2022 Intangible Assets Financial Statement Impact Comparison Report

Global Edition

Sponsored by Aon
Independently conducted and produced by Ponemon Institute LLC

Contents

1

A Tale of Two Types of Assets – Introduction

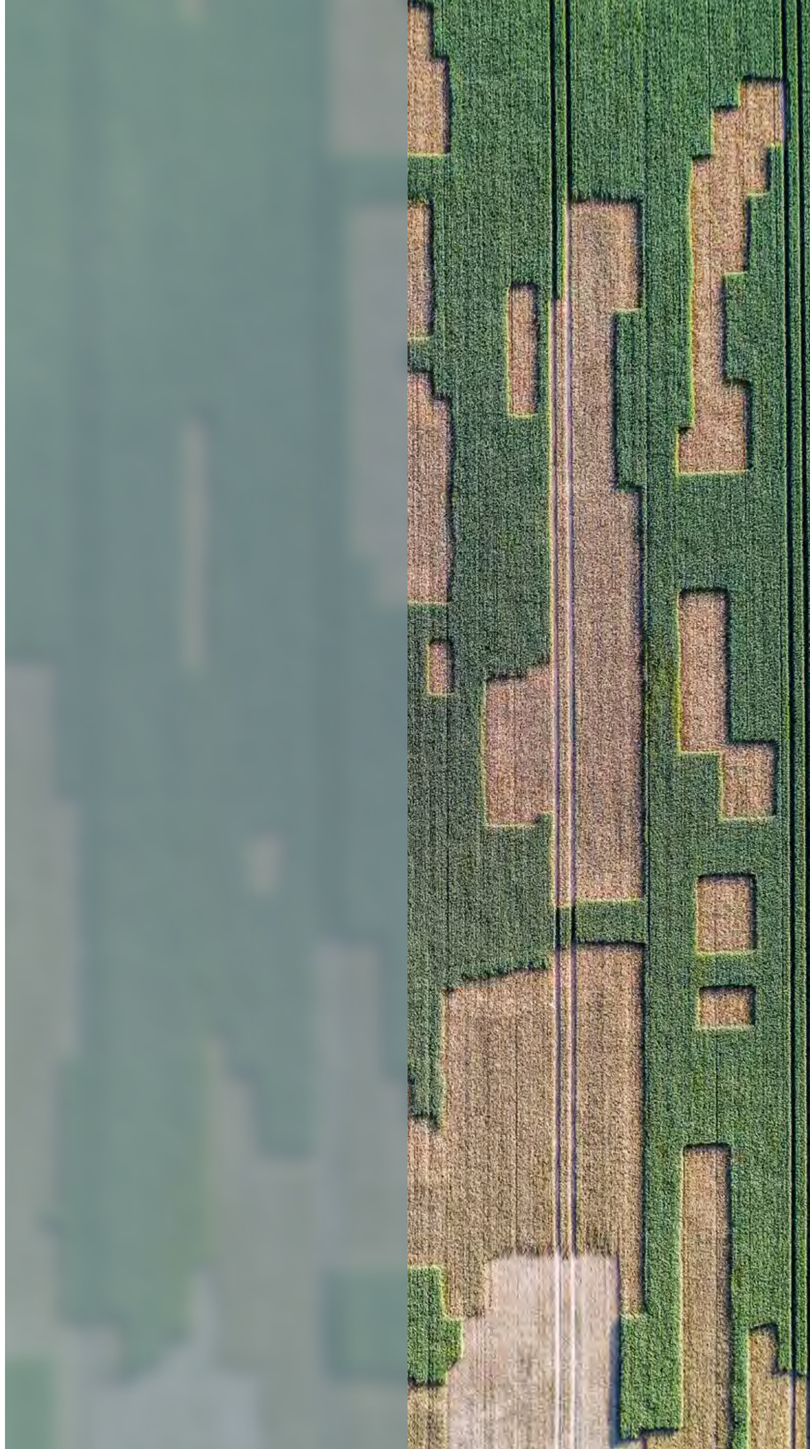
A Tale of Two Types of Assets – Introduction

Can organizations make better decisions regarding allocation of their finite resources between tangible[1] and intangible assets[2]?

Compared to tangible assets, what are the relative financial statement value and exposure[3] of intangible assets[4], such as data, intellectual property[5], computer systems and other specified digital assets?[6]

How do we measure return on investment[7] and return on equity for risk management decisions, given the rapid adoption of digital assets?[8]

> “Innovation leaders need to identify, value and track digital assets, intellectual property and new technologies. By doing so they can help businesses make better decisions regarding new solutions, leverage IP, transform their operations and mitigate risks.
>
> **Jillian Slyfield**
> Aon Chief Innovation Officer



[1] Property, Plant & Equipment (“PP&E”)

[2] Additional intangible assets that lack physical substance are beyond the scope of this study, such as goodwill, brand equity, licensing, 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

[3] Putting a dollar value on intangible assets and perils, even without long term historical benchmarking or perfect mathematical modelling, is a useful first step for leaders to make better decisions to allocate resources. For example, Fast Company’s “The 10 Most Innovative Finance Companies of 2022” includes Aon’s Quality of Intellectual Property valuation tool.

[4] Why is it important to identify your most valuable intangible assets?

[5] https://riskandinsurance.com/11-tips-designed-to-protect-any-companys-intellectual-property/?rid=42939

[6] “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.

[7] Cyber Insurance Is a Perfect Storm: Risk Quantification Can Rescue It – CPO Magazine

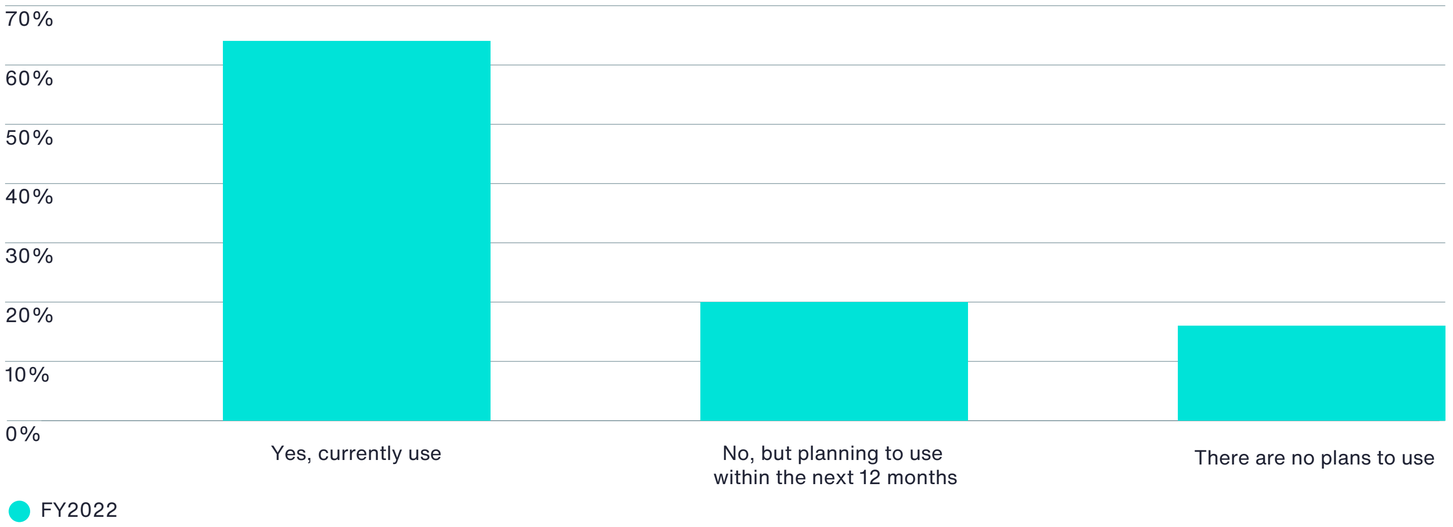
[8] According to recent research conducted by Reuters, an estimated 70% of new value created in the coming decade is forecast to be based on digitally-enabled platforms. Protecting Intellectual Property in the Digital Age

1 Complexity to Clarity

> Large, complex organizations that integrate a data and analytics-based enterprise risk management process are better positioned to mitigate risks to their intangible and digital assets, while protecting their balance sheet.

Lori Goltermann
Chief Client Officer & CEO
Global Enterprise Clients
Aon plc

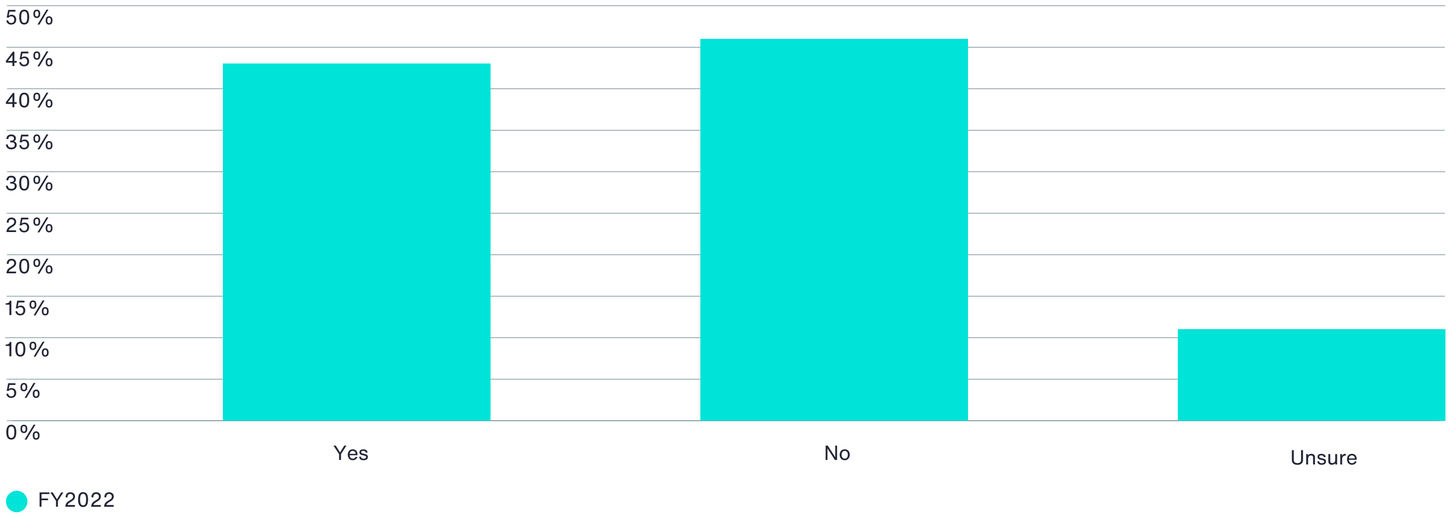
Figure A. 84 percent of Organizations use or Intend to use Cryptocurrency or Non-Fungible Tokens (NFT's) in 2022[9]



[9] 2022 Aon/Ponemon Intangible Assets Financial Impact Study.

Can digital and intellectual property[10] incidents become "black swans?"[11] If so, then these issues should be considered by the board of directors.[12] What about "gray swan" incidents?[13] While data on gray swan events are lacking, preparation is still possible to anticipate and combat these relatively rare but significantly risky events.[14] Less than half of organizations prepare for a cyber or IP black swan event.[15]

Figure B. 43 percent of Organizations Prepare for a Black Swan Event as Part of Their Enterprise Risk Management Approach[16]



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

[11] 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.

[12] Is Cyber Risk a D & O Risk? Ethical Boardroom.; IP Within the Boardroom: Is Intellectual Property a Director & Officer Issue? Ethical Boardroom; Why the pressure is on directors and officers over cyber

[13] The Signs Are There: Recognizing and Preparing for Gray Swans, such as cyber and intellectual property

[14] Black and Grey Swans: 5 Ways to Avoid Shocks - Aon https://www.aon.com/risk-services/professional-services/black-and-grey-swans-5-ways-to-avoid-shocks.jsp

[15] 2022 Aon/Ponemon Intangible Assets Financial Impact Study.

[16] 2022 Aon/Ponemon Intangible Assets Financial Impact Study.

The purpose of this research is to compare the relative insurance protection of specified tangible versus certain intangible assets. How do the potential losses related to intangible asset values from evolving perils, such as cryptocurrency[17] fraud, computer system disruptions and IP misappropriation, compare to potential losses related to tangible asset values from traditional perils, such as fires and weather? Given the melding of tangible and intangible asset values and perils with the advent of robotics, machine learning[18], Web3[19], metaverse[20], artificial intelligence[21], Internet of Things[22]/5G, augmented reality[23], NFTs[24], decentralized autonomous organizations, blockchain[25], decentralized finance (DeFI), smart contracts, cryptocurrency[26], etc.[27], is it even possible anymore to separate modelling of intangible assets and losses compared to tangible assets and losses?[28]

[17] Digital Assets: At the Intersection of Law, Regulation, Public Policy and Technological Innovation

[18] What governance structures shape the development and deployment of responsible machine learning tools?

[19] Are You Ready for Web3.0 and the Legal Issues it Will Bring? | Sheppard Mullin Richter & Hampton LLP - JDSupra; 3 Web3 Predictions for 2022

[20] The metaverse is a collective virtual open space, created by the convergence of virtually enhanced physical and digital reality. It is physically persistent and provides enhanced immersive experiences.

[21] AI: Insurance, business and liability considerations; How will AI expand and accelerate the impact of Big Data, including the volume, variety, and velocity of information? As AI evolves, how will it magnify the ability to use personal information in ways that can intrude on privacy interests? Do regulatory approaches focused on "automated decisions" encourage the development of privacy-centered AI, or do they hinder innovation? How significant is the threat of algorithmic bias, or the use of voice, facial recognition, or biometric sensing tools in the hands of malicious state or non-state actors?

[22] NIST Publishes Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products

[23] The virtual reality gaming trend is getting real when it comes to homeowner's insurance claims, with insurers saying popular virtual reality headsets are the cause of a 31% surge in claims.

