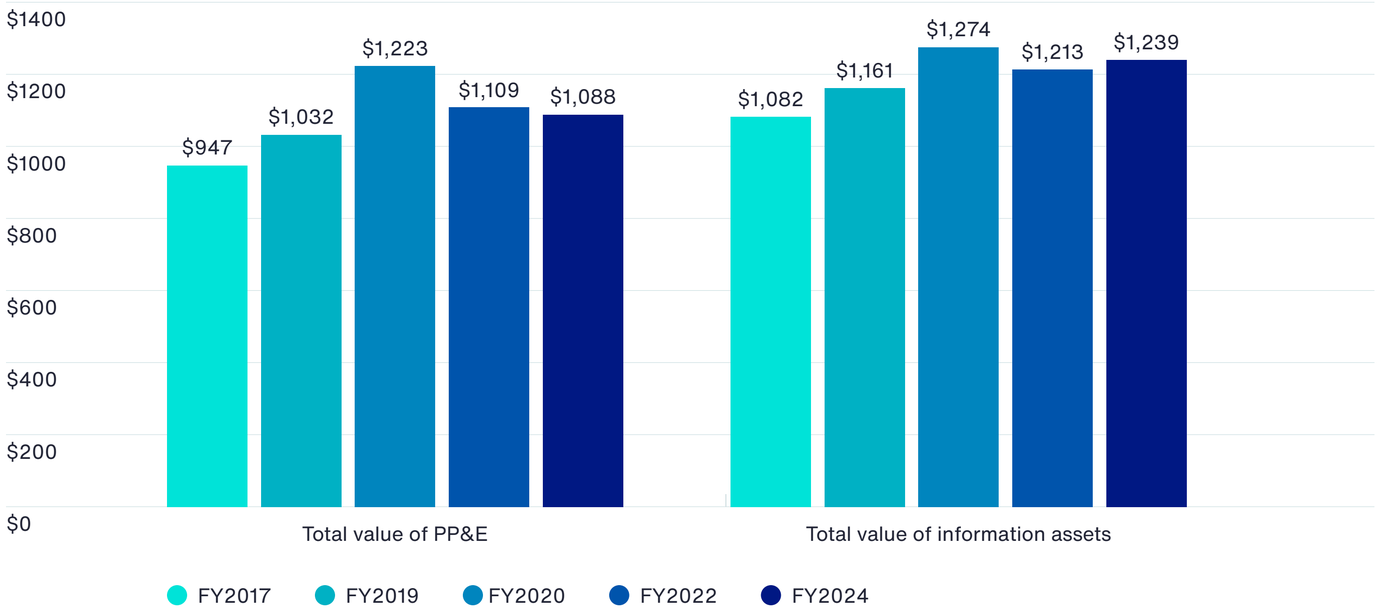
- The Valuation of Property, Plant and Equipment (PP&E), Information Assets and Probable Maximum Loss (PML)
- Cyber Risk Exposures Increase
- The Use of Cyber Insurance to Mitigate the Financial Consequences of Data Breaches and Security Exploits
- The Vulnerability of IP Assets

The Valuation of Property, Plant and Equipment (PP&E), Information Assets and Probable Maximum Loss (PML)

Organizations continue to value information assets slightly higher than they do PP&E. According to Figure 1, on average, the total value of PP&E, including all fixed assets plus SCADA and industrial control systems is approximately $1,088 million for the organizations represented in this research. The average total value of information assets, which includes customer records, employee records, financial reports, analytical data, source code, models, methods and other intellectual properties, is slightly higher, at $1,239 million.

Figure 1. The total value of PP&E and information assets

Extrapolated value ($ millions)



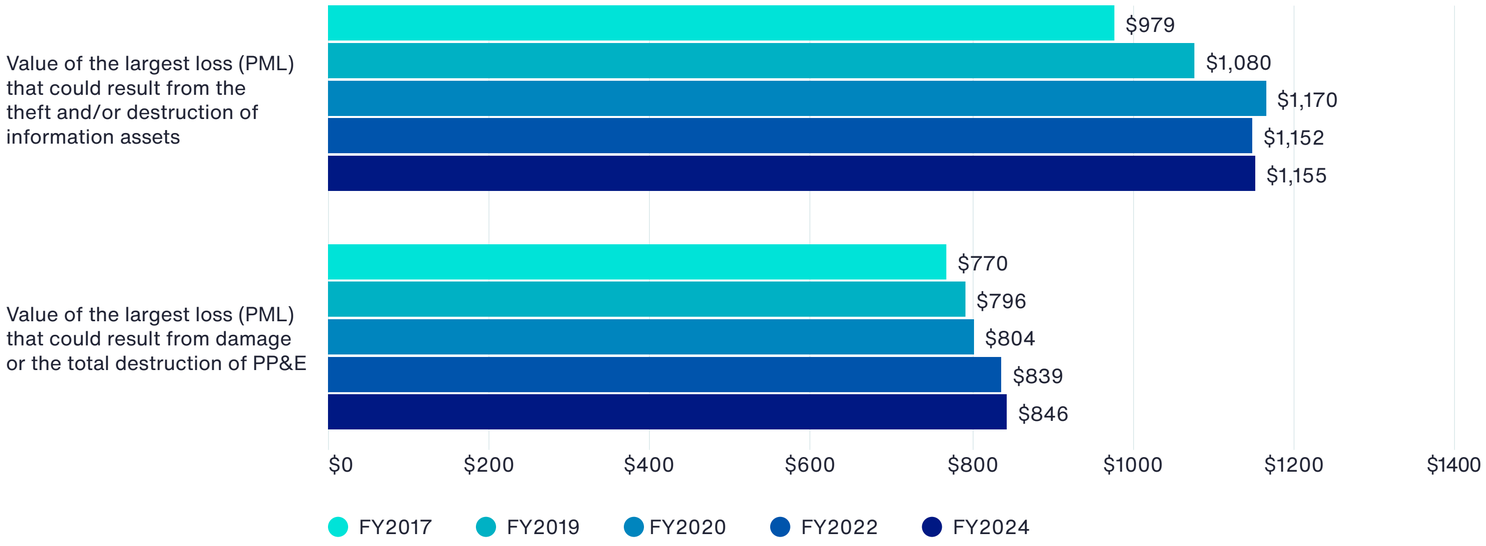
[66] Source: Institute of Risk Management

The value of PML is higher for information assets than for PP&E. Organizations estimate the average PML resulting from the theft or destruction of information assets at approximately $1,155 million, according to Figure 2. 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, on average, approximately $846 million. 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 2. The PML value for PP&E and information assets

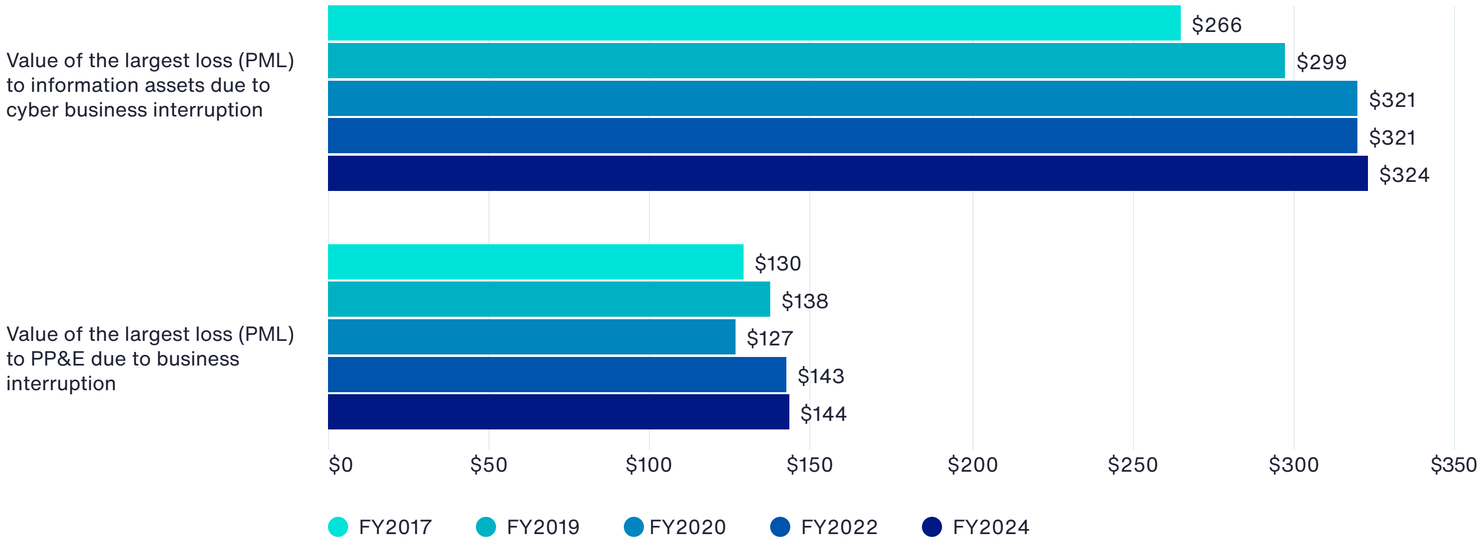
Extrapolated value ($ millions)



The impact of business disruption to information asset losses is more significant than the impact to PP&E. According to Figure 3, business disruption has a greater impact on information assets ($324 million)[67] than on PP&E ($144 million).

Figure 3. The impact of business disruption to information assets and PP&E

Extrapolated value ($ millions)

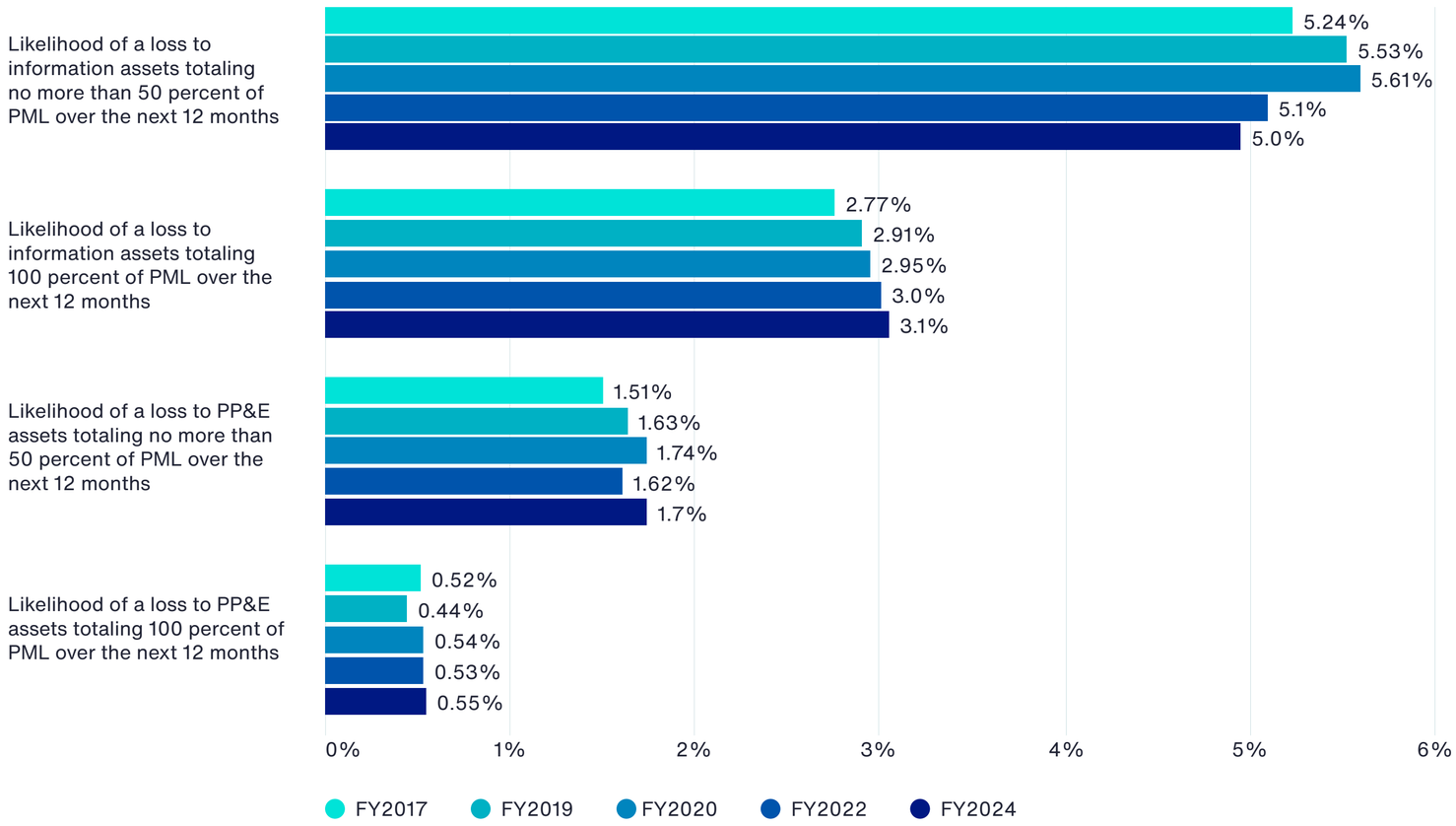


[67] While the survey results suggest Probably Maximum Loss in the neighborhood of $324 million, a growing number of organizations are using Risk Decision Platform Analysis and Cyber Modeling to suggest potential losses in excess of $500 million to over $1 billion and seek cyber insurance limit premium quotes and policy terms for such amounts.

The likelihood of a loss is higher for information assets than for PP&E. Organizations estimate the likelihood that they will sustain a loss relating to information assets totaling no more than 50 percent of PML over the next 12 months at 5 percent and 100 percent of PML at 3 percent, as shown in Figure 4. The likelihood of a loss relating to PP&E totaling no more than 50 percent of PML over the next 12 months is an average of 2 percent and at 100 percent of PML it is 0.55 percent.

Figure 4. Likelihood of loss to PP&E and information assets totaling more than 50 percent and 100 percent of PML over the next 12 months

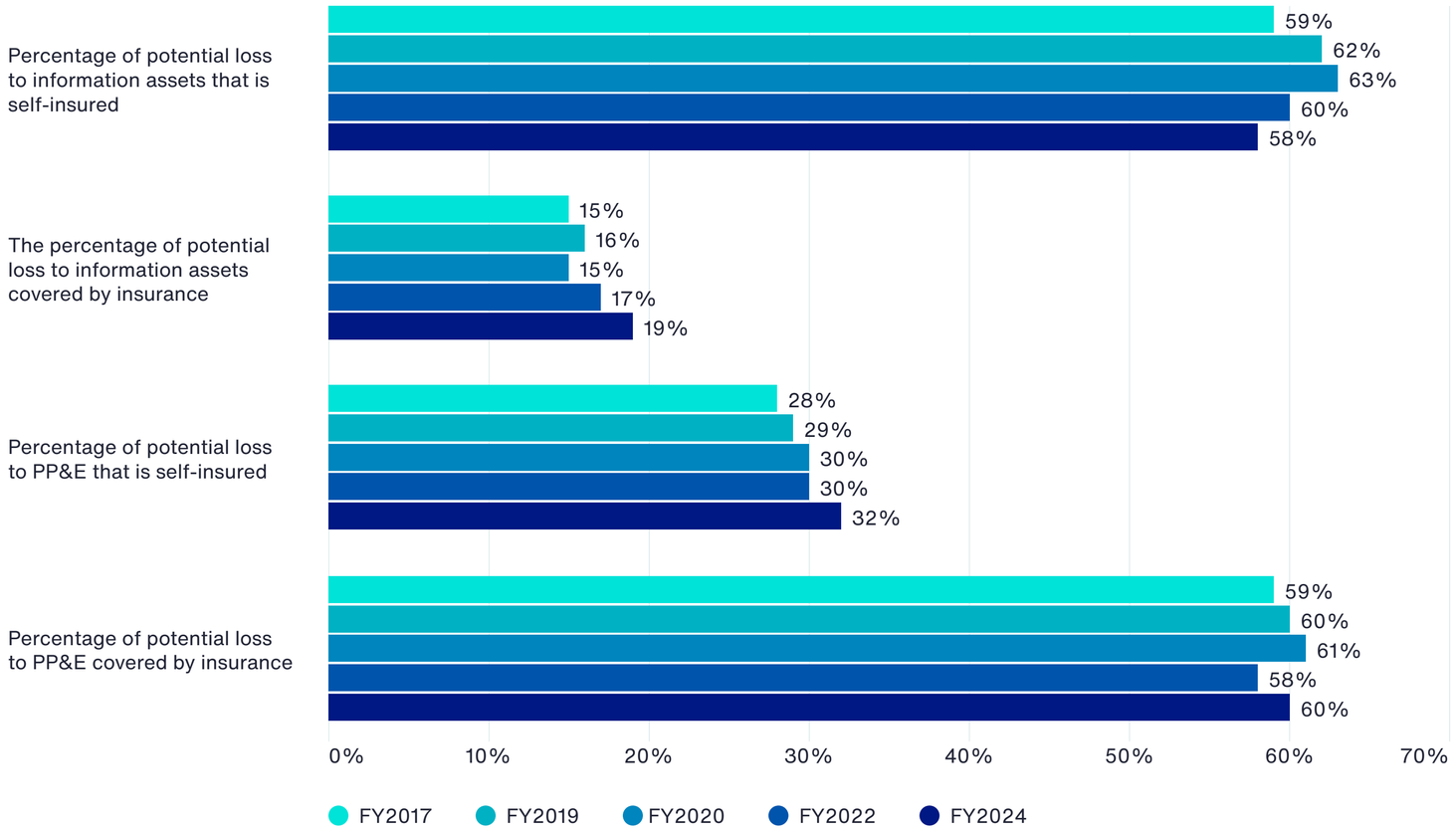
Extrapolated percentage



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 32 percent of PP&E assets are self-insured (Figure 5). Only an average of 19 percent of information assets are covered by insurance. Self-insurance is higher for information assets at 58 percent.