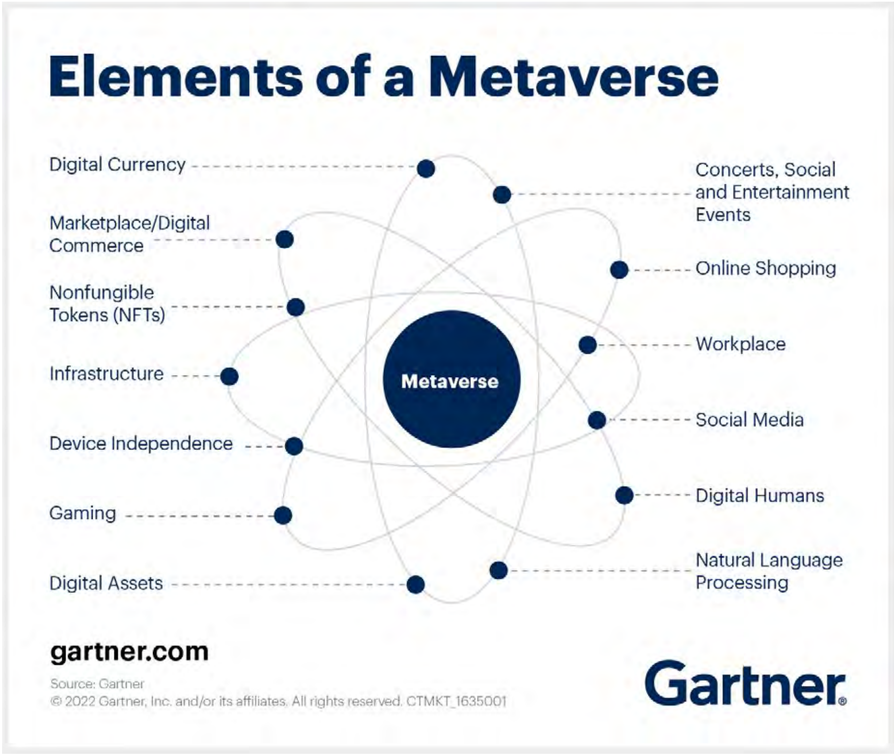
[24] How NFTs Create Value; NFT trends that will bring social media audiences into web3

[25] Cryptocurrencies hog the spotlight, but blockchain's biggest innovations are below the surface, saving billions each year for the world's largest companies. Forbes 50 Blockchain Leaders 2022

[26] Institutional cryptoasset trading soared in 2021. In 2020, institutions had only invested $120 billion in cryptoassets on Coinbase Global, but that figure soared to $1.14 trillion in 2021, more than double the $535 billion invested by retail traders. The dramatic increase in participation indicates how quickly cryptoassets are becoming a mainstream investment.

[27] Cryptocurrencies, Other Digital Assets and Blockchain - Financial Institution Risk Management | Aon

[28] Future Tech "Moonshots" that include radical technologies that could transform industries, economies and societies are beyond the scope of our 2022 research

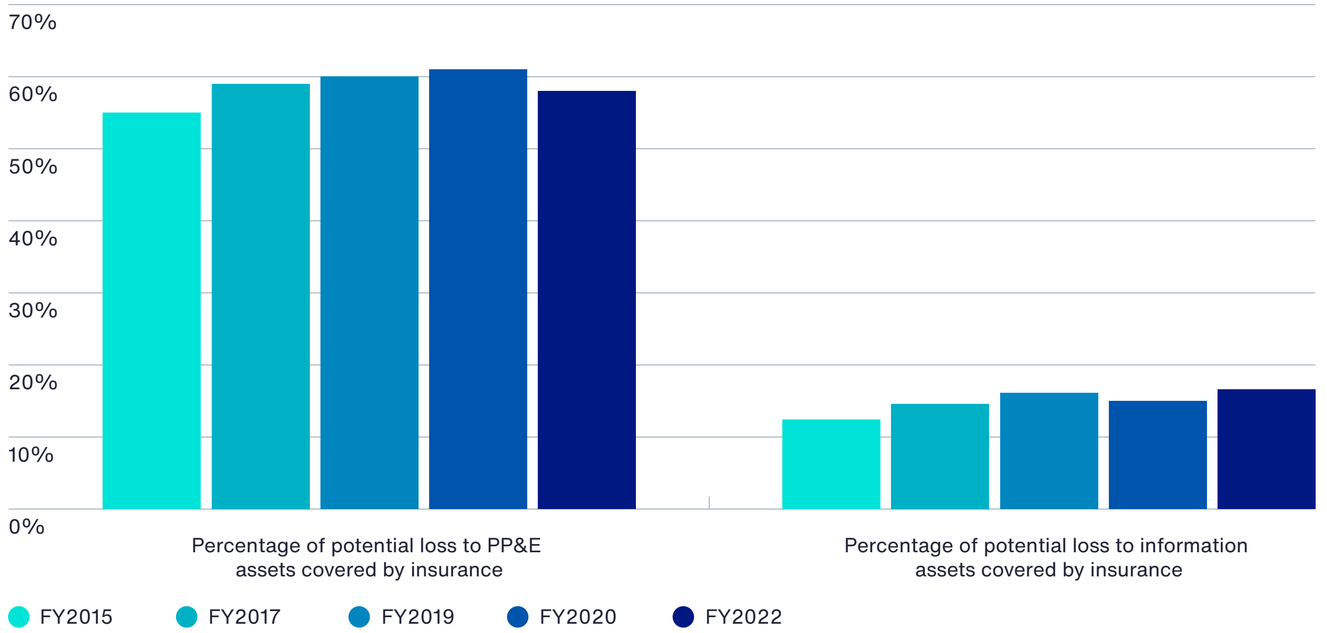


*Gartner®, "What is a Metaverse", Jan 28, 2022.

Since 2015, Aon and Ponemon Institute have studied the financial statement impact of tangible property compared to intangible assets. While initially focused on losses relating to cyber, the study's scope has expanded to include developing digital assets and intellectual property.[29] A better understanding of the relative financial statement impact of these losses will assist organizations to make better decisions[30], allocate resources and determine the optimal amount of risk transfer, including insurance[31], to mitigate the financial statement impact of intangible asset losses, and potentially increase the value of the underlying intangible assets.[32]

Tangible assets (despite lower value) are insured three times greater (58 percent vs 16.6 percent) than intangible assets (although intangible assets are gaining, particularly information assets).[33]

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



[29] 2022 Aon/Ponemon Intangible Assets Financial Impact Study.

[30] Treating Cyber Risks – Using Insurance and Finance." Chapter 10 of John Wiley and Sons Book: *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*; Haskel, Jonathan and Stian Westlake. *Capitalism Without Capital: The Rise of the Intangible Economy.* Princeton University Press: 2018.

[31] Cyber insurance can help businesses save millions of dollars and years of recovery in the event of a cyberattack.

[32] Right IP Strategy Can Maximize Value—IPO, M&A, Enterprise

[33] 2022 Aon/Ponemon Intangible Assets Financial Impact Study.

Cyber exposures can broadly include network business interruption, breach of privacy and security of personally identifiable information, ransomware, system failure, confiscating online bank accounts, creating and distributing viruses on computers, robotic malfunctions and disrupting a country's critical national infrastructure.[34] Cyber assessment severity and frequency[35] modeling show that the potential largest 2022 material financial statement impact in the majority of cyber incidents is business interruption, ransomware[36] and theft of intellectual property.[37]

At its most basic, insurance is a financial instrument — a way to finance 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 challenge for cyber insurance in 2022 is that, while organizations look to increase limits purchased, the cyber insurance market is reducing capacity, limiting the scope of coverage, increasing premiums, raising retentions/deductibles and adding underwriting scrutiny.[38]

[34] Lights Out! Can Insurance Help? Risk & Insurance.

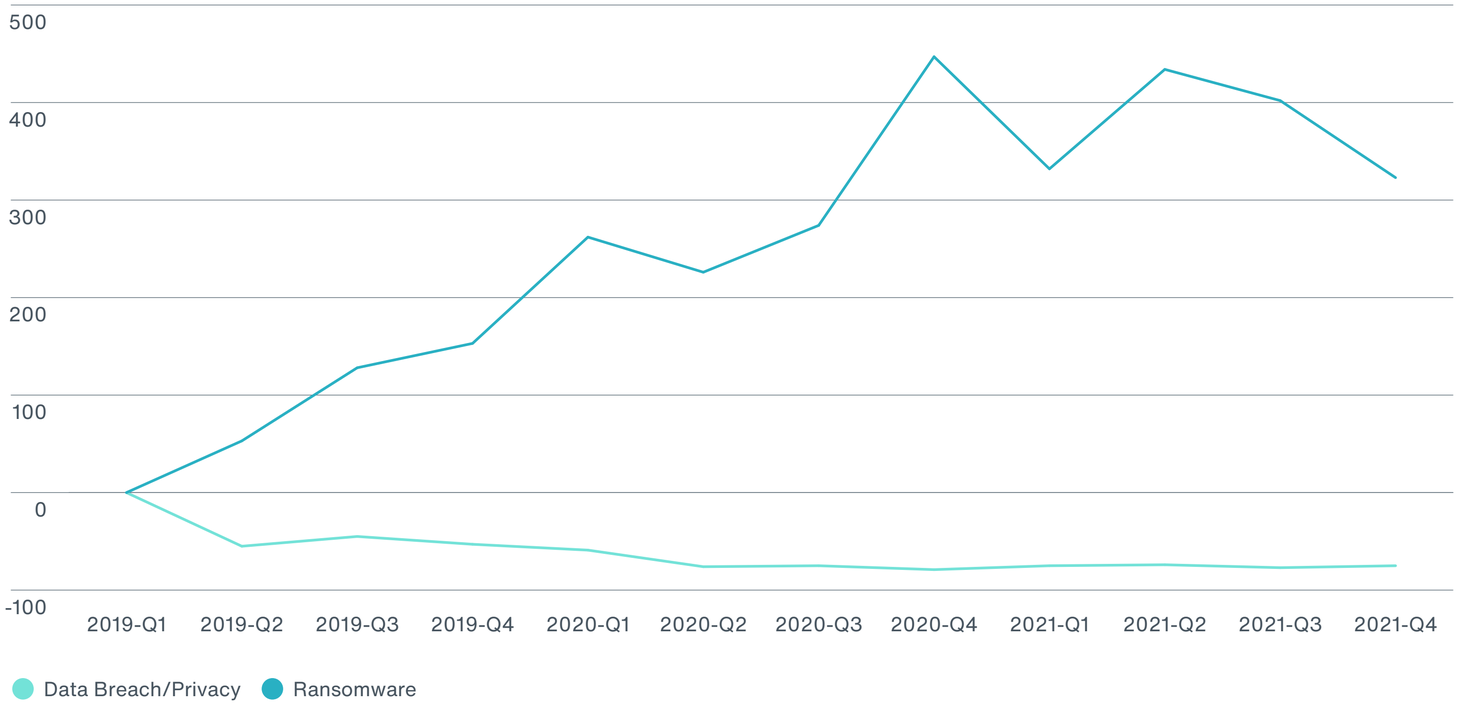
[35] According to a 2021 Annual Data Breach Report, the overall number of data compromises (1,862) is up more than 68 percent compared to 2020.

[36] IBM's 2022 Data Breach report (study also conducted by Ponemon), which covers 2021, also reported ransomware as the top attack type; phishing and unpatched vulnerabilities as leading infection vectors; manufacturing as the most attacked industry; and Asia as the most attacked region. Cost of a Data Breach Report 2021 | IBM

[37] https://www.aon.com/thought-leadership/ponemoninstitutereport.jsp

[38] Underwriters now take a fine-toothed comb to commercial cybersecurity practices, and regulators are starting to do the same. Scrutiny ratcheting up for companies' cyber insurance, practices | PropertyCasualty360

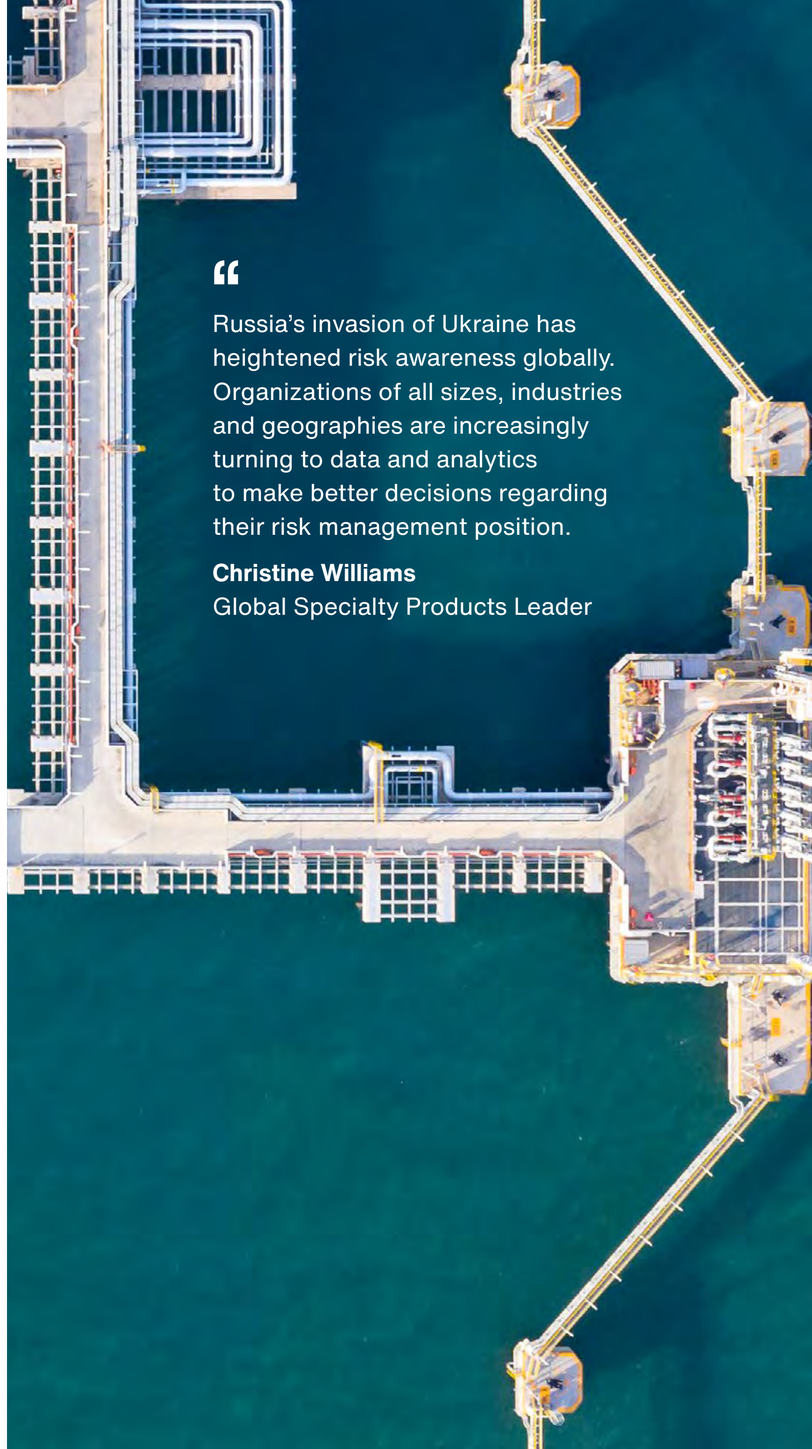
Ransomware Activity Materially Outpaced Data Breach/Privacy Event Activity



The Russian invasion of Ukraine will test the effectiveness of "war exclusions,"[39] "hostile act exclusions" and "cyberterrorism carvebacks" language in insurance policies for cyber-related losses.[40] Aon is seeing an increased focus on the cybersecurity sector (and related cyber insurance coverage)[41], which could boost spending this year above their prior budgeted amounts in order to address ransomware, protect datacenters, networks, vulnerability points and other highly sensitive data.[42] Cyber perils and solutions can vary by industry[43], size of organization[44], and geography.[45] Additional lines of insurance are also in flux due to the Russian attack on Ukraine.[46]

Cyber warfare is only one development in the intangible assets and perils world. Additional dynamic and fluid intangible assets opportunities and challenges include[47]:

- Biometric privacy lawsuit costs likely to exceed $8 billion by 2025[48]
- Increased frequency and severity of regulatory fines, penalties and assessments, including GDPR[49]
- Evolving cyber security regulation[50]



"Russia's invasion of Ukraine has heightened risk awareness globally. Organizations of all sizes, industries and geographies are increasingly turning to data and analytics to make better decisions regarding their risk management position.

Christine Williams
Global Specialty Products Leader

[39] Cyber Risk Toolkit: American Academy of Actuaries (War Exclusion on page 65)

[40] Ukraine conflict increases risk of systemic cyberattack and could see rates rise further; Cyber insurance claims expected to rise amid Ukraine-Russia war; Russia: The Sickness of a Nation

[41] On March 21, 2022, President Biden warned of evolving intelligence about potential cyberattacks. The FBI and the Cybersecurity & Infrastructure Security Agency (CISA) have warned about possible threats to U.S. and international satellite communications networks and the energy sector, and the pace of government warnings has increased.

[42] Ukraine invasion adds to insurers' cyber risks: Fitch | Business Insurance

[43] Cyber Insurance For Law Firms and Legal Organizations. Chapter 16 of The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals, Third Edition (americanbar.org) 2022; Navigating New Forms of Volatility - Building Reputational Resilience in the TMT Sector; Building reputational resilience | Aon

[44] The importance of intangible assets for your startup

[45] "The Price of Data Security: A guide to the insurability of GDPR fines across Europe, 3rd Edition".

[46] Political risk insurance market pulls back from eastern European exposures; Russia's Ukraine Invasion Deals Shock To Insurance Industry; Management Liability Market Outlook for 2022 Report | Aon

[47] "You cannot solve the risk management issue in the middle of a crisis, you obviously need to solve it ahead of time." — Ruth Porat, Alphabet CFO.

[48] With biometric data collection and use becoming more common and privacy laws expanding, the fines and settlements tied to regulatory violations will likely reach over $8 billion by 2025, according to recent commentary from Gartner. www.Gartner.com

[49] Fines for breaches of EU privacy law spike sevenfold to $1.2 billion, as Big Tech bears the brunt;Cyber Perils in a Growing Market – Helping EMEA organizations better understand the interconnectivity among multiple lines of insurance.; The Price of Data Security: A guide to the insurability of GDPR fines across Europe (3rd Edition, May 25, 2020).

[50] SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies; New Critical Infrastructure Cybersecurity Implementing New Breach Notification Requirements Signed into Law (The new law will require critical infrastructure entities to report certain covered cybersecurity incidents to government agencies within 72 hours; ransomware payments within 24 hours); Federal Banking Regulators Issue 36-Hour Cybersecurity Breach Notification Requirement; The Securities and Exchange Commission is exploring ways to improve cybersecurity in capital markets, including by extending compliance obligations to companies that currently don't have to meet them. Announced Cryptocurrency Executive Order Will Shape Federal Regulations for the $3 Trillion Digital Assets Market

- Cyber incidents were rated as the greatest peril to business in 2022[51], followed by business interruption and natural catastrophes[52]
- Ransomware is a patient mortality risk, driven by COVID-19 and third-party vendors[53]
- 87 percent of companies depend on their employees' ability to access business software and data from their personal devices. And that's likely to grow, as 36.2 million Americans are expected to work remotely by the year 2025, nearly double pre-pandemic levels[54]
- Should environmental, social and governance (ESG) and/or diversity, equity and inclusion (DE&I) be included with intangible assets?[55]
- As more gamers, sports, entertainment, creators and artists leverage NFTs as a monetization stream, the intellectual property rights as to who owns what using this new technology will increase litigation[56]

[51] Aon Global Risk Management Survey; The most important insurance purchase (excluding D&O) is led by 1) cyber, 2) professional indemnity and 3) property damage/business interruption.

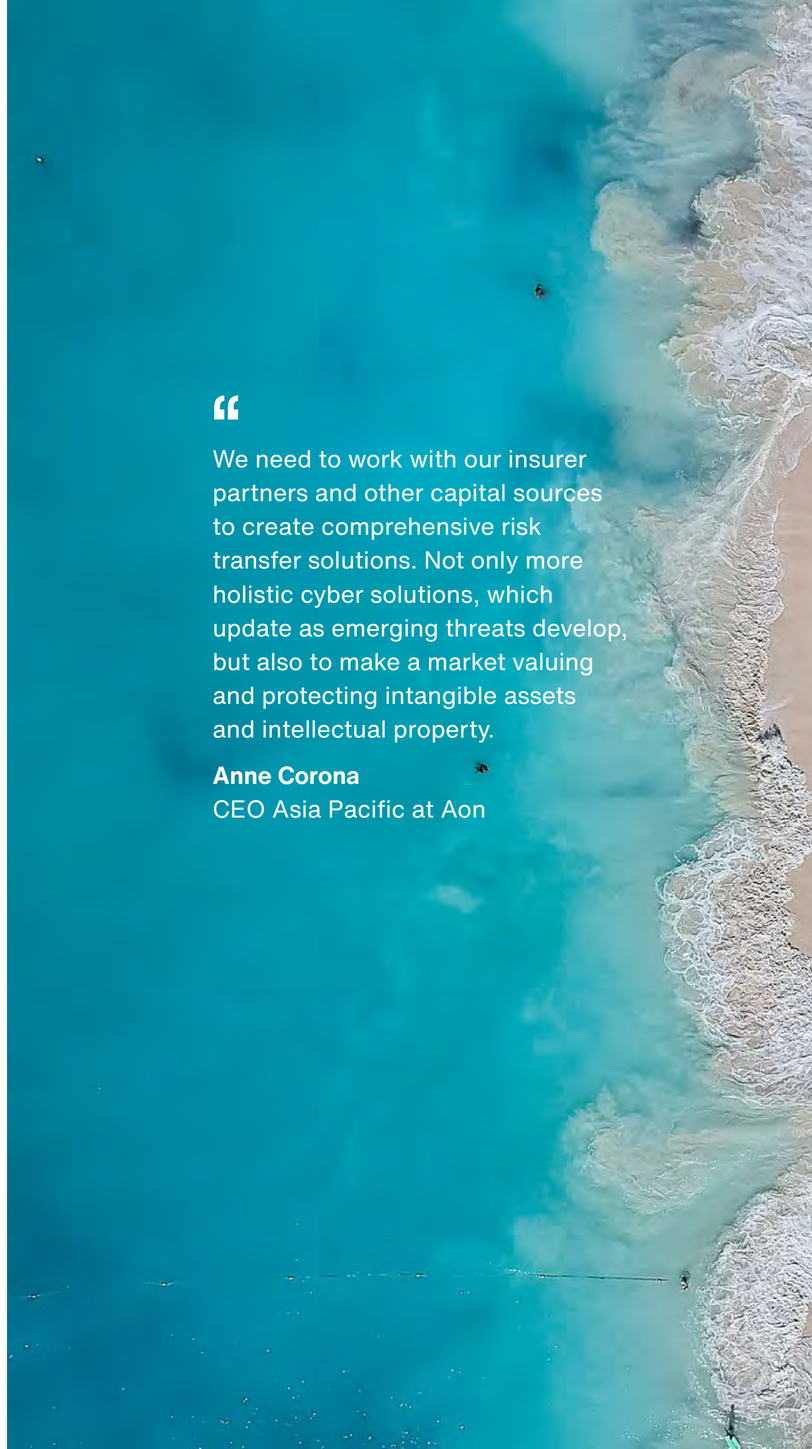
[52] Allianz Risk Barometer 2022: Cyber perils outrank Covid-19 and broken supply chains as top global business risk; Wake-up calls and eye-opening statistics reveal the full extent of cyber risk

[53] https://www.scmagazine.com/analysis/ransomware/report-ransomware-is-a-patient-mortality-risk-driven-by-covid-third-party-vendors

[54] https://www.phelps.com/insights/10-keys-to-an-effective-byod-and-remote-access-policy.html

[55] Yes, but not for the purposes of this study. We may consider ESG/DEI in the future as we collect and analyze data on a quantitative basis:

[56] Quentin Tarantino's 'Pulp Fiction' NFT Battle With Miramax Heats Up - WSJ



"We need to work with our insurer partners and other capital sources to create comprehensive risk transfer solutions. Not only more holistic cyber solutions, which update as emerging threats develop, but also to make a market valuing and protecting intangible assets and intellectual property.

Anne Corona
CEO Asia Pacific at Aon

Impact as an Intangible Asset

E	S	G
Environmental	**Social**	**Governance**
Climate Change	Human Capital	Accounting
Natural Resources	Product Liability	Diversity
Pollutions and Waste	Stakeholder Opposition	Business Ethics
Environment Opportunity	Social Opportunity	Competitive Practices

- Exponential crypto growth exceeds $2 trillion market capitalization[57]
- Cryptocurrency-based crime hit a record high last year, with criminals pocketing $14 billion worth of Bitcoin, Ethereum and other digital currencies from scams, ransomware and thefts[58]
- March 9, 2022: the Biden Administration released an Executive Order aimed at the crypto industry[59]
- New sources of capital are being formed to address intangible assets, such as insurance linked securities, captives (with reinsurance), alternative risk transfer, cyber pools, etc.[60]
- The most innovative companies based on their patent filings[61]

[57] Insurance for the booming crypto market | PropertyCasualty360

[58] https://go.chainalysis.com/2022-Crypto-Crime-Report.html

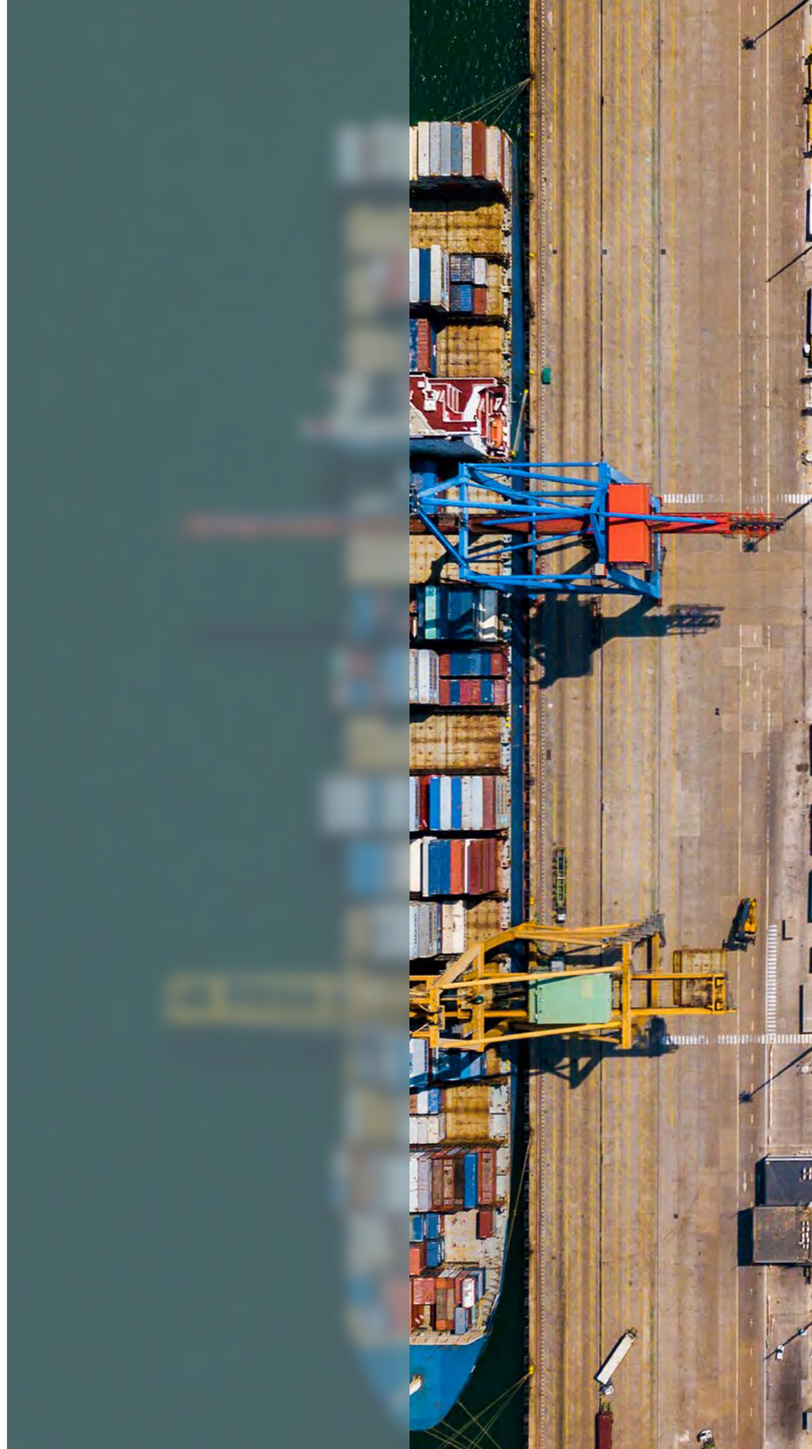
[59] The White House Fact Sheet – President-Biden-to-sign-executive-order-on-ensuring-responsible-innovation-in-digital-assets/: The long anticipated order's purpose is to "ensure the responsible innovation of digital assets" and was broken up into seven primary areas of focus. Notably the White House addressed the need for fair and equitable access to safe and affordable financial services, while also calling for enhanced attention to consumer, investor, and business protections. The order also confirmed the importance of the research being done on Central Bank Digital Currency (CBDC) and encouraged the Fed to continue its experimentation. The EO provides some much-needed guidance to the industry and should encourage further adoption from financial institutions (including insurance companies).