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

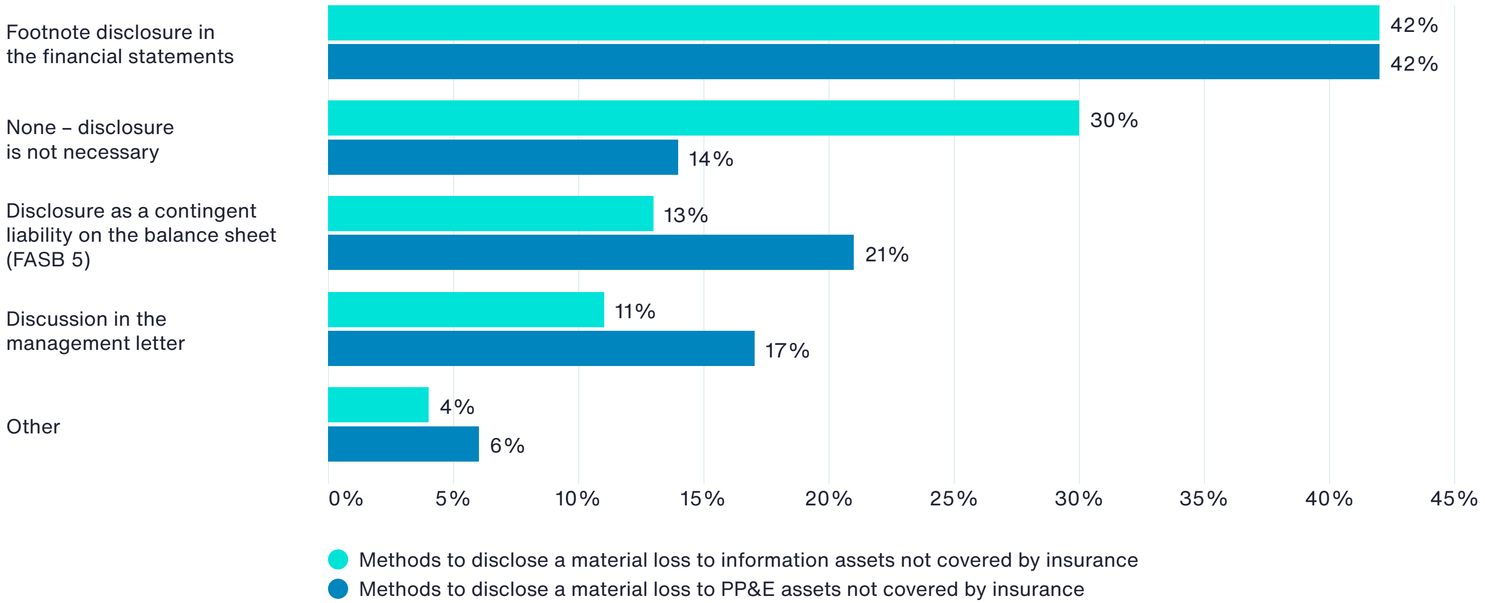
Extrapolated percentage



Thirty percent of respondents believe no disclosure of a material loss to information assets not covered by insurance is required. In contrast, only 14 percent of respondents say no disclosure is necessary for a material loss to PP&E assets not covered by insurance is required. Figure 6 focuses on how organizations would disclose a material loss. Forty-two percent of respondents say their company would disclose a material loss to PP&E and information assets not covered by insurance in the footnotes of its financial statements.

Twenty-one percent of respondents say their organizations would disclose a material loss to PP&E as a contingent liability on the balance sheet (FASB 5). Thirteen percent of respondents say an information loss would be reported as a contingent liability.

Figure 6. How would your company disclose a material loss to PP&E and information assets not covered by insurance?

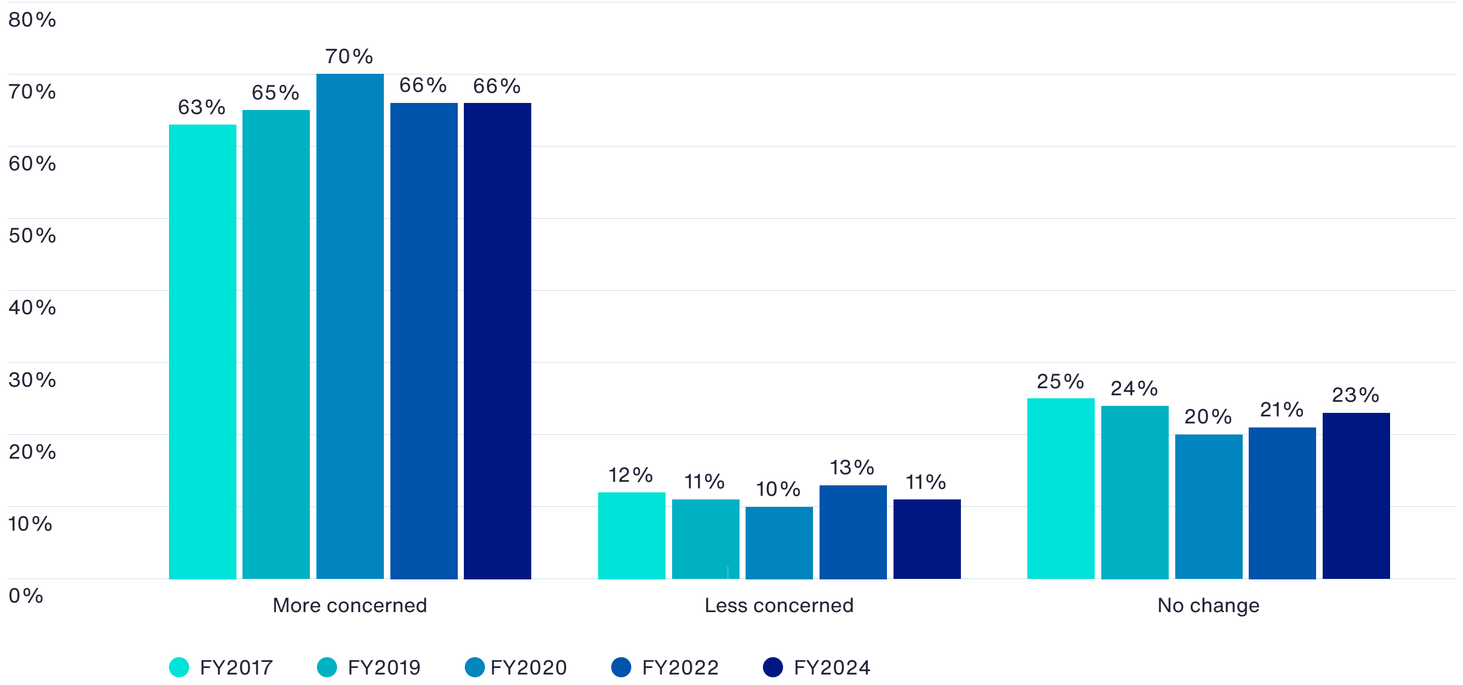


2 Cyber Risk Exposures Increase

Fifty-six percent of respondents say their organizations had a material or significantly disruptive security exploit or data breach one or more times in the past 24 months. The average total financial impact of these incidents was $5 million. According to Figure 7, 66 percent of these respondents say the incident increased their company's concerns over cyber liability.

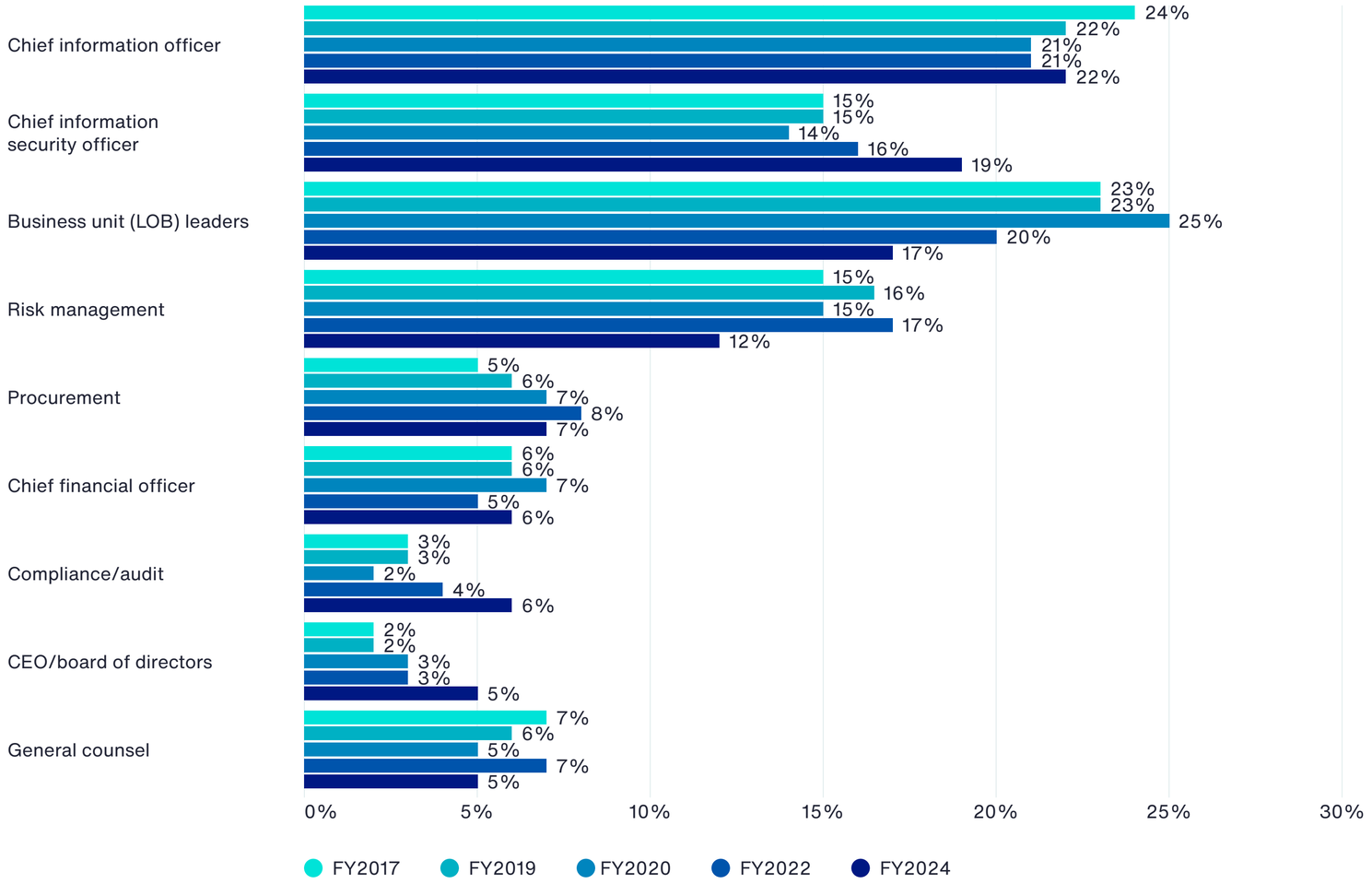
> "Artificial intelligence is growing in importance as both a threat, and a mitigation mechanism, with respect to cyber IT Security resilience – but nothing will ever completely replace the importance of human collaboration.
>
> **Joe Martinez**
> Chief Security Officer
> Aon

Figure 7. How did the security exploit or data breach affect your company's concerns over cyber liability?



Forty-one percent of respondents say responsibility for cyber risk management mostly resides in the IT (22 percent) and IT security functions (19 percent). As shown in Figure 8, the risk management and lines of business functions have declined in responsibility for cyber risk management (12 percent and 17 percent of respondents, respectively).

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

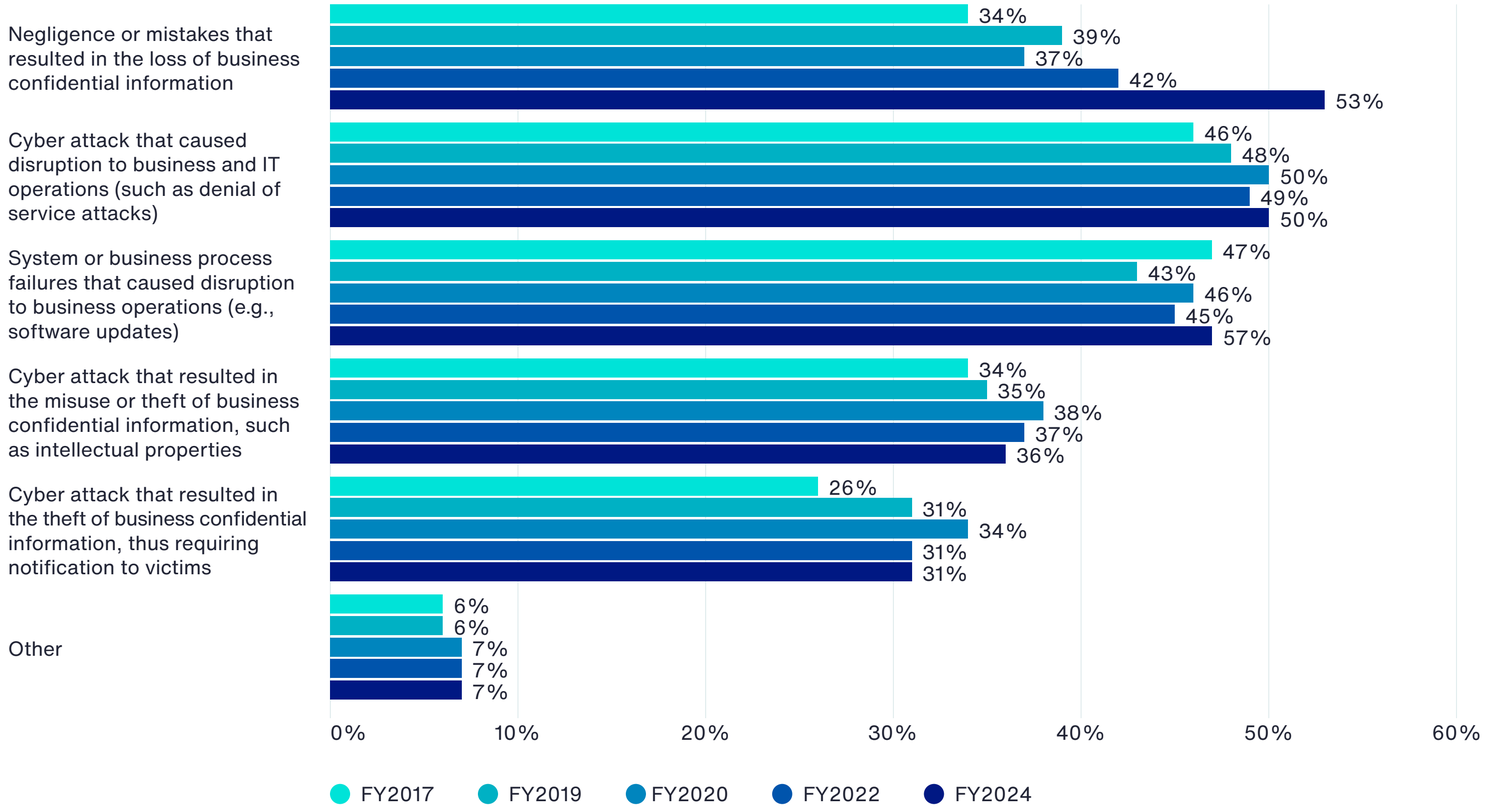


Data breaches and security exploits caused by negligence or mistakes increases significantly. Figure 9 lists the security incidents that 56 percent of the organizations in this research had. The most frequent type of incident was one that was caused by negligence or mistakes that resulted in the loss of business confidential information (53 percent of respondents).