[60] Long-tail risks, including climate change and cyber risk, are creating unprecedented volatility. There are solutions to these challenges but they require collective action, focused efforts, and new strategies. To successfully address these new forms of volatility, we have to access new forms of capital. The capital across the balance sheets of all the insurers in the world is about $4.5 trillion, but we also need to connect with sources of capital that can play a role through those partners. Whether it's in pension or sovereign funds, that could open up the window to the better part of $150 trillion. So, magnifying that $4.5 trillion to $150 trillion with the mission of matching capital to risk, to reduce volatility as companies take action or address these other forms of volatility is a tremendous opportunity.

[61] https://www.econsight.ch/en/ranking-the-most-innovative-companies-in-the-world/

The coronavirus (COVID-19) pandemic supply chain challenges negatively affected tangible property manufacturing and shipments, and provided more opportunities for intangible Information Technology Security vendors (with added risk scrutiny). While remote work may have decreased in person office "property" type exposures, contingent business interruption exposures increased correlated to remote working. Yet, the majority of third-party vendors aren't meeting insurance obligations. In fact, more than 20 percent of third-party vendors simply don't respond when asked to verify commercial insurance coverage.[62] Worse, multiple studies show that a majority of organizations have insufficient understanding of their third-party cyber risks and fail to formally assess their risk exposure.[63] Given statistics that show a multi-party data breach creates 26 times the financial damage of a single-party breach, increased cyber insurance carrier underwriter scrutiny is focused on vendors.[64]

> "As the global digital economy becomes increasingly interconnected, companies must look to manage risks associated with third parties by requiring that suppliers and vendors carry standard levels of insurance, especially for cyber, tech E&O and IP perils.
>
> **Derek Lietz**
> Aon Vendor Risk Management Global Leader



[62] https://www.propertycasualty360.com/2022/02/22/majority-of-third-party-vendors-arent-meeting-insurance-obligations/?kw=Majority%20of%20third-party%20vendors%20aren%27t%20meeting%20insurance%20obligations&utm_campaign=workerscompwatch&utm_content=20220301&utm_medium=enl&utm_source=email&utm_term=pc360&slreturn=20220206162832

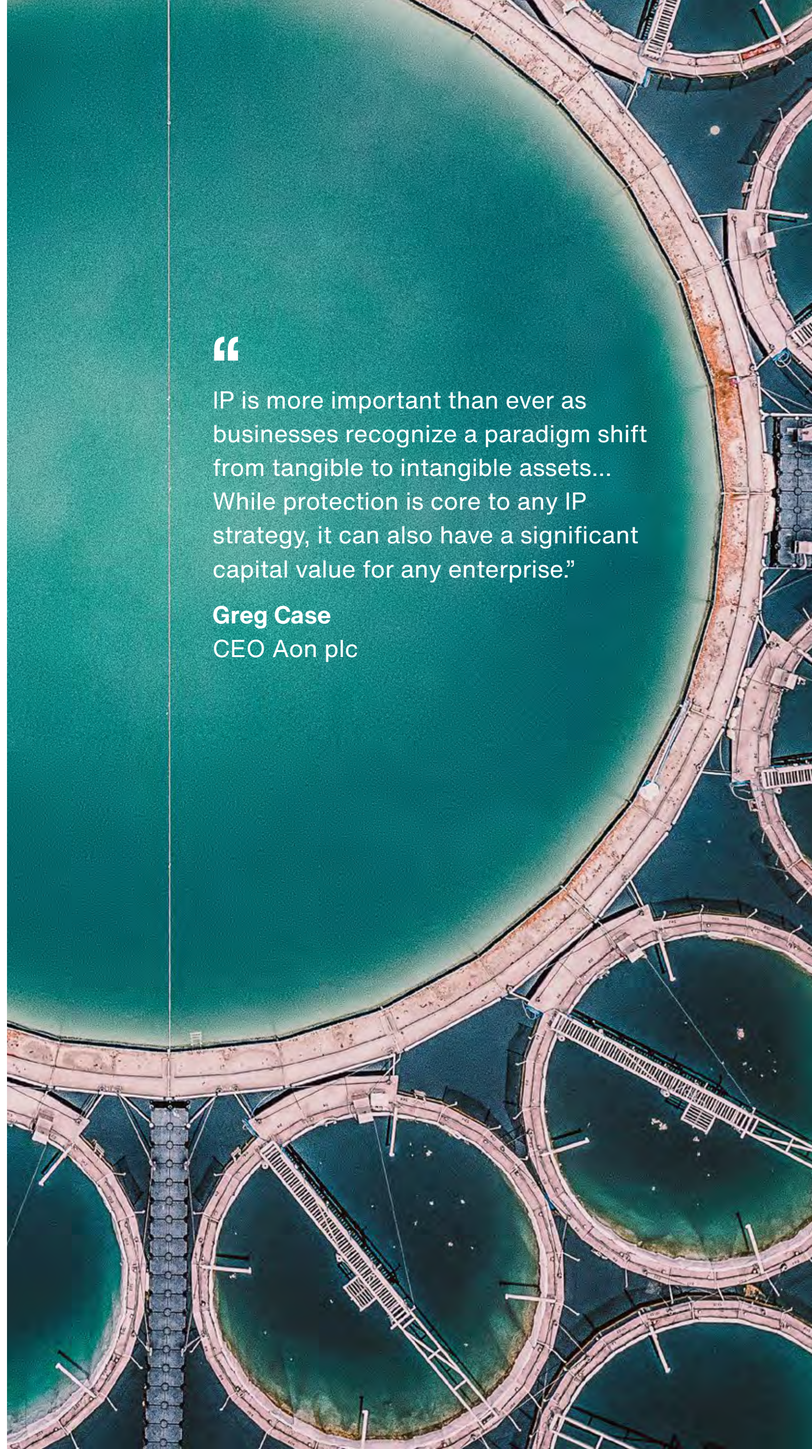
[63] 2022 PWC Global Digital Trust Insights Survey

[64] https://www.helpnetsecurity.com/2021/09/27/multi-party-data-breach/

> “We are focused on addressing client need around long-tail risks — particularly IP and cyber — and there is a tremendous market opportunity that goes along with it.
>
> **Greg Case**
> CEO Aon plc[65]

As the COVID-19 pandemic evolves into an endemic[66], what is the effect on intellectual property assets, perils[67] and opportunities?[68] Are there new insurance[69] and capital enhancement solutions? For instance, where does IP fit into virtual trademarks and the metaverse?[70] How about NFTs and blockchain?[71]

The modern patent litigation space is largely driven by tech companies, including computers, electronics, networking, software and semiconductors.[72] Together, these companies represented 45 percent of patent defenses in 2021, and this percentage has only grown over time.[73] The technology industries haven’t been the only contributor to the overall increase. For example, the number of litigations in the automotive industry—historically not a particularly litigious space pre-electric vehicles/autonomous vehicles—nearly doubled from 2019 to 2021.[74]



[65] Aon plc Quarterly Earnings Call, pp. 16 - 17

[66] The end is near: The new pandemic data looks promising — for some, anyway: The end is near, for some anyway, as the new pandemic data looks promising — CNN; Rapid emergence of SARS-CoV-2 Omicron variant is associated with an infection advantage over Delta in vaccinated persons:

[67] What is Intellectual Property Theft?

[68] Intellectual property in a post-pandemic future part I – The world has become more IP-intensive; IP assets in a post-pandemic world part II - What exactly is IP culture?

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

[70] https://www.amicalaw.com/virtualtrademarks

[71] IP trends for 2022: Blockchain and non-fungible tokens

[72] Here the technology industry includes software, electronics, computers, networking and semiconductors

[73] Patent Litigation Trends - 2021 Year End Report | Aon

[74] Corporate industry data derived from Factset (2022). Corporate Metadata [Data File]. https://www.factset.com. Litigation data derived from Lex Machina.

Top Technical Fields in PCT Applications

Which countries specialize in which technologies?

Applicants from China and the U.S. filed more applications in the field of computer technology, those from the Republic of Korea filed intensively for patents related to digital communication. For Japan and Germany, top technology field was electrical machinery.

Following are some of the key takeaways from this research.

Companies value information assets slightly higher than they do PP&E[75]. The average total value of PP&E is approximately $1,109 million for the companies represented in this research. The average total value of information assets is slightly higher at **$1,213 million**.

The value of Probable Maximum Loss ("PML")[76] **is higher for information assets than for PP&E**. Companies estimate the average PML resulting from stolen or destroyed information at approximately **$1,152 million**. In contrast, the average value of the largest loss that could result from damage or total destruction of PP&E is approximately **$839** million. Business disruption has a greater impact on information assets (**$321 million**)[77] than on PP&E (**$143 million**).

Insurance coverage is higher for PP&E than for information assets. On average, approximately 58 percent of PP&E assets are covered by insurance and approximately **30 percent** of PP&E assets are self-insured.[78] While the likelihood of a loss is higher for information assets than for PP&E, only an average of 17 percent of information assets are covered by insurance, while self-insurance is higher for information assets at 60 percent.

Thirty-three percent of respondents believe no disclosure of a material[79] **loss to information assets is required. Forty-two** percent of respondents say their company would disclose a material loss to PP&E and information assets that is not covered by insurance in its financial statements as a footnote disclosure. However, **33 percent** of respondents do not believe disclosure of a material loss to information assets is necessary.

The majority of companies had a material or significantly disruptive security exploit or data breach one or more times in the past 24 months. Fifty percent of respondents report that their company had such a security incident. The average total financial impact of these incidents was $5 million.[80] Sixty-six percent of these respondents say the incident increased their company's concerns over cyber liability.

The number of organizations that believe their cyber insurance is sufficient increased from 53 percent to 58 percent since the last study. However, despite the extent of cyber risk, only 30 percent of respondents say their companies currently have cyber insurance coverage, with an average limit of $16 million. Fifty-eight percent of these respondents believe this insurance is sufficient with respect to coverage terms and conditions, exclusions, retentions, limits and insurance carrier financial security.

Cyber liability and intellectual property risks rank in the top 10 of all business risks facing companies. Eighty-six percent of respondents believe are a serious business risk. **Twenty percent** of respondents say cyber risk is the number one or two business risk. **Thirty-five percent** of respondents rank it among the top five and **31 percent** of respondents rank it among the top 10 business risks. **Eighty-two percent** of respondents rate the risk to their company's intellectual property among the top 10 of all business risks.

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

[76] 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).

[77] While the survey results suggest Probable Maximum Loss at approximately $321 million, a growing number of companies are using Risk Decision Platform Analysis and Cyber Modeling to suggest potential losses in excess of $500 million to over $1 billion and are seeking cyber insurance limit premium quotes and policy terms for such amounts.

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

[79] 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.

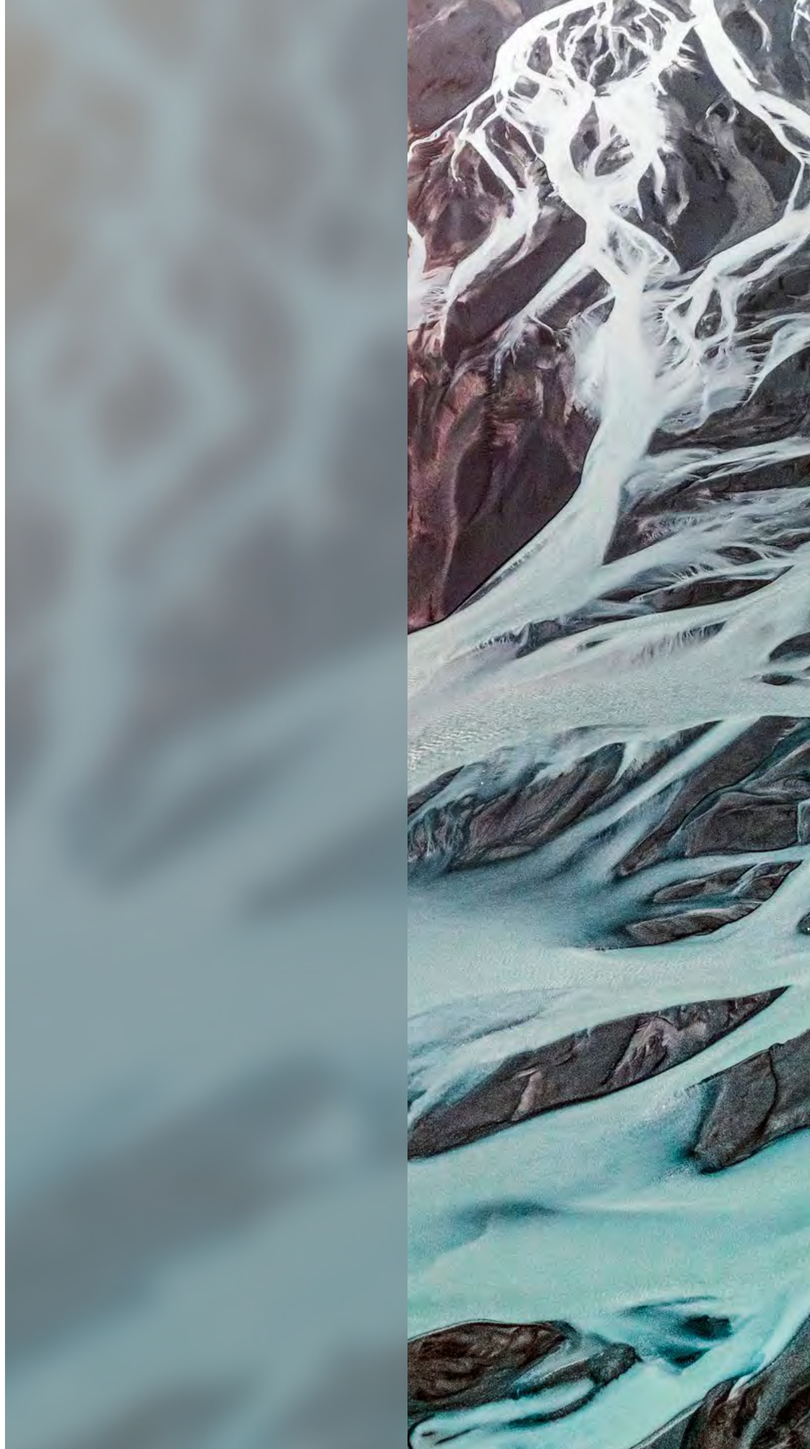
[80] This included all costs, including out-of-pocket expenditures such as consultant and legal fees, indirect business costs such as productivity losses, diminished revenues, legal actions, customer turnover and reputational damages.

In the past two years, 35 percent of respondents say their company experienced a material IP event.[81] Most of these incidents involved trade secret rights (**41 percent** of respondents). Fewer events involved copyright rights (**26 percent** of respondents), and patent rights (**25 percent** of respondents). Companies represented in this research estimate that the average total value of their IP assets such as trademarks, patents, copyrights, trade secrets and know-how is **$597 million**.

Most companies' insurance does not cover all consequences of an IP event. Only **31 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. More than one-third of respondents (34 percent) say the policy does not cover IP events.[82]

As a complement to a cyber risk policy, few companies have a trade secret theft insurance policy and/or an intellectual property liability policy. Only 29 percent of respondents say they have a trade secret theft insurance policy and a similar percentage of respondents (**31 percent**) have an intellectual property liability policy. However, there is significant misunderstanding regarding the scope of intellectual property coverage within such policies.[83] In fact, IP insurance can be purchased to address IP infringement allegations even after litigation has been filed.[84] However, such "burning building" IP policies are very expensive with large retentions — though they could be useful in helping to close an M & A transaction.[85]

Most companies do not include the possibility of a Black Swan event as part of their enterprise risk management approach. Almost half of respondents (48 percent) say an external cyber and intellectual property incident can become a Black Swan for their companies. However, 46 percent of respondents say their risk management approach does not include the impact of a Black Swan event.



[81] "IP event" includes "challenge to company rights," "infringement of company rights," and "allegation of company infringement of third-party rights" pursuant to Question 30c in the Appendix hereto.

[82] 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 percent of organizations have insurance coverage for trade secrets or patents.

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

[84] Cadence, Synopsys settle Avant IP litigation

[85] Id.

2

Key Findings

2 Key Findings

This report features the consolidated findings of all regions in this research. All respondents are generally 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.[86]
The complete audited findings are presented in the appendix of this report. We have organized the report according to the following topics:

- Differences between the valuation and Probable Maximum Loss of Property, Plant & Equipment, and intangible assets
- The cyber risk experience of companies
- Perceptions about the financial impact of cyber exposures
- The risk to intellectual property

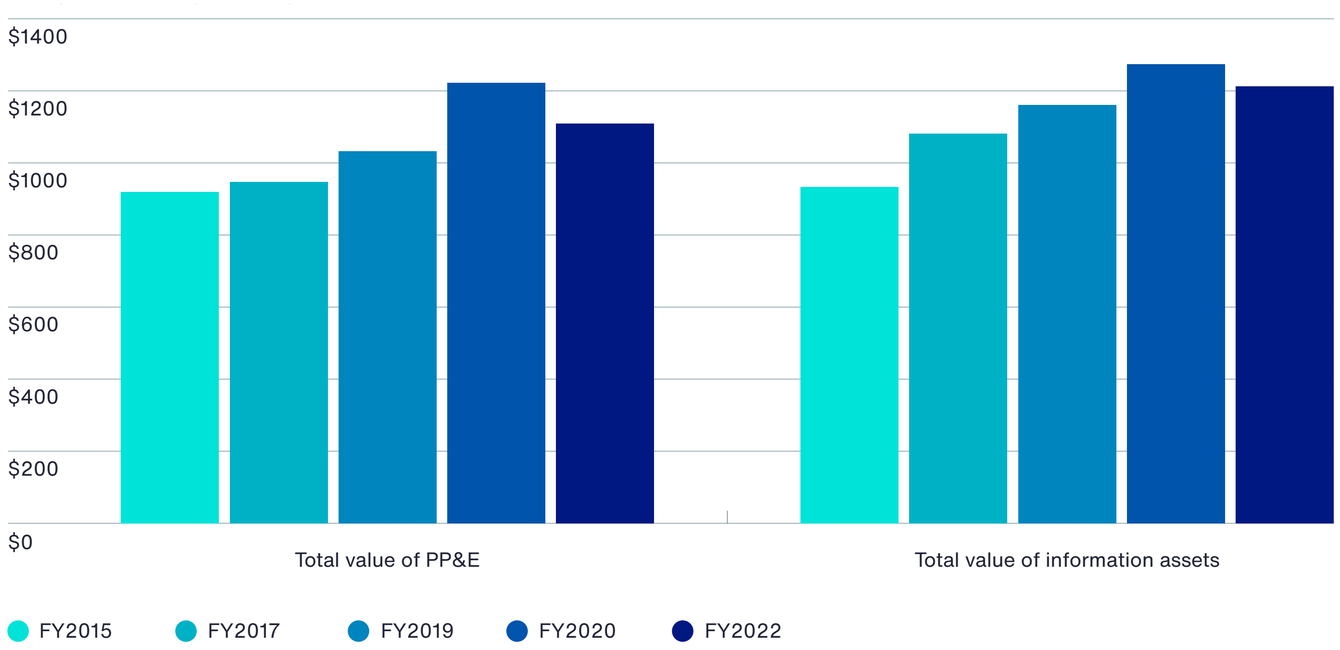
[86] Source: Institute of Risk Management

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

Companies value information assets slightly higher than they do PP&E. According to Figure 2, on average, the total value of PP&E, including all fixed assets plus SCADA and industrial control systems is approximately $1,109 million for the companies represented in this research. The average total value of information assets, which includes customer records, employee records, financial reports, analytical data, source code, models, methods and other intellectual properties, is slightly higher, at $1,213 million.

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

Extrapolated value ($ millions)

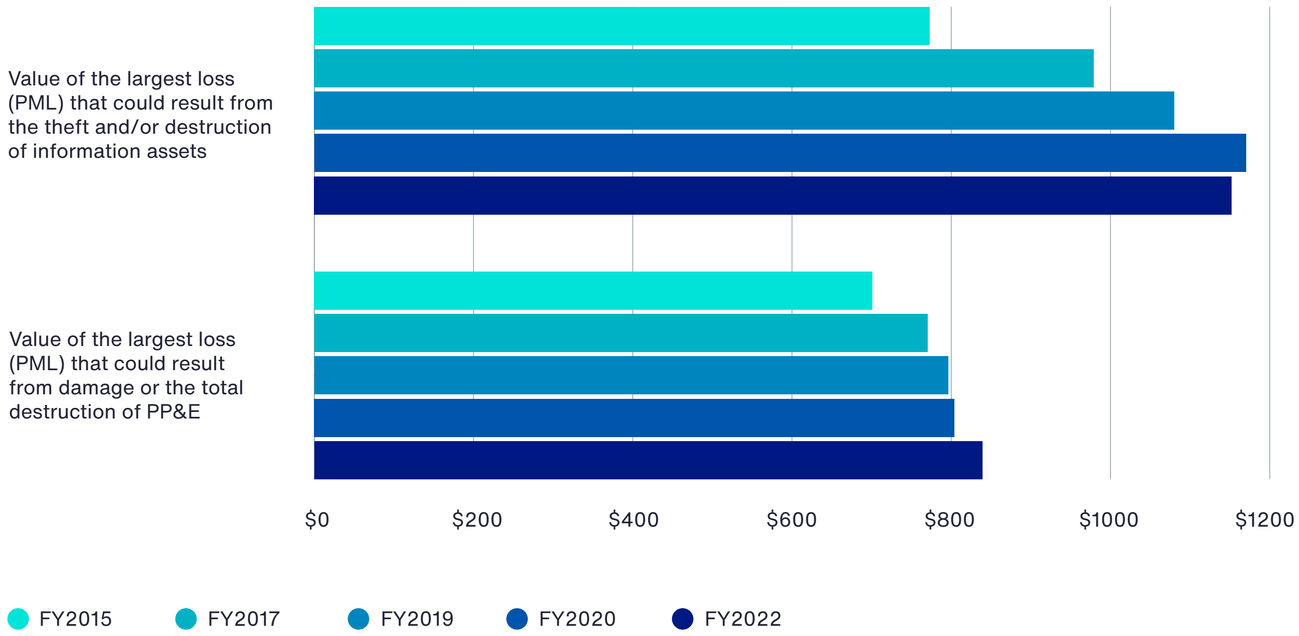


The value of PML is higher for information assets than for PP&E. Companies estimate the average PML resulting from the theft or destruction of information assets at approximately $1,152 million, according to Figure 3. This assumes the normal functioning of passive protective cybersecurity solutions such as perimeter controls, data loss prevention tools, data encryption, identity and access management systems and more.

In contrast, the value of the largest loss that could result from damage or total destruction of PP&E is, on average, approximately $839 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 3. The PML value for PP&E and information assets

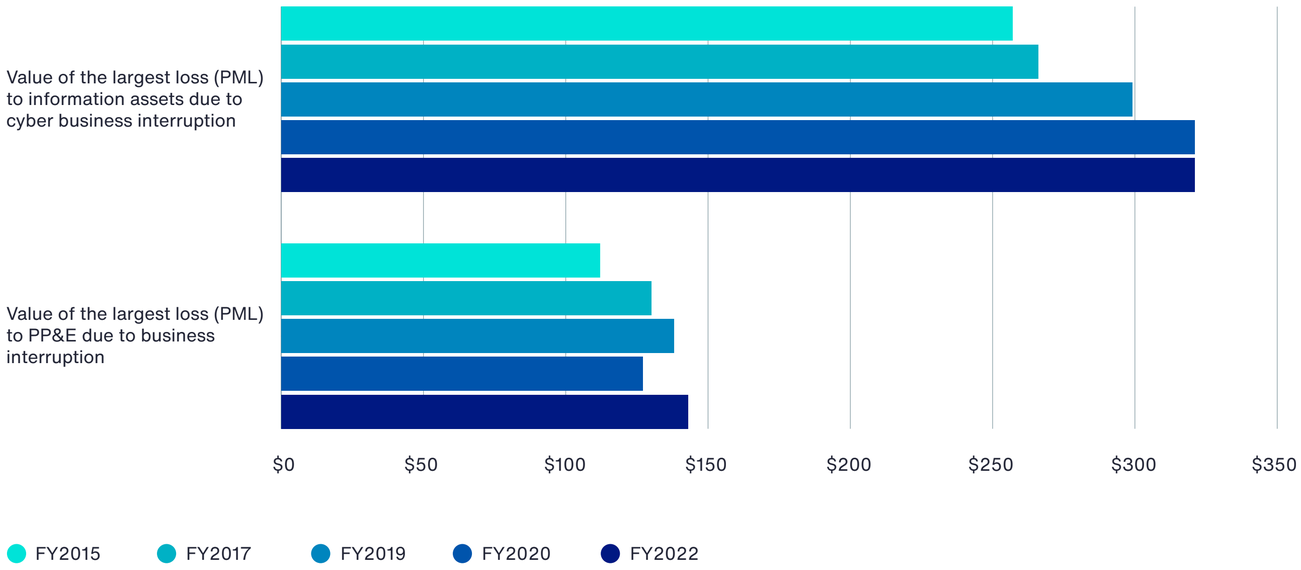
Extrapolated value ($ millions)



The impact of business disruption to information asset losses is more significant than the impact to PP&E. According to Figure 4, business disruption has a greater impact on intangible assets ($321 million)[87] than on PP&E ($143 million).

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

Extrapolated value ($ millions)

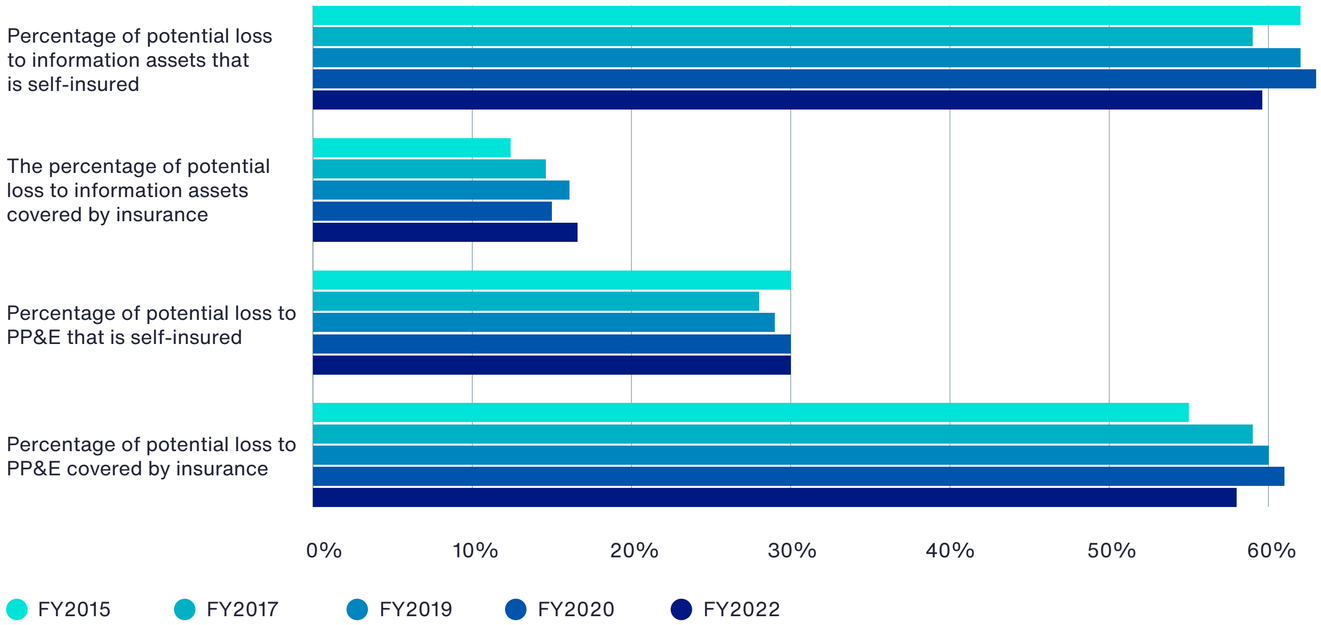


[87] While the survey results suggest Probably Maximum Loss in the neighborhood of $321 million, a growing number of companies are using Risk Decision Platform Analysis and Cyber Modeling to suggest potential losses in excess of $500 million to over $1 billion and seek cyber insurance limit premium quotes and policy terms for such amounts.