Fifty percent of respondents say it was a cyber attack that caused a disruption to business and IT operations. Forty-seven percent of respondents say a system or business process failure caused disruption to business operations.

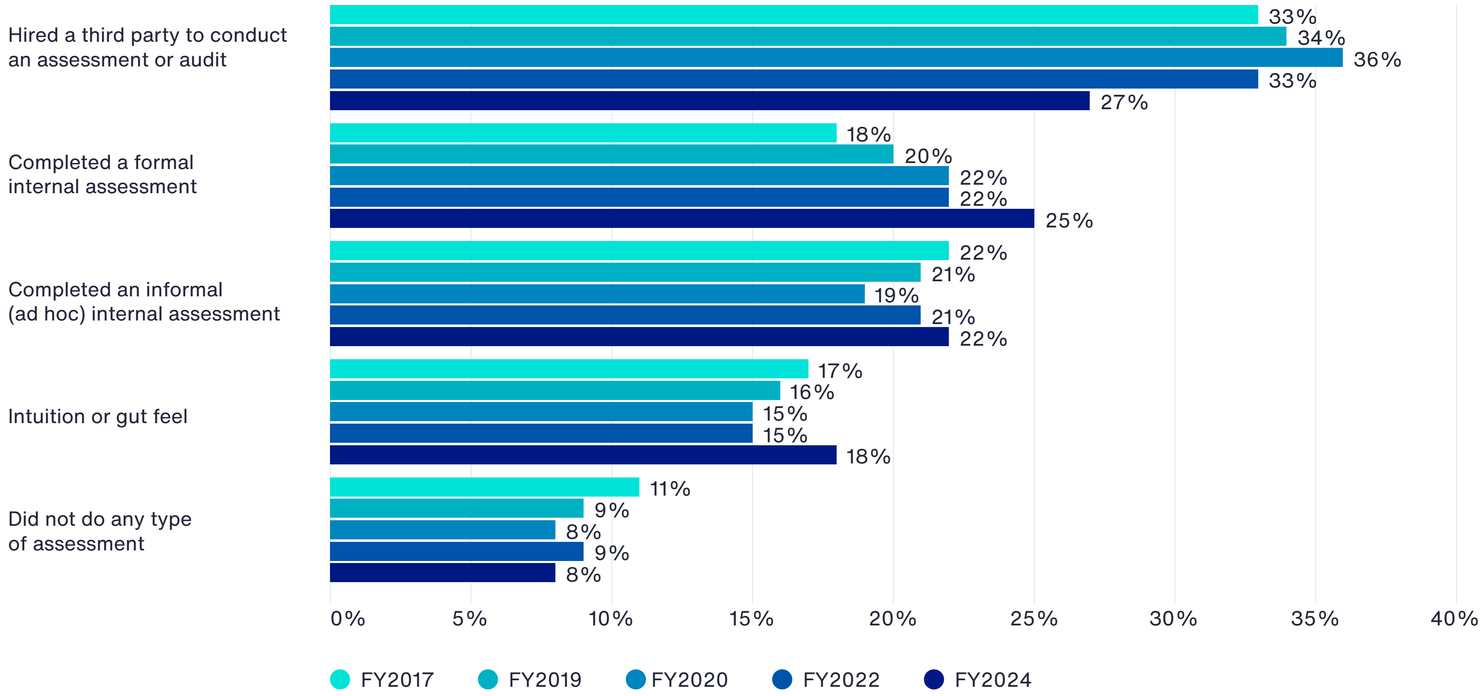
Figure 9. What type of data breach or security exploit did your company experience?

More than one response permitted



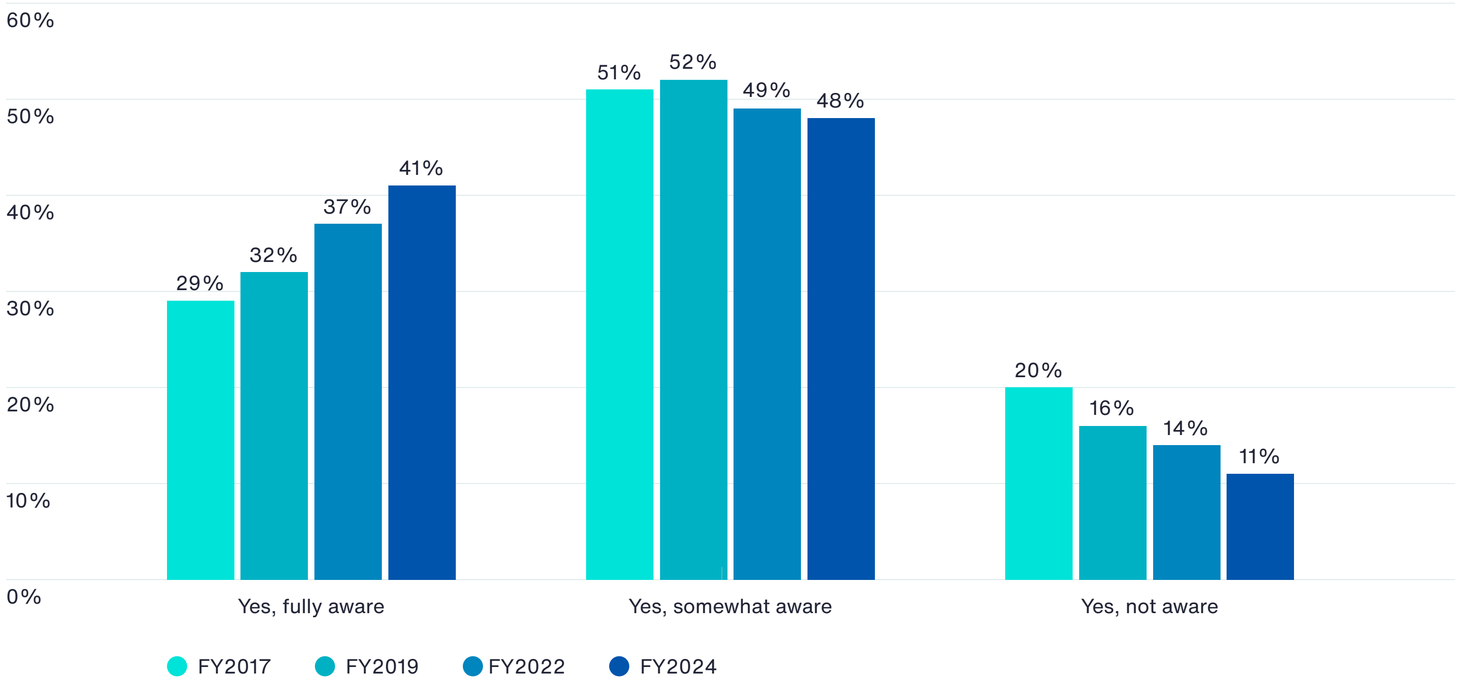
The use of third parties to assess cyber risk has declined. According to Figure 10, to determine the cyber risk to their company, 27 percent of respondents say the company hired a third party to conduct an assessment or audit. However, formal internal assessments is slowly increasing (25 percent of respondents). Twenty-two percent of respondents say their organizations did an informal (ad hoc) internal assessment. Only 18 percent of respondents say it was based on intuition or gut feel.

Figure 10. How did you determine the level of cyber risk to your company?



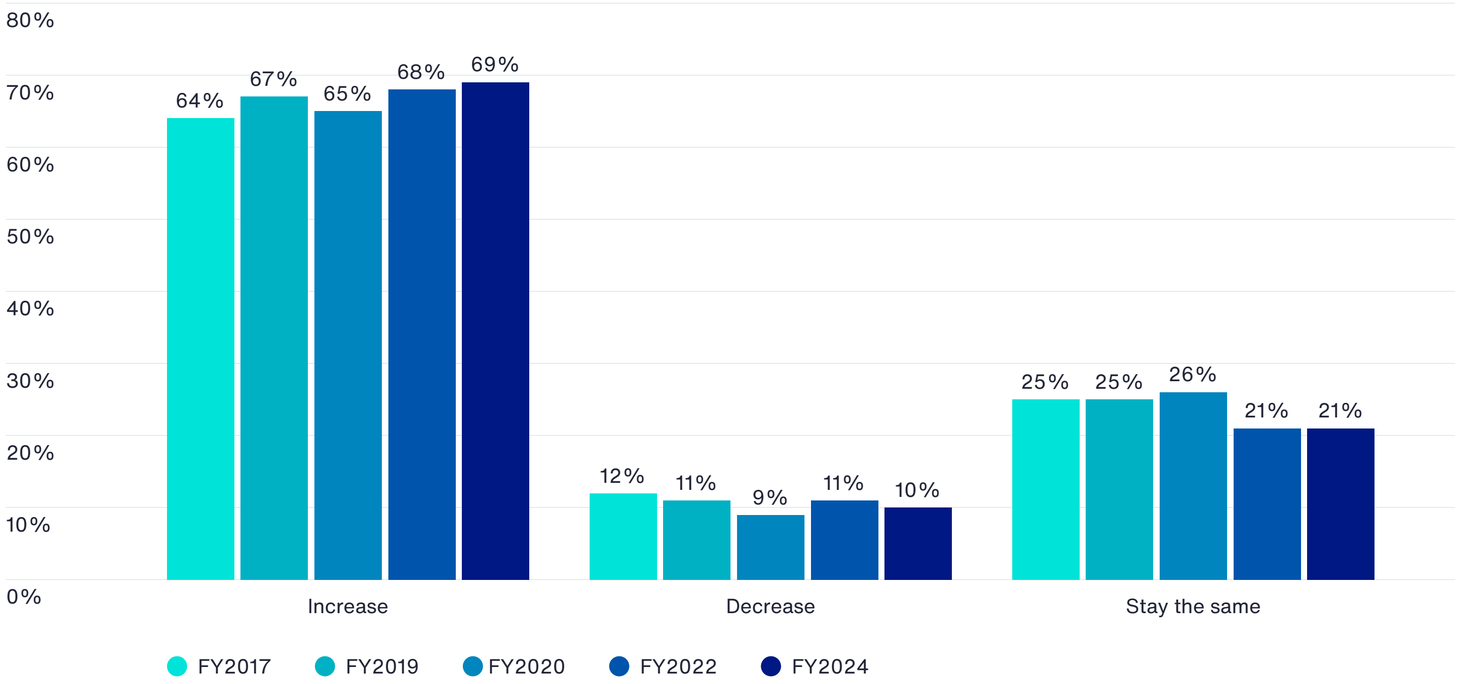
More organizations are becoming aware of the economic and legal consequences from an international data breach or security exploit. As revealed in Figure 11, 89 percent of respondents are either fully (41 percent) or somewhat aware (48 percent) of the consequences that could result from a data breach or security exploit in other countries in which their company operates. Only 11 percent of respondents say they are not aware of the consequences, a significant decline from 20 percent in 2017.

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



Organizations' exposure to cyber risk is increasing. While organizations are predicting that their cyber risk exposure will increase, 32 percent of respondents say there is no plan to purchase standalone cyber insurance. As the data in Figure 12 show, 69 percent of respondents believe their company's exposure to cyber risk will increase and 21 percent of respondents say it will stay the same. Only 10 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?

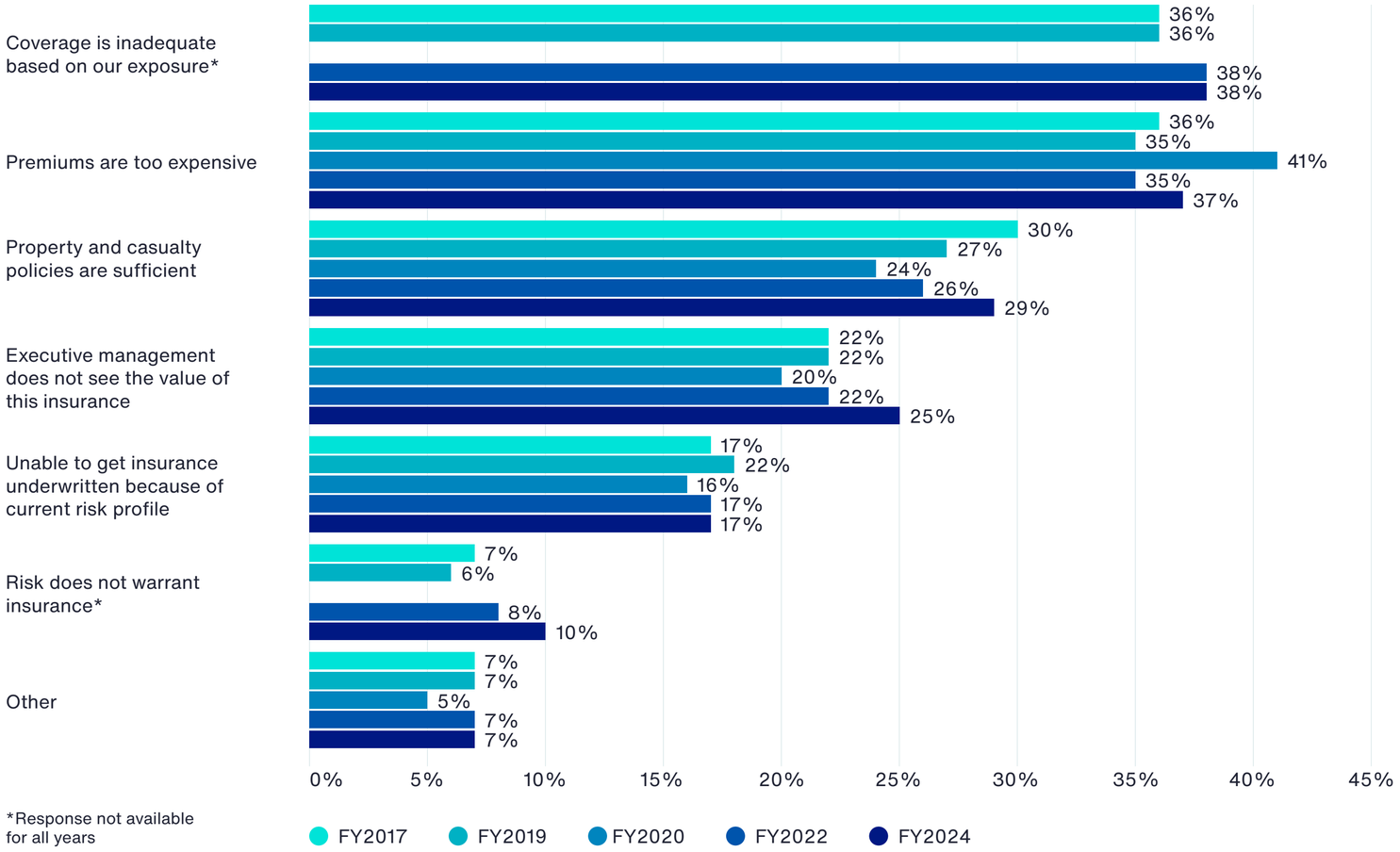


Most organizations are postponing the purchase of a standalone cyber insurance. Thirty-two percent of respondents say their organizations have no plans to purchase a standalone cyber insurance policy. Only 18 percent of respondents say their company will purchase standalone cyber insurance policy in the next 12 months. Half of respondents (50 percent) say they will purchase a standalone cyber insurance policy in the next 24 months (28 percent) or more than 24 months (22 percent).

According to Figure 13, the main reasons for **not** purchasing a standalone cyber security insurance policy are: coverage is inadequate based on their exposure (38 percent of respondents), premiums are too expensive (37 percent of respondents) and there are too many exclusions, restrictions and uninsurable risks (29 percent of respondents).

Figure 13. What are the main reasons why your company will not purchase standalone cyber security insurance?

More than one response permitted

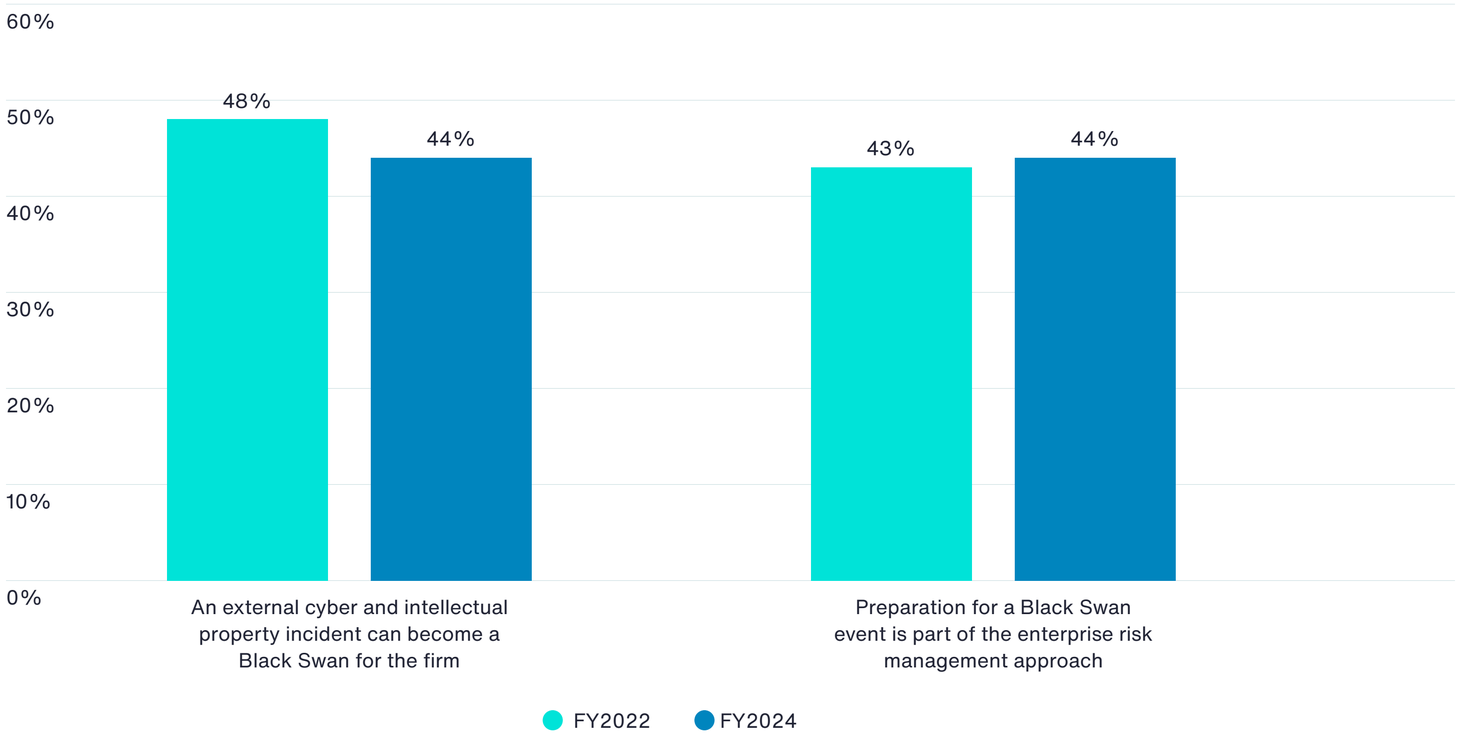


*Response not available for all years

Most organizations are not preparing for a Black Swan event as part of their enterprise risk management approach, although 44 percent of respondents say their organizations had an external cyber or IP incident that became such an event. A Black Swan is an event that is an "outlier" as it lies outside the realm of regular expectations.[68] As shown in Figure 14, while 44 percent of respondents say an external cyber and intellectual property incident has become a Black Swan event for their organizations, only 44 percent of respondents say preparation for such an event is part of their enterprise risk management approach.[69]

Figure 14. Are organizations prepared for a Black Swan event?

Yes responses only



[68] A black swan is an unpredictable event that is beyond what is normally expected of a situation and has potentially severe consequences, such as the COVID-19 pandemic. Black swan events are characterized by their extreme rarity, their severe impact, and the widespread insistence they were obvious in hindsight.

[69] Due to their severe impact, "black swans" should be considered by the board of directors. Is cyber risk a D&O risk? (ethicalboardroom.com). While data on gray swan events are lacking, preparation is still possible to anticipate and combat these relatively rare but significantly risky events. Black and Grey Swans: 5 Ways to Avoid Shocks - Aon

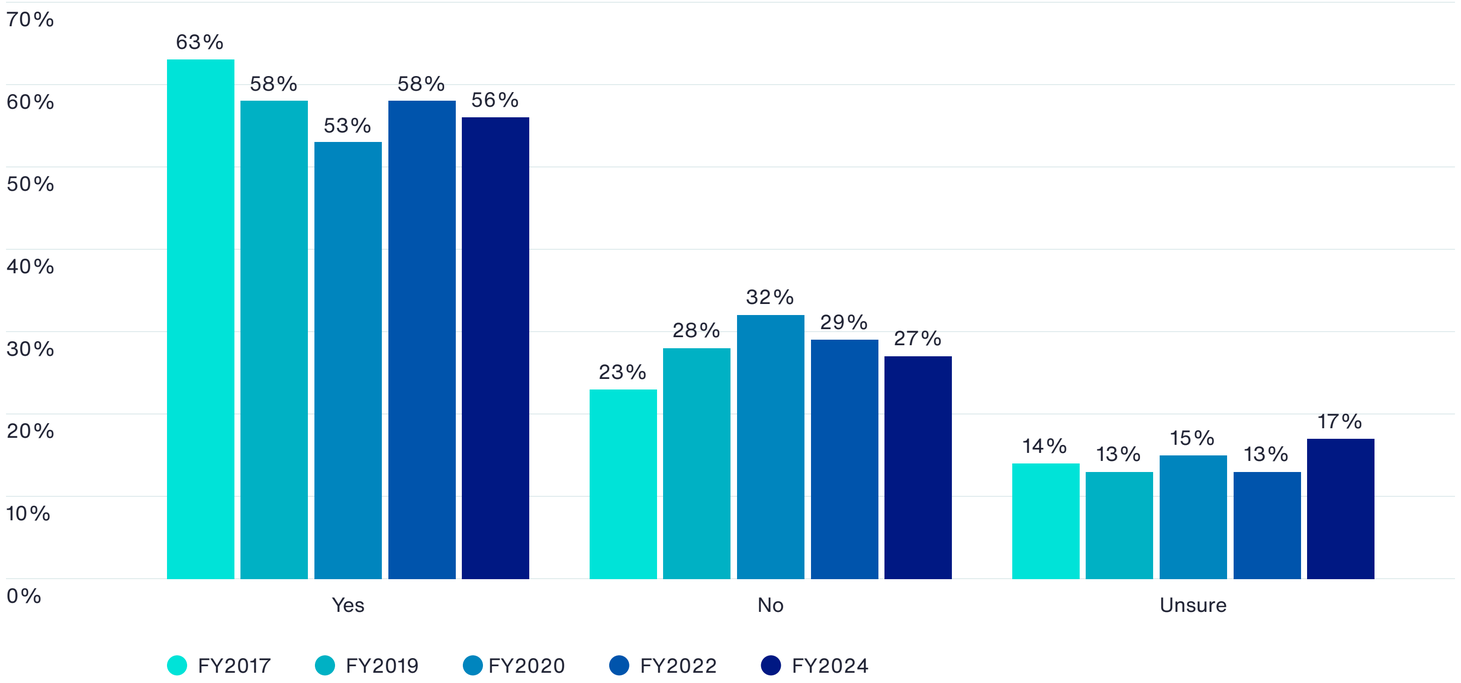
The Use of Cyber Insurance to Mitigate the Financial Consequences of Data Breaches and Security Exploits

Only 30 percent of respondents say their organizations have cyber insurance included within a Technology Errors or Omission or similar policy, not including Property, General Liability or Crime policy and responded to the questions in this section.

Since 2017, fewer organizations believe their cyber insurance coverage is sufficient. Despite the extent of cyber risk, which exceeds that of PP&E risk, only 30 percent of respondents say their organizations currently have cyber insurance coverage with an average limit of $17 million.

As Figure 15 reveals, 56 percent of these respondents believe their insurance is sufficient with respect to coverage terms and conditions, exclusions, retentions, limits and insurance carrier financial security, a significant decline from 63 percent in 2017.[70]

Figure 15. Is your company's cyber insurance coverage sufficient?



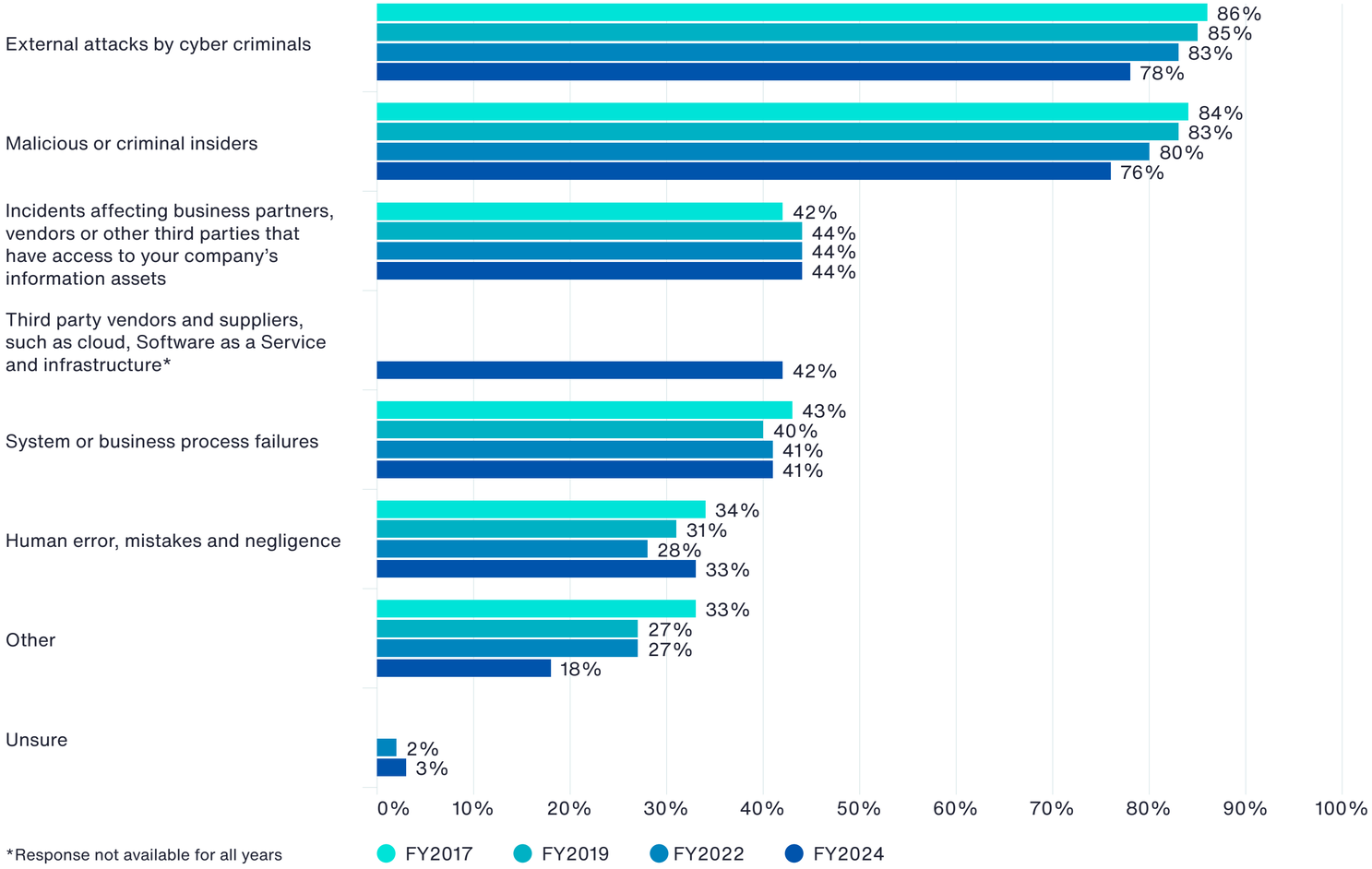
[70] The Future of Insurance to Address Cyber Perils. Insurance Thought Leadership.

More than half of respondents (53 percent) say it was error and negligence that was the root cause of their data breach or security exploit, yet only 33 percent of respondents say their insurance covers these types of incidents. Figure 16 lists the types of incidents organizations' insurance covers. As shown, 78 percent of respondents say it covers external attacks by cyber criminals and 76 percent of respondents covers was malicious or criminal insiders.

> "Risk capital providers must bring the breadth of their expertise, relationships and analytics to unlock traditional and alternative capital, which is accessed regardless of market, geography or financial instrument to create greater value and help organizations grow.
>
> **Anne Corona**
> CEO, Aon Asia

Figure 16. What types of incidents does your organization's cyber insurance cover?