There is a significant difference between the insurance coverage of PP&E and information assets. On average, approximately 58 percent of PP&E assets are covered by insurance and approximately 30 percent of PP&E assets are self-insured (Figure 5). Only an average of 17 percent of information assets are covered by insurance. Self-insurance is higher for information assets at 60 percent.

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

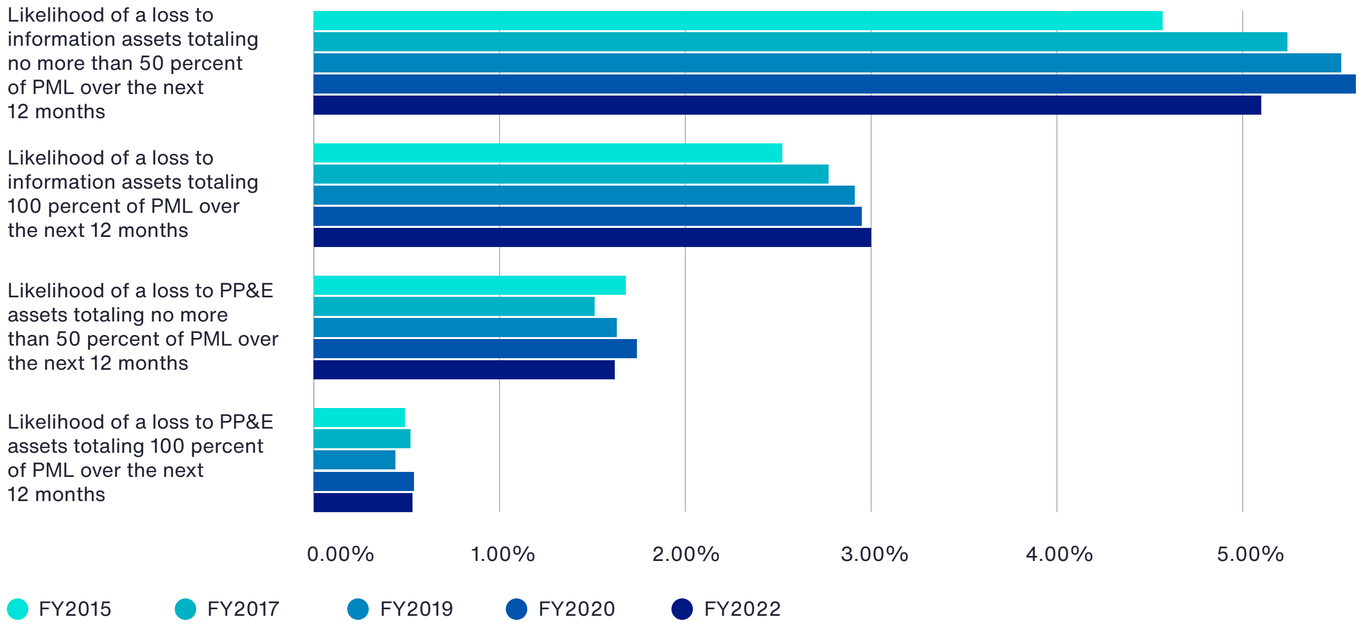
Extrapolated percentage



The likelihood of a loss is higher for information assets than for PP&E. Companies estimate the likelihood that they will sustain a loss relating to information assets totaling no more than 50 percent of PML over the next 12 months at 5.1 percent and 100 percent of PML at 3 percent, as shown in Figure 6. 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 1.62 percent and at 100 percent of PML it is 0.53 percent.

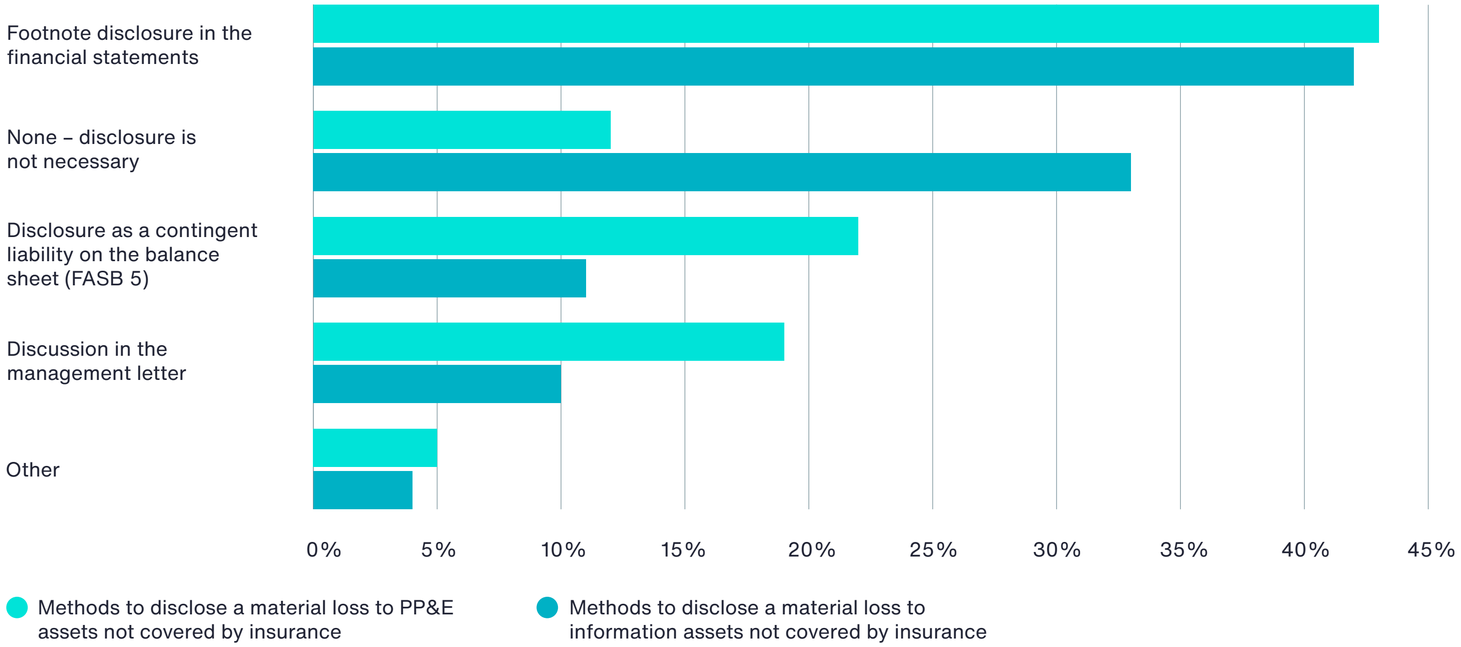
Figure 6. Likelihood of loss to PP&E and information assets totaling more than 50 percent and 100 percent of PML over the next 12 months

Extrapolated percentage



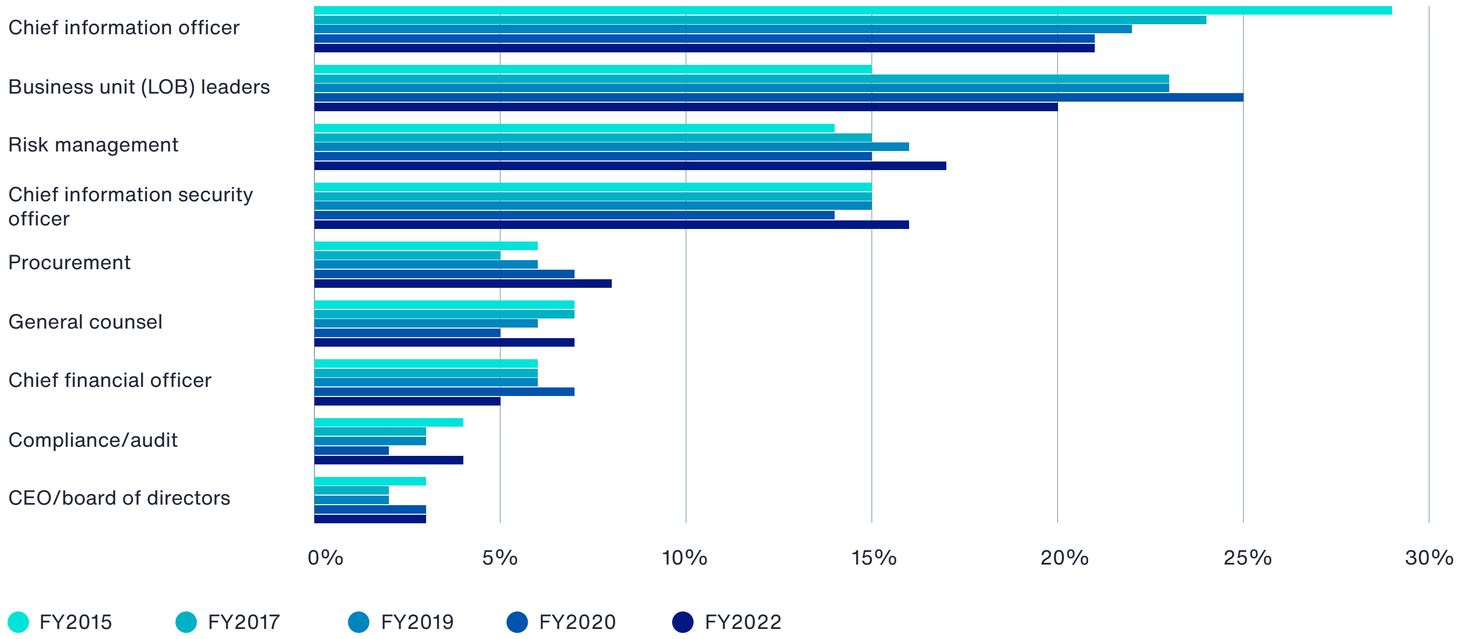
Thirty-three percent of respondents believe no disclosure of a material loss to information assets is required. Figure 7 focuses on how companies would disclose a material loss. Forty-two percent of respondents say their company would disclose a material loss to PP&E assets that is not covered by insurance in the footnotes of its financial statements, followed by a disclosure as a discussion in the management letter (33 percent of respondents).

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



Responsibility for cyber risk management is dispersed throughout the organization. As shown in Figure 8, no one function is clearly responsible for managing cyber risks in their organizations.[88] The top two are the chief information officer (21 percent of respondents) and business unit leaders (20 percent of respondents).[89]

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

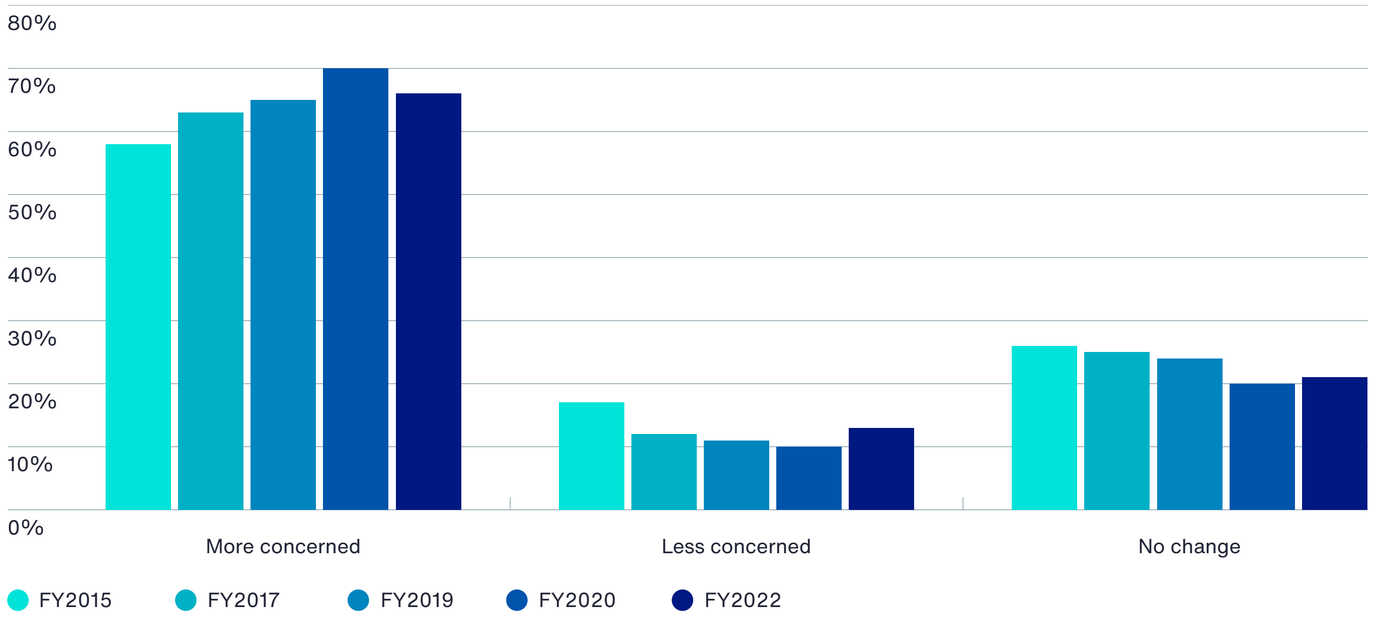


[88] ***"Treating Cyber Risks – Using Insurance and Finance."*** Chapter 10 of John Wiley and Sons Book: ***The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities.***

[89] Is Cyber Risk a D & O Risk? Ethical Boardroom.