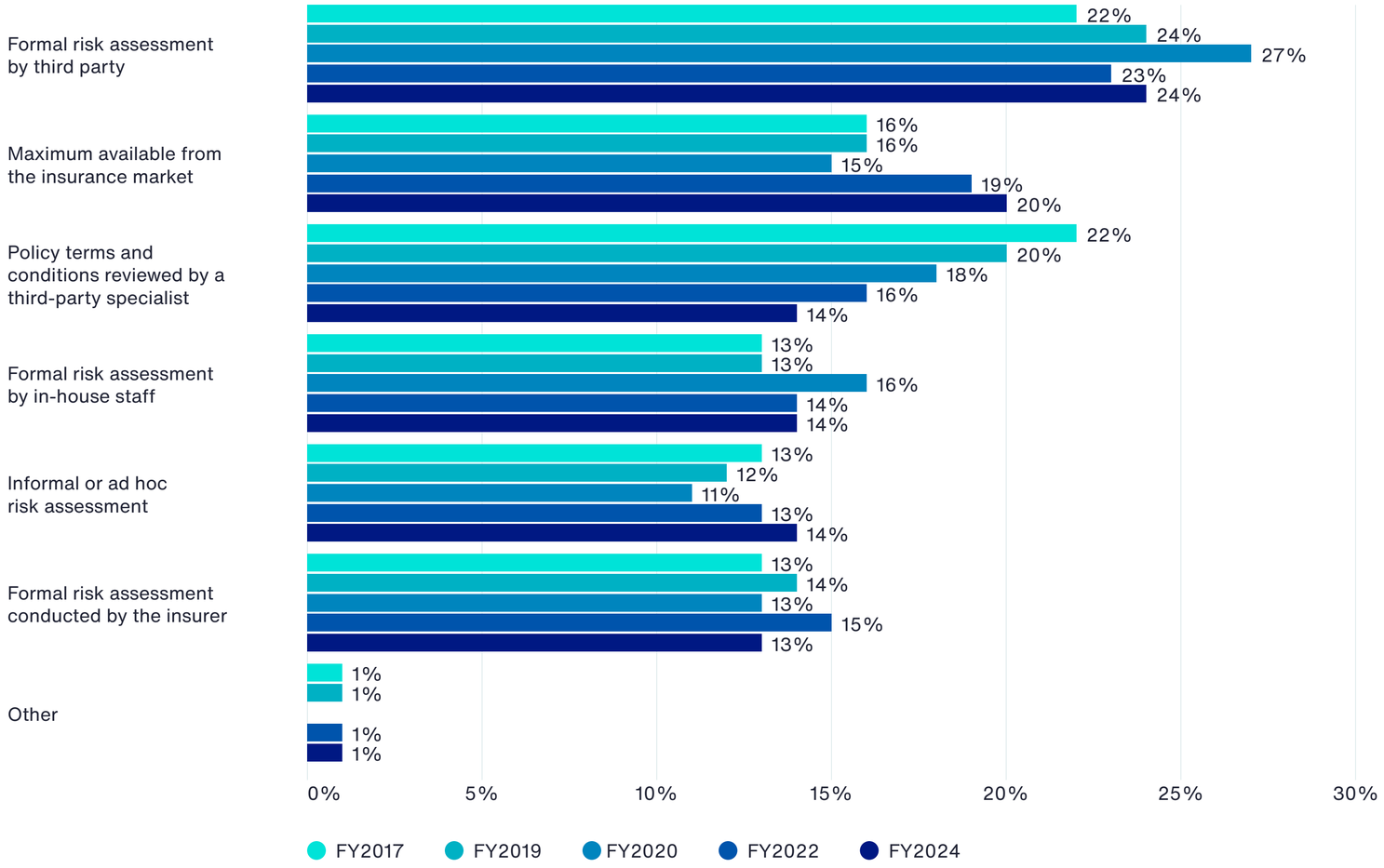
More than one response permitted



*Response not available for all years

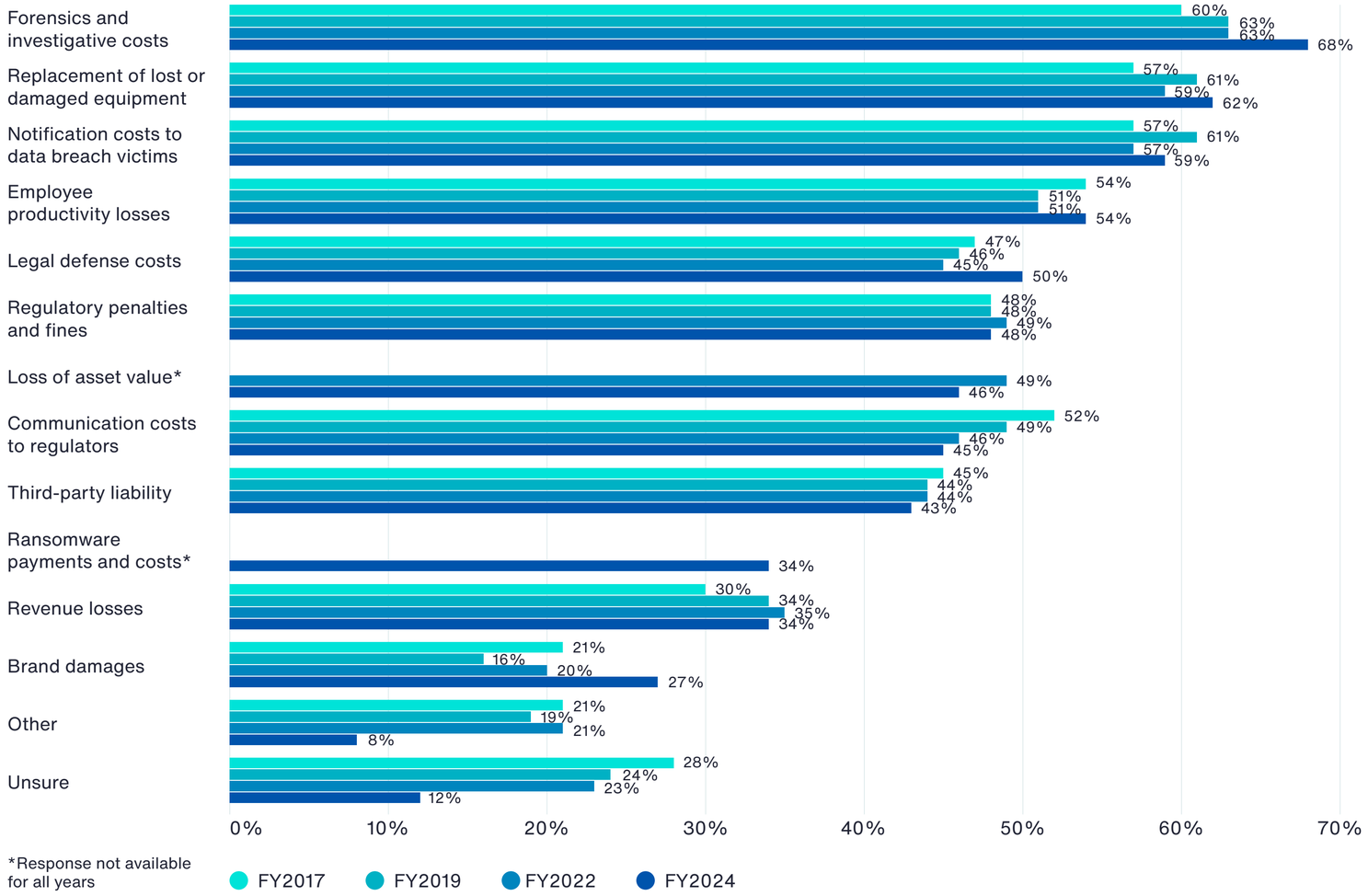
According to Figure 17, the adequacy of coverage is determined mainly by a formal risk assessment by a third party (24 percent of respondents), maximum value from the insurance market (20 percent of respondents) and policy terms and conditions reviewed by a third-party specialist (14 percent of respondents).

Figure 17. How organizations determine the adequacy of coverage



Few cyber insurance providers are covering ransomware payments and costs to recover from the attack. Figure 18 lists the various reimbursements and services insurance organizations offer. The top three are forensics and investigative costs, replacement of lost or damaged equipment and notification costs to data breach victims, 68 percent, 62 percent and 59 percent of respondents respectively). Thirty-four percent of respondents say their insurance reimburse costs related to ransomware.

Figure 18. What coverage does this insurance offer your company?



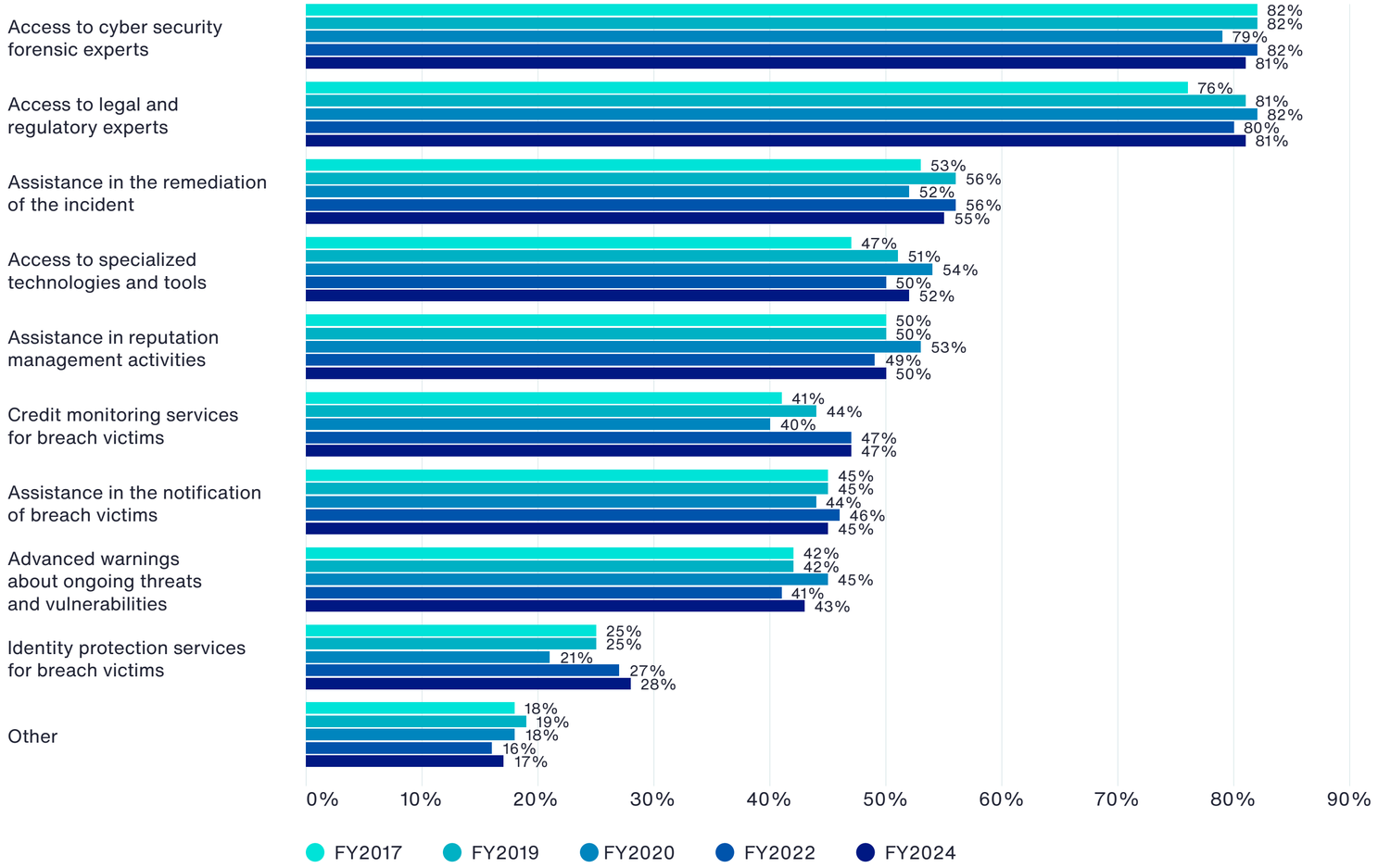
*Response not available for all years

Access to forensic, legal and regulatory experts are other services provided. According to Figure 19, the primary services provided by the insurer are access to cyber security forensic experts and legal and regulatory experts (both 81 percent of respondents, respectively). This is followed by assistance in the remediation of the incident (55 percent of respondents) and access to specialized technologies and tools (52 percent of respondents).

> "International access to London and Bermuda market capital enables positive insurance premium arbitrage and helps to optimize terms and conditions throughout the tower. Furthermore, Aon's tailored MGA facilities based in London can provide discreet and accretive capital to that available in the open market.
>
> **Beverley Alderson**
> Global Broking Center
> Aon

Figure 19. Other services provided by the cyber insurer

More than one response permitted

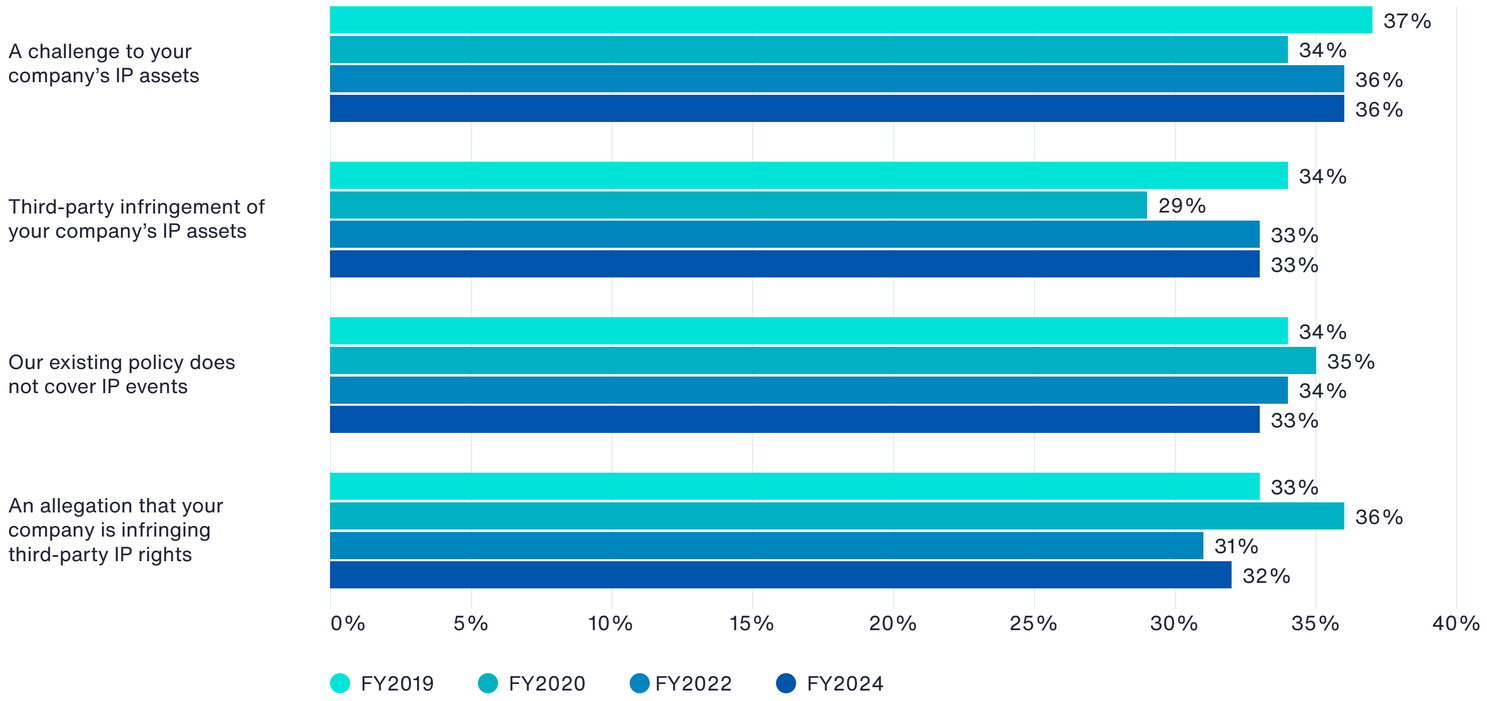


2 The Vulnerability of IP Assets

The IP events that existing insurance policies cover. According to Figure 20, of the 67 percent of respondents with cyber insurance that have policies covering IP events, 36 percent of respondents say their organizations' existing insurance policy covers a challenge to their IP assets, 33 percent say it covers third-party infringement of their IP assets and 31 percent of respondents say it covers an allegation that their company is infringing third-party IP rights.[71]

Figure 20. Does your company's existing insurance policy cover any of the following IP events?

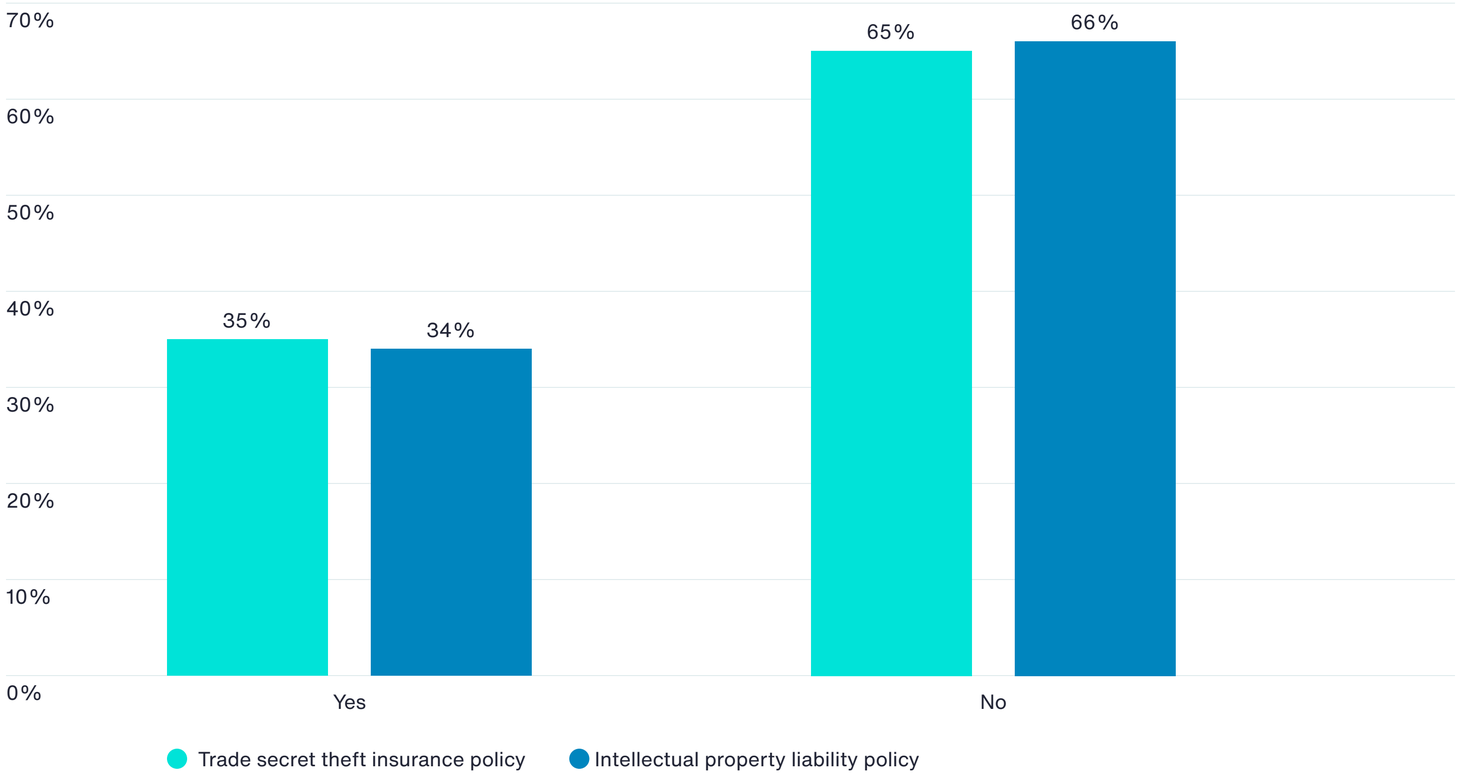
More than one response permitted



[71] Evolution of Insurance Coverage for Intellectual Property Litigation Policyholders and coverage practitioners should be aware of changes in available coverage.

Despite the potential risk, few organizations have a trade secret theft insurance policy and/or an intellectual property liability policy. As shown in Figure 21, only 35 percent of respondents say they have a trade secret theft insurance policy and a similar percentage of respondents (34 percent) have an intellectual property liability policy.[72]

Figure 21. Does your company have a trade secret and/or IP liability policy?

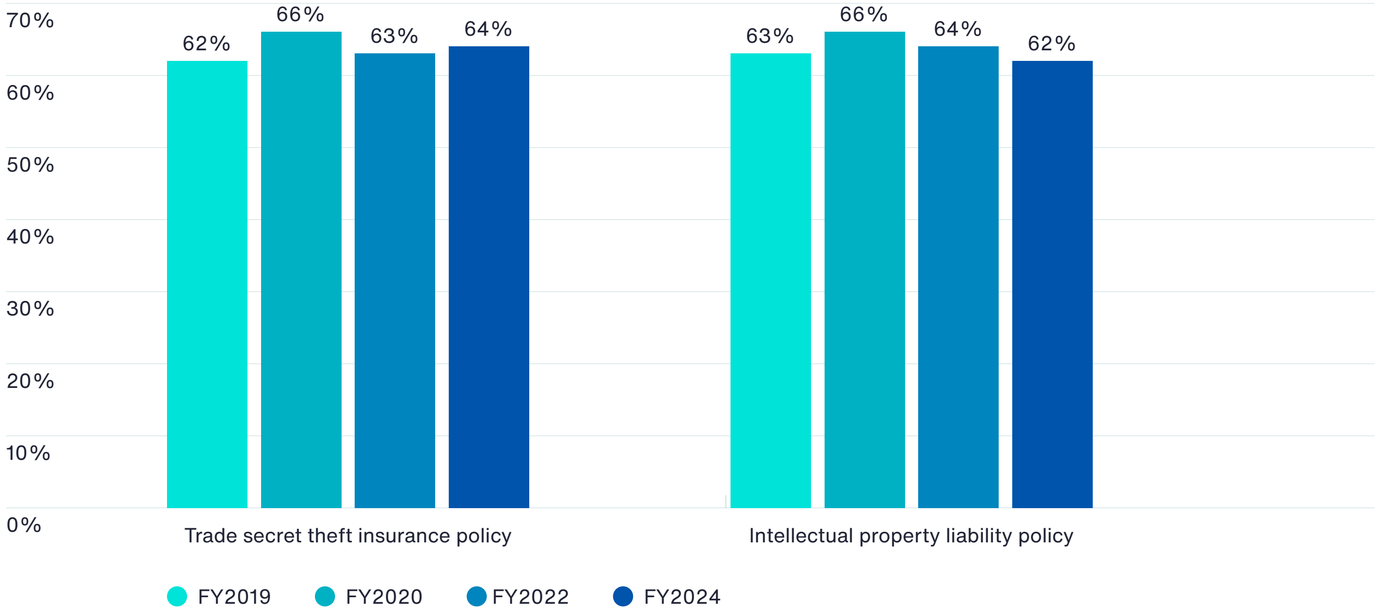


[72] A detailed review of insurance policies indicates that IP coverage is included in existing policies at a much lower rate than survey responses reflect – especially for patent infringement and trade secrets theft, which detailed reviews show less than 5% of organizations have insurance coverage for trade secrets or patents.

While most organizations do not have specific IP insurance policies, there is significant interest in purchasing them. According to Figure 22, 64 percent of respondents are very interested or interested in purchasing a trade secret insurance policy and 62 percent say their organizations would purchase an intellectual property liability policy.

Figure 22. If no, what is your company's level of interest in purchasing a trade secret theft insurance policy and/or an IP liability policy?

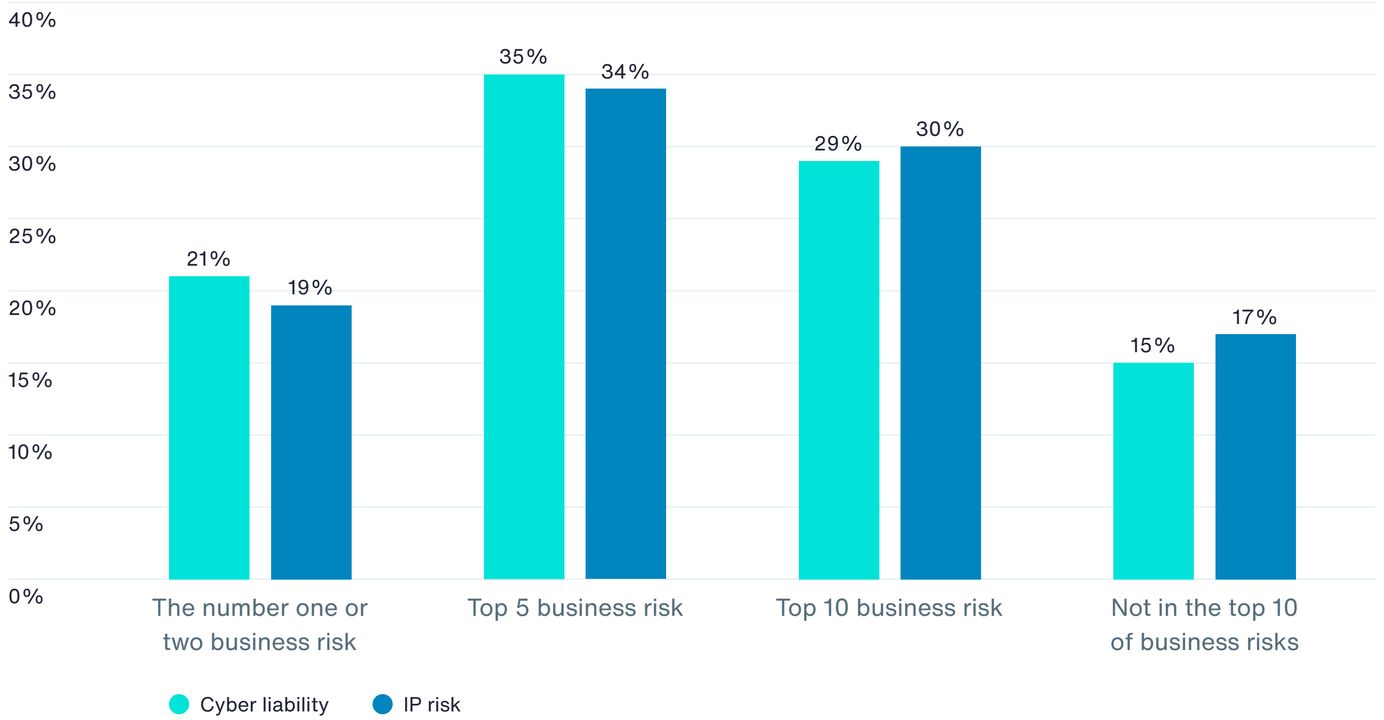
Very interested and Interested responses combined



Cyber liability and IP risks rank in the top 10 of all business risks facing organizations. According to Figure 23, 56 percent of respondents consider cyber risk as the number one or two business risk (21 percent of respondents) and among the top five (35 percent of respondents). Similarly, 53 percent of respondents rate the risk to their company's intellectual property (IP) among the top 5 off all business risks (19 percent + 34 percent).

Even though calculating the frequency and severity of intangible asset risks compared to intangible asset value relative to other organization assets is not a perfectly scientific mathematical exercise, we cannot afford to ignore the risks that are hardest to measure – especially when they may pose the greatest threats to our organizations. "The most calamitous failures of prediction usually have a lot in common. We focus on those signals that tell a story about the world as we would like it to be, not how it really is. We ignore the risks that are hardest to measure, even when they pose the greatest threats to our well-being. We make approximations and assumptions about the world that are much cruder than we realize. We abhor uncertainty, even when it is an irreducible part of the problem we are trying to solve."[73]

Figure 23. How do cyber and IP risks compare to other business risks?

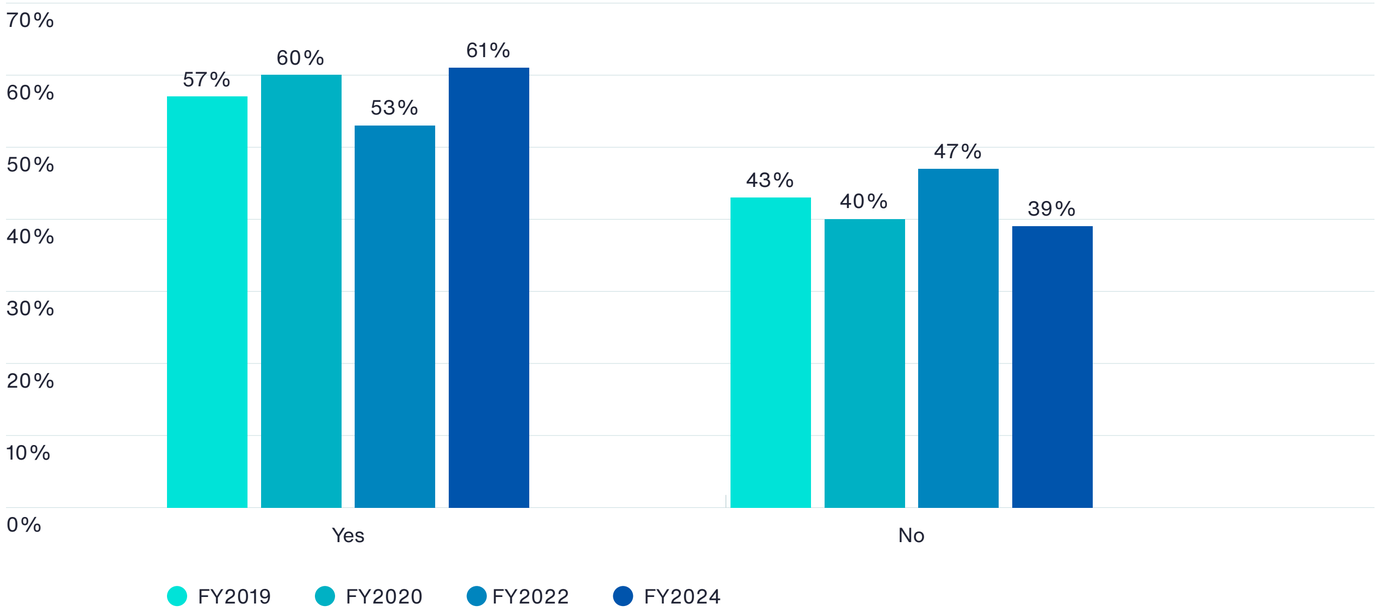


[73] Nate Silver, The Signal and the Noise: Why So Many Predictions Fail-but Some Don't.

The percentage of respondents who say their organizations have a strategy to manage risks to IP increased. Organizations 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 $600 million. An average of 47 percent of organizations' total assets are IP assets.

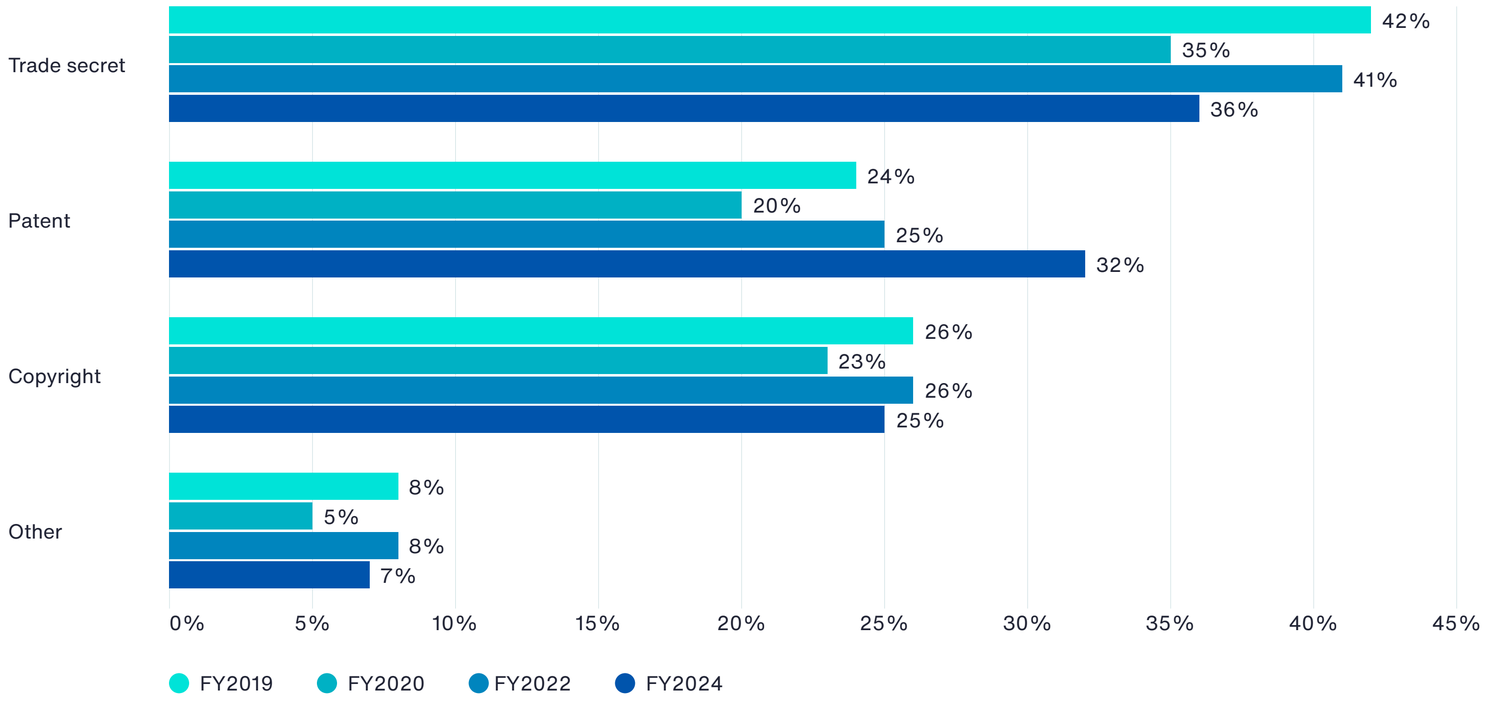
As shown in Figure 24, 61 percent of respondents say their enterprise risk management activities include risks to their IP, a significant increase from 2022.