The majority of companies had a material or significantly disruptive security exploit or data breach one or more times in the past 24 months. Fifty percent of respondents report that their company had such a security incident. The average total financial impact of these incidents was $5 million. According to Figure 9, 66 percent of these respondents say the incident increased their company's concerns over cyber liability.[90]

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

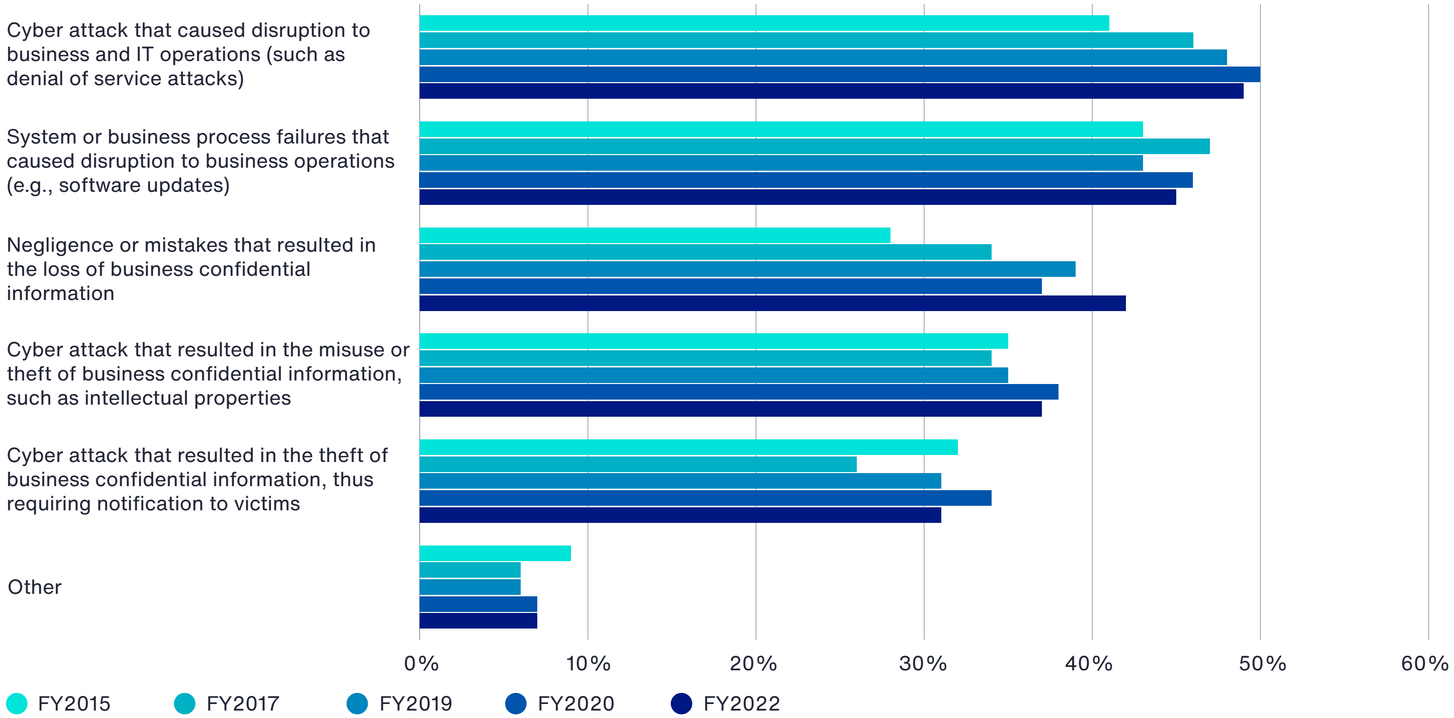


[90] How Cyber Criminals Are Taking Advantage Of COVID-19

The types of security incidents that 50 percent of the companies in this research had are listed in Figure 10. The most frequent type of incident was one that caused disruption to business and IT operations (49 percent of respondents) or resulted in a system or business process failure that caused disruption to business operations (45 percent of respondents). This is followed by 42 percent of respondents who say the cyber attack resulted in negligence or mistakes that resulted in the loss of business information.

Figure 10. What type of data breach or security exploit did your company experience?

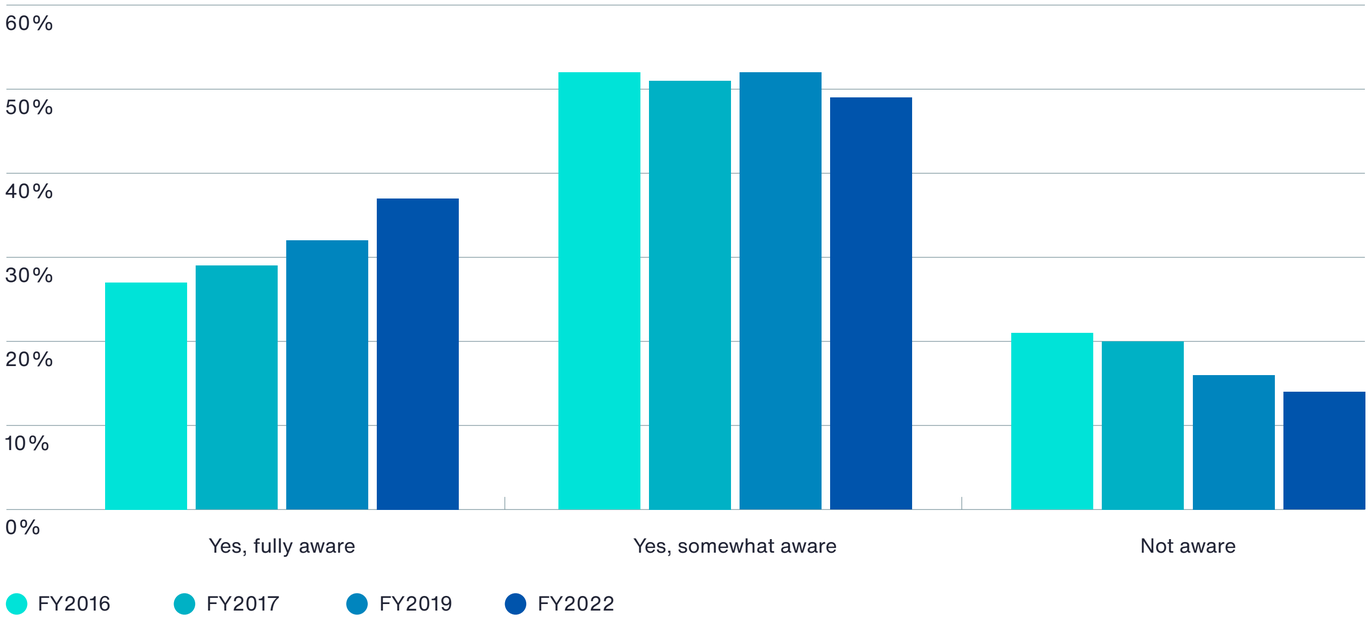
More than one response permitted



Perceptions about the financial impact of cyber exposures

Organizations are aware of the economic and legal consequences from an international data breach or security exploit. As revealed in Figure 11, 86 percent of respondents are either fully (37 percent) or somewhat (49 percent) aware of the consequences that could result from a data breach or security exploit in other countries where their company operates. Only 14 percent of respondents say they are not aware of the consequences.[91]

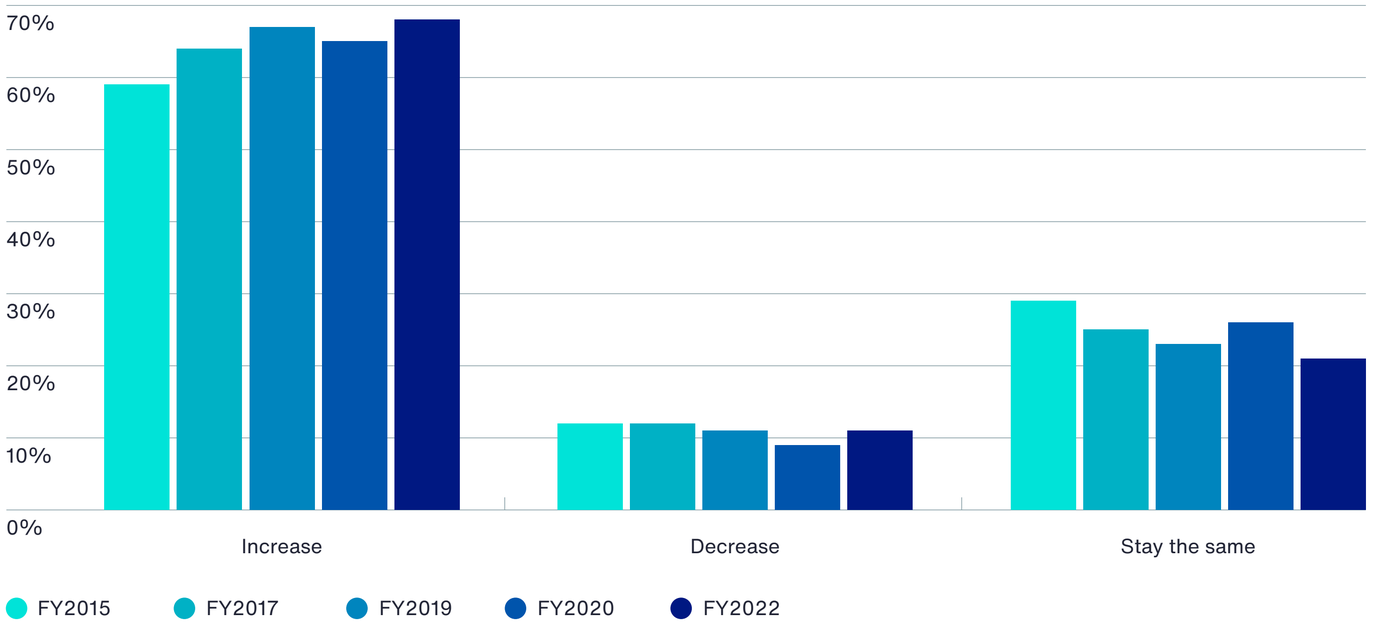
Figure 11. Awareness of the economic and legal consequences from an international data breach or security exploit



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

Companies' exposure to cyber risk is not decreasing. While organizations are predicting that their cyber risk exposure will increase, 37 percent of respondents say there is no plan to purchase standalone cyber insurance. As the data in Figure 13 show, 68 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 11 percent of respondents expect it to actually decrease.

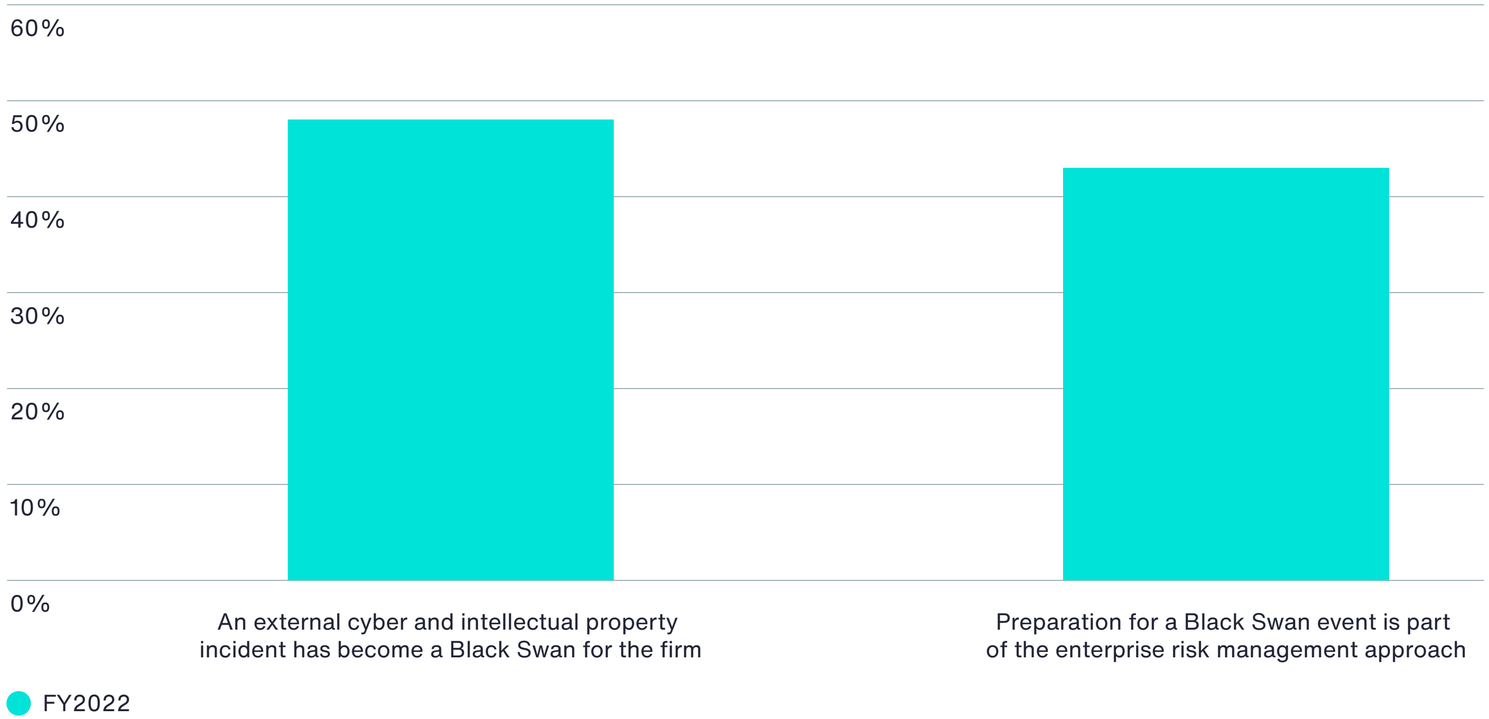
Figure 12. Will your company's cyber risk exposure increase, decrease or stay the same over the next 24 months?



Companies are not prepared for a Black Swan event. While 48 percent of respondents say an external cyber and intellectual property incident can become a Black Swan for their companies, only 43 percent of respondents say preparation for a Black Swan event is part of their enterprise risk management approach.