Figure 24. Do your company's enterprise risk management activities include risks to IP?



In the past two years, 50 percent of respondents say their company experienced a material IP event. According to Figure 25, most of these incidents involved trade secrets (36 percent of respondents). However, more material IP security exploits involved patents, an increase from 25 percent of respondents to 32 percent).

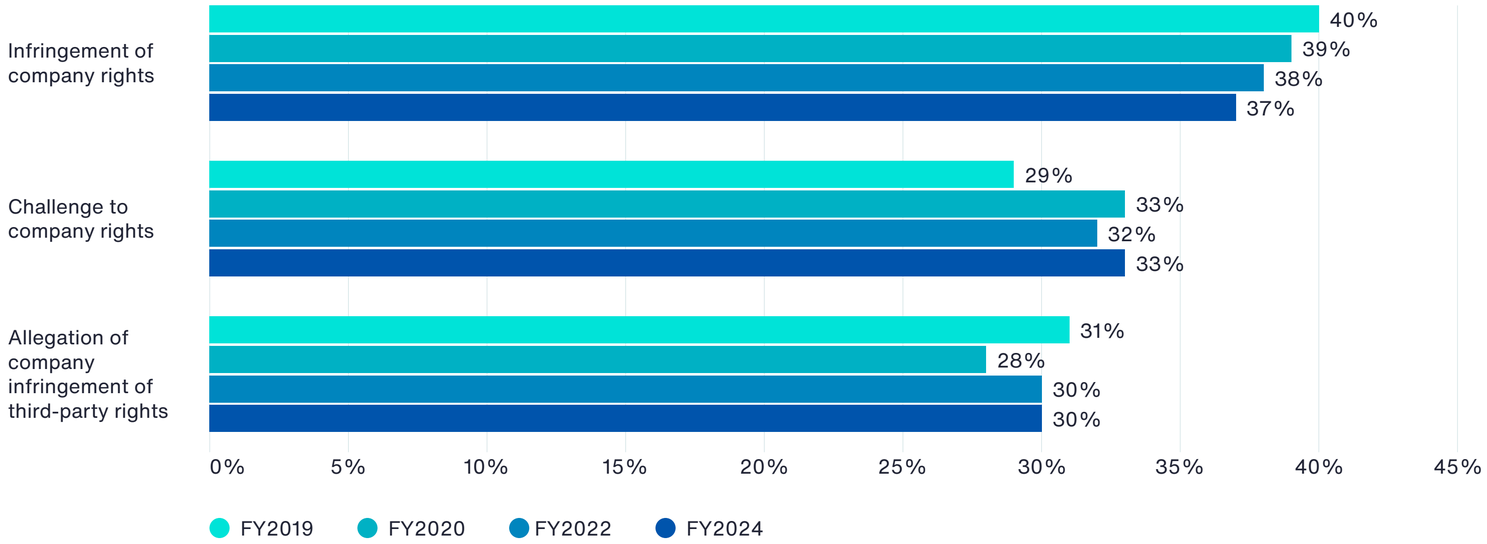
Figure 25. What type of IP assets were involved in a material IP event?



According to Figure 26, an IP material event can be described as an infringement of company rights (37 percent of respondents), challenge to company rights (33 percent of respondents) or an allegation of company infringement of third-party rights (30 percent of respondents).

Figure 26. What best describes the IP material event?

Only 1 response permitted



3

Appendix 1. Methods & Caveats

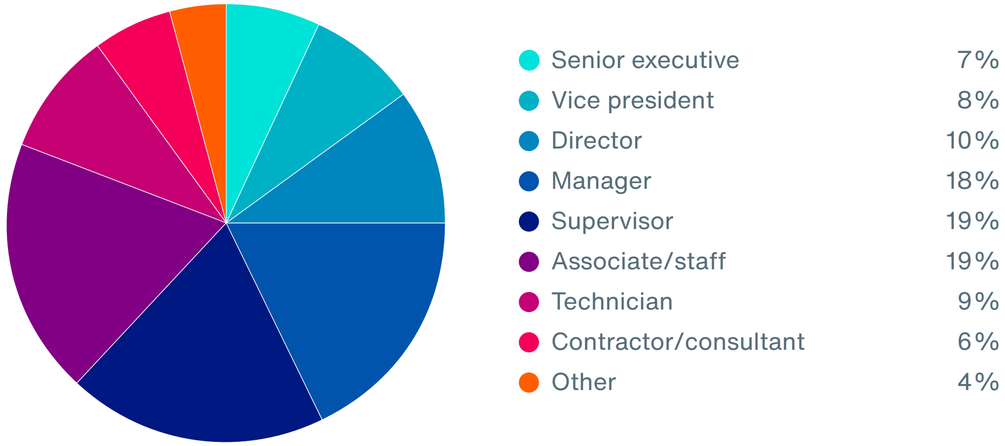
3 Methods

The consolidated sampling frame is composed of 61,073 individuals located in North America, EMEA, Asia-Pac and LATAM. Respondents are involved in their company's cyber risk management as well as enterprise risk management activities. As Table 1 shows, 2,671 respondents completed the survey, of which 290 were rejected for reliability issues. The final sample consisted of 2,381 surveys, a 3.9 percent response rate.

Table 1. Sample response	Freq	Pct%
Total sampling frame	63,112	100.0%
Total returns	2,790	4.4%
Rejected or screened surveys	327	0.5%
Final sample	2,463	3.9%

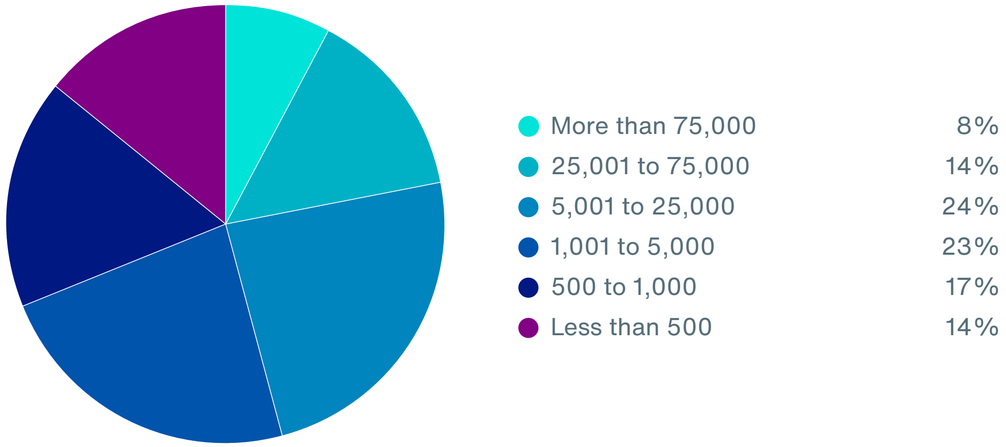
Pie Chart 1 reports the current position or organizational level of the respondents. More than half (62 percent) of the respondents reported their current position as supervisory level or above.

Pie Chart 1. Current position or organizational level



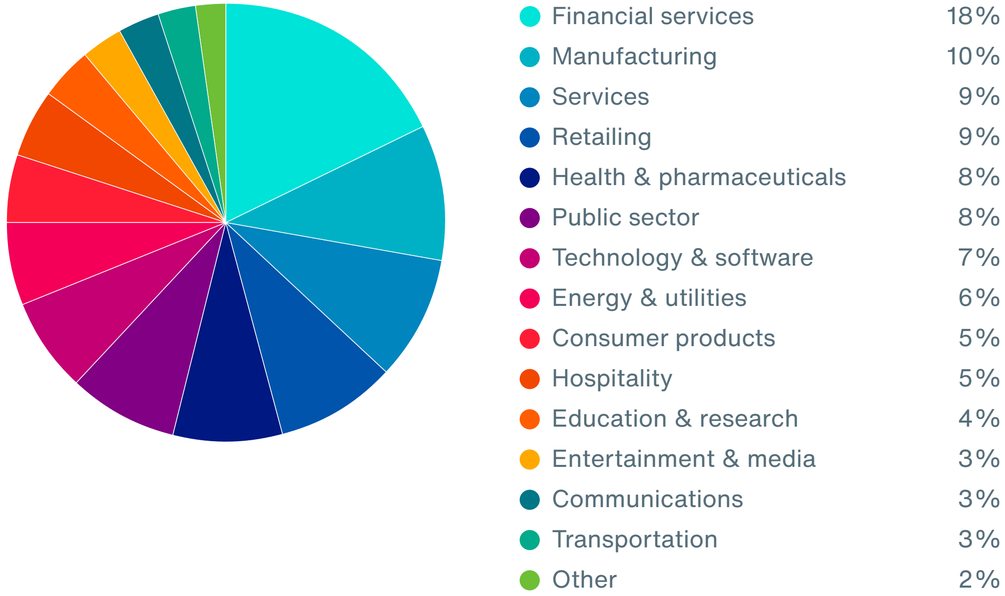
As Pie Chart 2 reveals, 69 percent of the respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 2. Worldwide headcount of the organization



Pie Chart 3 reports the primary industry classification of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by manufacturing (10 percent of respondents), services (9 percent of respondents), retailing (9 percent of respondents), health and pharmaceuticals, and public sector (each at 8 percent of respondents).[74]

Pie Chart 3. Primary industry focus



[74] **Cyber Insurance For Law Firms and Legal Organizations.** Chapter 15 of The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals, Second Edition.

3 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.

4

Appendix 2.
Detailed Survey Results

4 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 November and December 2023.

Survey response	FY2024
Sampling frame*	63,112
Total returns	2,790
Rejected surveys	327
Final sample	2,463
Response rate	3.9%

*The sampling frame is a consolidation of four regions: EMEA, APAC, LATAM and North America.

Screening questions

S1. How familiar are you with cyber risks facing your company today?	FY2024
Very familiar	28%
Familiar	37%
Somewhat familiar	35%
Not familiar (stop)	0%
Total	100%

S2. Are you involved in your company's cyber risk management activities?	FY2024
Yes, significant involvement	36%
Yes, some involvement	64%
No involvement (stop)	0%
Total	100%

S3. What best defines your role?	FY2024
Risk management	28%
Finance, treasury & accounting	32%
Corporate compliance/audit	15%
Security/information security	12%
General management	7%
Legal (OGC)	6%
None of the above (stop)	0%
Total	100%

S4. Are you involved in your company's enterprise risk management activities?	FY2024
Yes, significant involvement	41%
Yes, some involvement	59%
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).	FY2024
Less than $1 million	5%
$1 to 10 million	11%
$11 to 50 million	15%
$51 to 100 million	22%
$101 to 500 million	20%
$501 to 1 billion	14%
$1 to 10 billion	9%
More than $10 billion	4%
Total	100%
Extrapolated value (US$ millions)	$1,087.52

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.	FY2024
Less than $1 million	5%
$1 to 10 million	12%
$11 to 50 million	17%
$51 to 100 million	22%
$101 to 500 million	22%
$501 to 1 billion	12%
$1 to 10 billion	8%
More than $10 billion	2%
Total	100%
Extrapolated value (US$ millions)	$846.02

[86] Source: Institute of Risk Management

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.	FY2024
Less than $1 million	13%
$1 to 10 million	23%
$11 to 50 million	27%
$51 to 100 million	19%
$101 to 500 million	12%
$501 to 1 billion	5%
$1 to 10 billion	1%
More than $10 billion	0%
Total	100%
Extrapolated value (US$ millions)	$144.03

Q3. What percentage of this potential loss to PP&E assets is covered by insurance, including captives reinsured but not including captives not reinsured?	FY2024
Less than 5%	1%
5% to 10%	2%
11%to 20%	5%
21% to 30%	6%
31% to 40%	9%
41% to 50%	10%
51% to 60%	12%
61% to 70%	18%
71% to 80%	14%
81% to 90%	13%
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?	FY2024
Less than 5%	11%
5% to 10%	13%
11% to 20%	14%
21% to 30%	12%
31% to 40%	14%
41% to 50%	14%
51% to 60%	9%
61% to 70%	6%
71% to 80%	4%
81% to 90%	2%
91% to 100%	1%
Total	100%
Extrapolated value	32%

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?	FY2024
Less than 0.1%	23%
0.1% to 0.5%	12%
0.6% to 1.0%	16%
1.1% to 2.0%	17%
2.1% to 3.0%	14%
3.1% to 4.0%	8%
4.1% to 5.0%	5%
5.5% to 10.0%	2%
More than 10.0%	3%
Total	100%
Extrapolated value	1.7%

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?	FY2024
Less than 0.1%	64%
0.1% to 0.5%	14%
0.6% to 1.0%	11%
1.1% to 2.0%	4%
2.1% to 3.0%	2%
3.1% to 4.0%	1%
4.1% to 5.0%	2%
5.1% to 10.0%	2%
More than 10.0%	0%
Total	100%
Extrapolated value	0.55%

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?	FY2024
Disclosure as a contingent liability on the balance sheet (e.g., FASB 5)	21%
Footnote disclosure in the financial statements	42%
Discussion in the management letter	17%
None – disclosure is not necessary	14%
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 either a precise quantification or estimate.	FY2024
Less than $1 million	5%
$1 to 10 million	7%
$11 to 50 million	14%
$51 to 100 million	21%
$101 to 500 million	21%
$501 to 1 billion	18%
$1 to 10 billion	9%
More than $10 billion	5%
Total	100%
Extrapolated value (US$ millions)	$1,239.30

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.	FY2024
Less than $1 million	7%
$1 to 10 million	10%
$11 to 50 million	17%
$51 to 100 million	22%
$101 to 500 million	21%
$501 to 1 billion	11%
$1 to 10 billion	7%
More than $10 billion	5%
Total	100%
Extrapolated value (US$ millions)	$1,154.89

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.	FY2024
Less than $1 million	16%
$1 to 10 million	22%
$11 to 50 million	22%
$51 to 100 million	17%
$101 to 500 million	12%
$501 to 1 billion	7%
$1 to 10 billion	4%
More than $10 billion	0%
Total	100%
Extrapolated value (US$ millions)	$323.90

Q10. What percentage of this potential loss to information assets is covered by insurance, including captives reinsured but not including captives not reinsured?	FY2024
Less than 5%	28%
5% to 10%	28%
11% to 20%	13%
21% to 30%	8%
31% to 40%	6%
41% to 50%	5%
51% to 60%	4%
61% to 70%	3%
71% to 80%	2%
81% to 90%	2%
91% to 100%	1%
Total	100%
Extrapolated value	19%

Q11. What percentage of this potential loss to information assets is self-insured, including captives not reinsured?	FY2024
Less than 5%	2%
5% to 10%	3%
11% to 20%	4%
21% to 30%	3%
31% to 40%	8%
41% to 50%	10%
51% to 60%	17%
61% to 70%	23%
71% to 80%	16%
81% to 90%	10%
91% to 100%	4%
Total	100%
Extrapolated value	58%

Q12. What is the likelihood your company will sustain a loss to information assets totaling no more than 50 percent of PML over the next 12 months?	FY2024
Less than 0.1%	3%
0.1% to 0.5%	4%
0.6% to 1.0%	6%
1.1% to 2.0%	9%
2.1% to 3.0%	11%
3.1% to 4.0%	15%
4.1% to 5.0%	17%
5.1% to 10.0%	18%
More than 10.0%	17%
Total	100%
Extrapolated value	5.0%

Q13. What is the likelihood your company will sustain a loss to information assets totaling 100 percent of PML over the next 12 months??	FY2024
Less than 0.1%	9%
0.1% to 0.5%	8%
0.6% to 1.0%	12%
1.1% to 2.0%	12%
2.1% to 3.0%	15%
3.1% to 4.0%	18%
4.1% to 5.0%	13%
5.1% to 10.0%	9%
More than 10.0%	4%
Total	100%
Extrapolated value	3.1%

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?	FY2024
Disclosure as a contingent liability on the balance sheet (FASB 5)	13%
Footnote disclosure in the financial statements	42%
Discussion in the management letter	11%
None – disclosure is not necessary	30%
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 4 percent of an organization's worldwide revenue?	FY2024
Yes, fully aware	41%
Yes, somewhat aware	48%
Not aware	11%
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.	FY2024
Yes	56%
No [skip to Q17]	44%
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.	FY2024
Cyber attack that caused disruption to business and IT operations (such as denial of service attacks)	50%
Cyber attack that resulted in the theft of business confidential information, thus requiring notification to victims	31%
Cyber attack that resulted in the misuse or theft of business confidential information, such as intellectual properties	36%
Negligence or mistakes that resulted in the loss of business confidential information	53%
System or business process failures that caused disruption to business operations (e.g., software updates)	47%
Other	7%
Total	223%

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.	FY2024
Zero	5%
Less than $10,000	7%
$10,001 to $100,000	9%
$100,001 to $250,000	15%
$250,001 to $500,000	18%
$500,001 to $1,000,000	14%
$1,000,001 to $5,000,000	12%
$5,000,001 to $10,000,000	7%
$10,000,001 to $25,000,000	6%
$25,000,001 to $50,000,000	5%
$50,00,001 to $100,000,000	2%
More than $100,000,000	0%
Total	100%
Extrapolated value US$	$5,022,223

Q16d. If yes, how has the above security exploit or data breach changed your company's concerns about cyber liability?	FY2024
More concerned	66%
Less concerned	11%
No change	23%
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?	FY2024
Increase	69%
Decrease	10%
Stay the same	21%
Total	100%

Q18a. From a business risk perspective, how do cyber risks compare to other business risks. Please select one best choice.	FY2024
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	35%
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	15%
Total	100%

Q18b. How did you determine the level of cyber risk to your company?	FY2024
Completed a formal internal assessment	25%
Completed an informal (ad hoc) internal assessment	22%
Hired a third party to conduct an assessment or audit	27%
Intuition or gut feel	18%
Did not do any type of assessment	8%
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?	FY2024
Yes	30%
No (please skip to Q21)	70%
Total	100%

Q19b. If yes, what limits do you purchase	FY2024
Less than $1 million	10%
$1 million to $5 million	31%
$6 million to $20 million	47%
$21 million to $100 million	9%
More than $100 million	3%
Total	100%
Extrapolated value (US$ millions)	$16.53

Q19c. Is your company's cyber insurance coverage sufficient with respect to coverage terms and conditions, exclusions, retentions, limits and insurance carrier financial security?	FY2024
Yes	56%
No	27%
Unsure	17%
Total	100%

Q19d. How does your company determine the level of coverage it deems adequate?	FY2024
Formal risk assessment by in-house staff	14%
Formal risk assessment conducted by the insurer	13%
Formal risk assessment by third party	24%
Informal or ad hoc risk assessment	14%
Policy terms and conditions reviewed by a third-party specialist	14%
Maximum available from the insurance market	20%
Other	1%
Total	100%

Q19e. What types of incidents does your organization's cyber insurance cover? Please select all that apply.	FY2024
External attacks by cyber criminals	78%
Malicious or criminal insiders	76%
System or business process failures	41%
Human error, mistakes and negligence	33%
Incidents affecting business partners, vendors or other third parties that have access to your company's information assets	44%
Third party vendors and suppliers, such as cloud, Software as a Service and infrastructure *	42%
Other	18%
Unsure	3%
Total	334%

Q19f. What coverage does this insurance offer your company? Please select all that apply.	FY2024
Forensics and investigative costs	68%
Notification costs to data breach victims	59%
Communication costs to regulators	45%
Employee productivity losses	54%
Replacement of lost or damaged equipment	62%
Revenue losses	34%
Legal defense costs	50%
Loss of asset value	46%
Regulatory penalties and fines	48%
Third-party liability	43%
Brand damages	27%
Ransomware payments and costs	34%
Other	8%
Unsure	12%
Total	588%

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.	FY2024
Access to cyber security forensic experts	81%
Access to legal and regulatory experts	81%
Access to specialized technologies and tools	52%
Advanced warnings about ongoing threats and vulnerabilities	43%
Assistance in the remediation of the incident	55%
Assistance in the notification of breach victims	45%
Identity protection services for breach victims	28%
Credit monitoring services for breach victims	47%
Assistance in reputation management activities	50%
Other	17%
Total	498%

Q20a. Does your company plan to purchase standalone cyber insurance?	FY2024
Yes, in the next 12 months	18%
Yes, in the next 24 months	28%
Yes, in more than 24 months	22%
No	32%
Total	100%

Q20b. If no, what are the **two** main reasons why your company is not planning to purchase standalone cyber security insurance?	FY2024
Premiums are too expensive	37%
Coverage is inadequate based on our exposure	38%
Risk does not warrant insurance	10%
Property and casualty policies are sufficient	29%
Executive management does not see the value of this insurance	25%
Unable to get insurance underwritten because of current risk profile	17%
Other	7%
Total	163%

Q21. Who in your company is **most responsible** for cyber risk management? Please select your two top choice.	FY2024
CEO/board of directors	5%
Chief financial officer	6%
Business unit (LOB) leaders	17%
Chief information officer	22%
Chief information security officer	19%
Risk management	12%
Procurement	7%
General counsel	5%
Compliance/audit	6%
Other	1%
Total	100%

Q22a. Does your organization use or plan to use cryptocurrency or non-fungible token assets?	FY2024
Yes, currently use	64%
No, but planning to use within the next 12 months	21%
There are no plans to use	15%
Total	100%

Q22b. Does your organization use or plan to use artificial intelligence products or services?	FY2024
Yes, currently use	67%
No, but planning to use within the next 12 months	19%
There are no plans to use	14%
Total	100%

Part 3. Intellectual Property risks

Q23. 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?	FY2024
Yes	61%
No	39%
Total	100%

Q24a. What is the total value of your company's IP assets such as trademarks, patents, copyrights, trade secrets and know-how?	FY2024
Less than $1 million	1%
$1 to 10 million	10%
$11 to 50 million	17%
$51 to 100 million	24%
$101 to 500 million	28%
$501 to 1 billion	14%
$1 to 10 billion	4%
More than $10 billion	2%
Total	100%
Extrapolated value	$599.27

Q24b. What is the IP asset percentage value of your company's total assets (intellectual property includes trademarks, patents, copyrights, trade secrets and know-how)?	FY2024
Less than 5%	6%
5% to 10%	11%
11% to 25%	15%
26% to 50%	20%
51% to 75%	25%
More than 75%	23%
Total	100%
Extrapolated value	47%

Q25a. Did your company experience a material IP event in the past 24 months?	FY2024
Yes	50%
No	50%
Total	100%

Q25b. If yes, what type of IP assets were involved in the event?	FY2024
Patent	32%
Trade secret	36%
Copyright	25%
Other	7%
Total	100%

Q25c. If yes, what best describes the event?	FY2024
Challenge to company rights	33%
Infringement of company rights	37%
Allegation of company infringement of third-party rights	30%
Total	100%

Q26. How do IP risks compare to other business risks?	FY2024
IP risk is the number one or two business risk for my company	19%
IP risk is a top 5 business risk for my company	34%
IP risk is a top 10 business risk for my company	30%
IP risk is not in the top 10 of business risks for my company	17%
Total	100%

Q27. Does your company's existing insurance policy (e.g., property, general liability or crime) cover any of the following IP events?	FY2024
A challenge to your company's IP assets	36%
Third-party infringement of your company's IP assets	33%
An allegation that your company is infringing third-party IP rights	32%
Our existing policy does not cover IP events	33%
Total	134%

Q28a. Does your company have a trade secret theft insurance policy as a complement to a cyber risk policy?	FY2024
Yes	35%
No	65%
Total	100%

Q28b. 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?	FY2024
Very interested	33%
Interested	31%
Somewhat interested	28%
Not interested	8%
Total	100%

Q29a. Does your company have an intellectual property liability policy?	FY2024
Yes	34%
No	66%
Total	100%

Q29b. If not, what is your company's level of interest in purchasing an intellectual property liability policy?	FY2024
Very interested	31%
Interested	31%
Somewhat interested	26%
Not interested	12%
Total	100%

Q30. Can an external cyber and intellectual property incident become a Black Swan for your firm?	FY2024
Yes	44%
No	48%
Unsure	8%
Total	100%

Q31. For a Black Swan, even if you cannot predict the event type, firms are able to prepare for the impact of the event. Is preparation for a Black Swan event part of your enterprise risk management approach?	FY2024
Yes	44%
No	46%
Unsure	10%
Total	100%

Part 4. Role & Organizational Characteristics

D1. What level best describes your current position?	FY2024
Senior executive	7%
Vice president	8%
Director	10%
Manager	18%
Supervisor	19%
Associate/staff	19%
Technician	9%
Contractor/consultant	6%
Other	4%
Total	100%

D2. What is the worldwide employee headcount of your company?	FY2024
Less than 500	14%
500 to 1,000	17%
1,001 to 5,000	23%
5,001 to 25,000	24%
25,001 to 75,000	14%
More than 75,000	8%
Total	100%

D3. What best describes your company's industry focus?	FY2024
Communications	3%
Consumer products	5%
Defense & aerospace	1%
Education & research	4%
Energy & utilities	6%
Entertainment & media	3%
Financial services	18%
Health & pharmaceuticals	8%
Hospitality	5%
Manufacturing	10%
Public sector	8%
Retailing	9%
Services	9%
Technology & software	7%
Transportation	3%
Other	1%
Total	100%

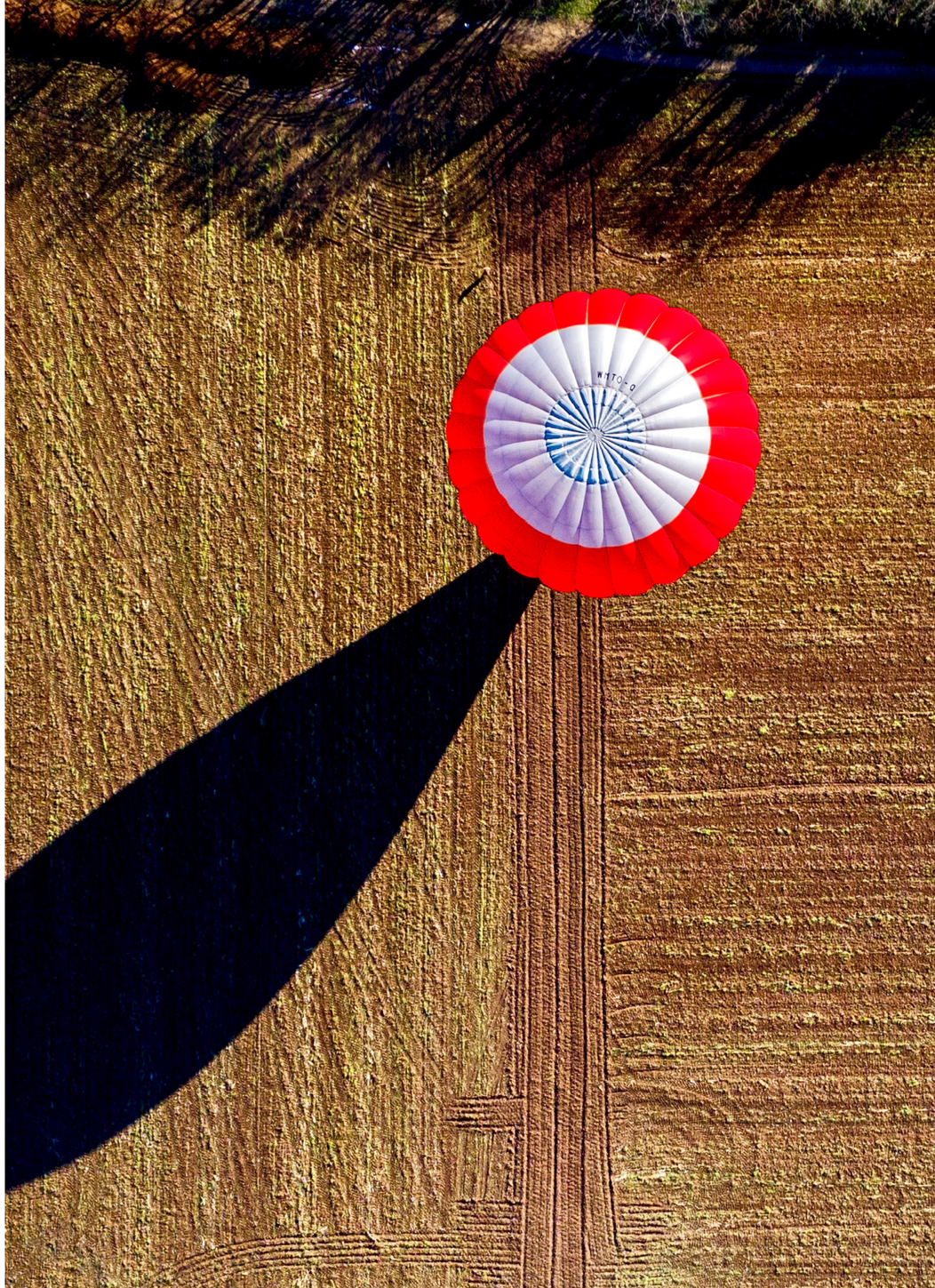
Acknowledgements

The 2024 Intangible Assets Financial Statement Impact Comparison Report is the fifth intangible assets/cyber risk transfer research paper that examines 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
Intangible Assets Global Collaboration Co-Leader
Aon

Christine Williams
Managing Director
Greater New York Region
Aon

Kevin Kalinich Esq
Intangible Assets Global Collaboration Leader
Aon



DISCLAIMER: the paper was written without the assistance of any Language Learning Models, including but not limited to BERT, Claude, Cohere, Ernie, Falcon 40B, Gemini, Gemma, GPT, Lamda, Llama, Mistral, Orca, Palm, Phi-1, StableLM, or Vicuna 33B. All research, writing and editing was executed by human authors.

> It's tough to make predictions, especially about the future.
>
> **Yogi Berra**

> I am heartened that a younger generation of computer scientists is taking existential risk seriously. We humans should make our best efforts to stay around.
>
> **Geoffrey Hinton**
> Godfather of AI

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 C**ouncil of American Survey Research Organizations (CASRO)**,we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

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.

About

Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Through actionable analytic insight, globally integrated Risk Capital and Human Capital expertise, and locally relevant solutions, our colleagues provide clients in over 120 countries and sovereignties with the clarity and confidence to make better risk and people decisions that help protect and grow their businesses.

Follow Aon on LinkedIn, X, Facebook and Instagram. Stay up-to-date by visiting Aon's newsroom and sign up for news alerts here.