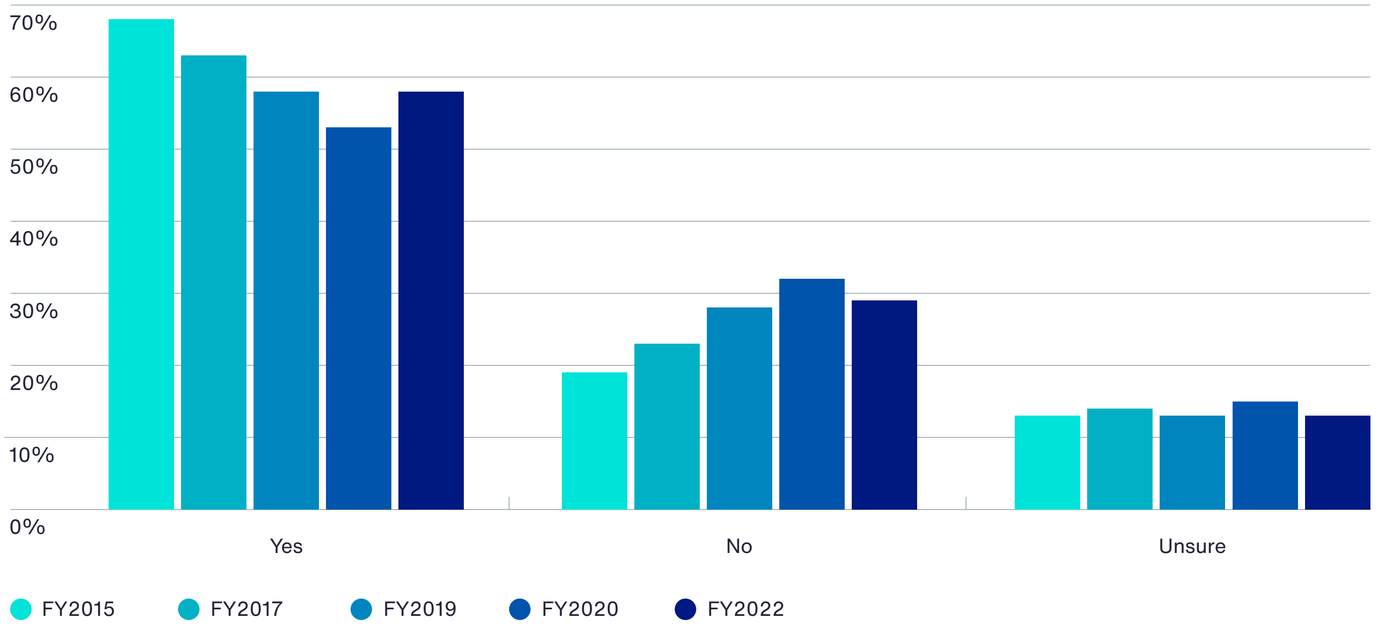
Figure 13. Are companies prepared for a Black Swan event?

Yes responses only



Organizations that believe their cyber insurance is sufficient has increased. As Figure 14 reveals, 58 percent of these respondents believe this insurance is sufficient with respect to coverage terms and conditions, exclusions, retentions, limits and insurance carrier financial security, an increase from 53 percent of respondents.[92] However despite the extent of cyber risk, which exceeds that of PP&E risk, only 30 percent of respondents say their companies currently have cyber insurance coverage with an average limit of $16 million.

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

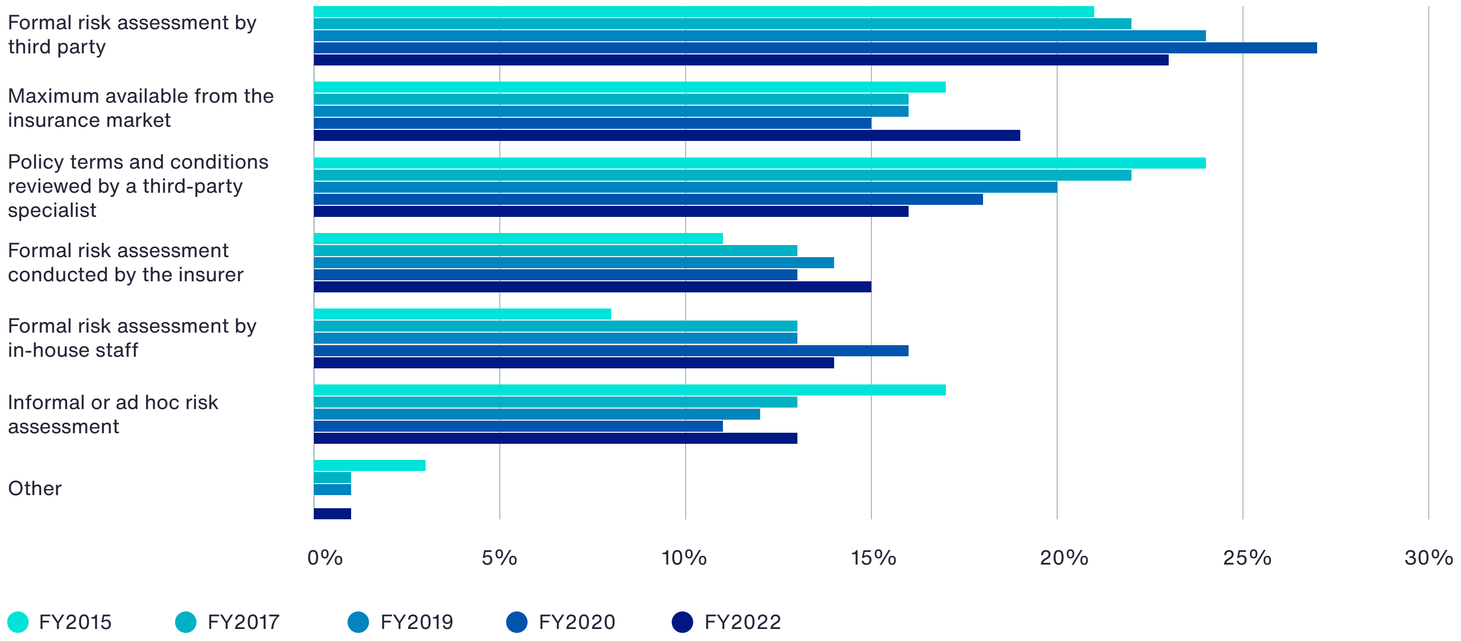


[92] ***The Future of Insurance to Address Cyber Perils.*** Insurance Thought Leadership.

According to Figure 15, the adequacy of coverage is determined mainly by a formal risk assessment by a third party (23 percent of respondents), maximum value from the insurance market (19 percent of respondents) and policy terms and conditions reviewed by a third-party specialist (16 percent of respondents).

Understanding the context of each organization's industry, size, geography, cyber resiliency and risk management appetite is critical. For instance, the IBM/ Ponemon industry leading "Cost of a Data Breach" 2021 study[93] is useful for small and medium enterprises, but each specific cyber exposure's circumstance should be modeled actuarially by situation, and adjusted accordingly.

Figure 15. How companies determine the adequacy of coverage

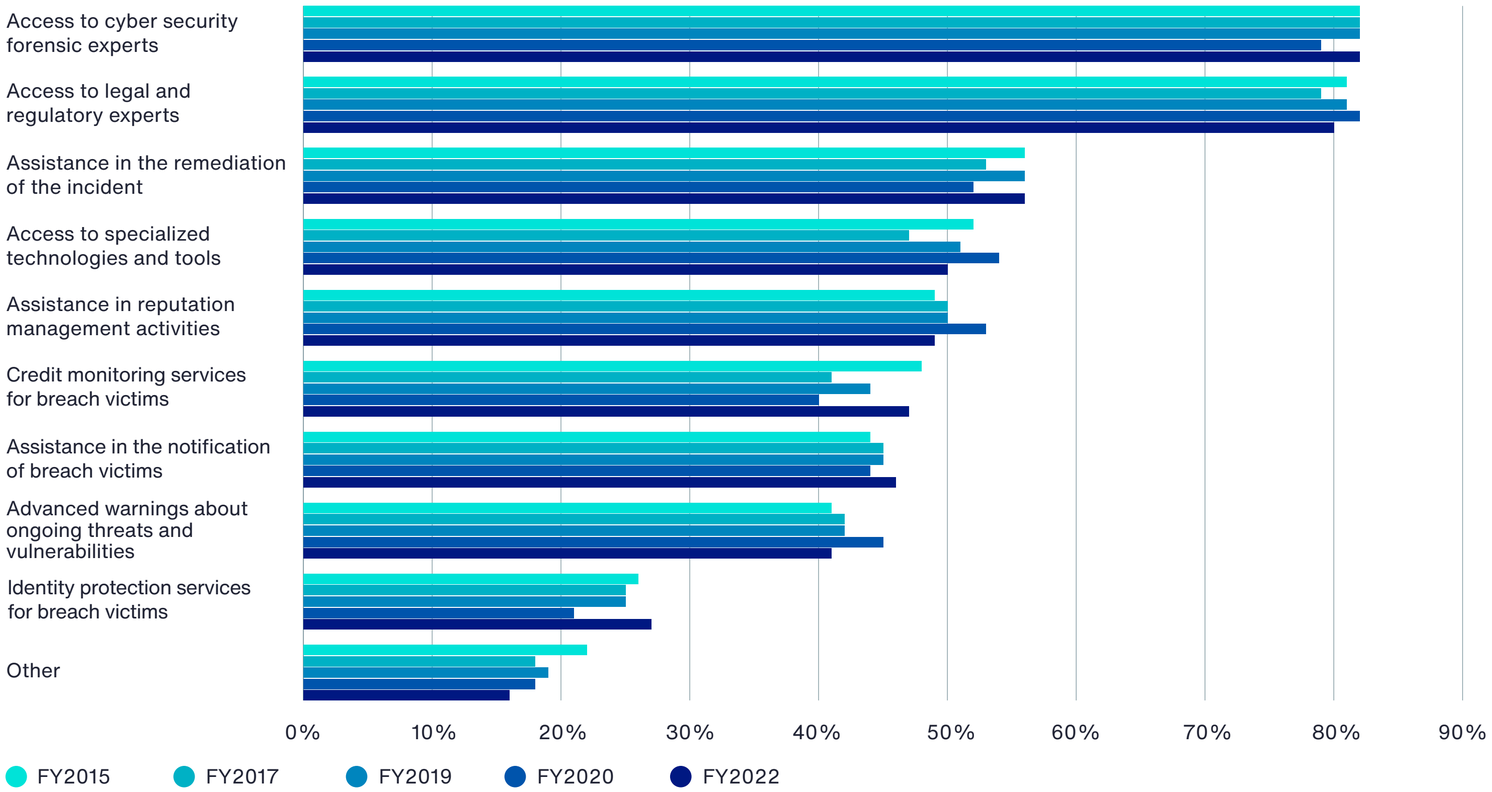


[93] Cost of a Data Breach Report 2021

According to Figure 16, the primary services provided by the insurer are access to cyber security forensic experts and legal and regulatory experts (82 percent and 80 percent of respondents, respectively). This is followed by assistance in the remediation of the incident (56 percent of respondents) and access to specialized technologies and tools (50 percent of respondents).

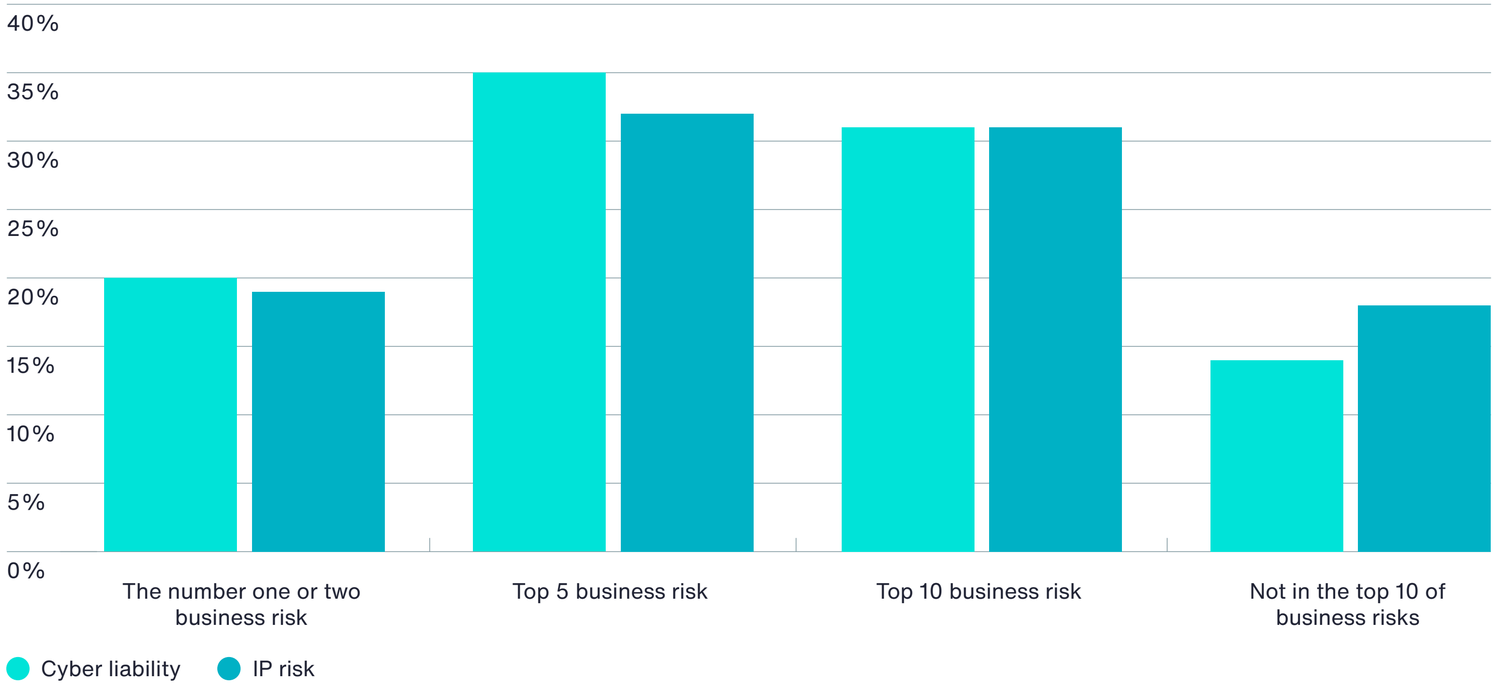
Figure 16. Other services provided by the cyber insurer

More than one response permitted



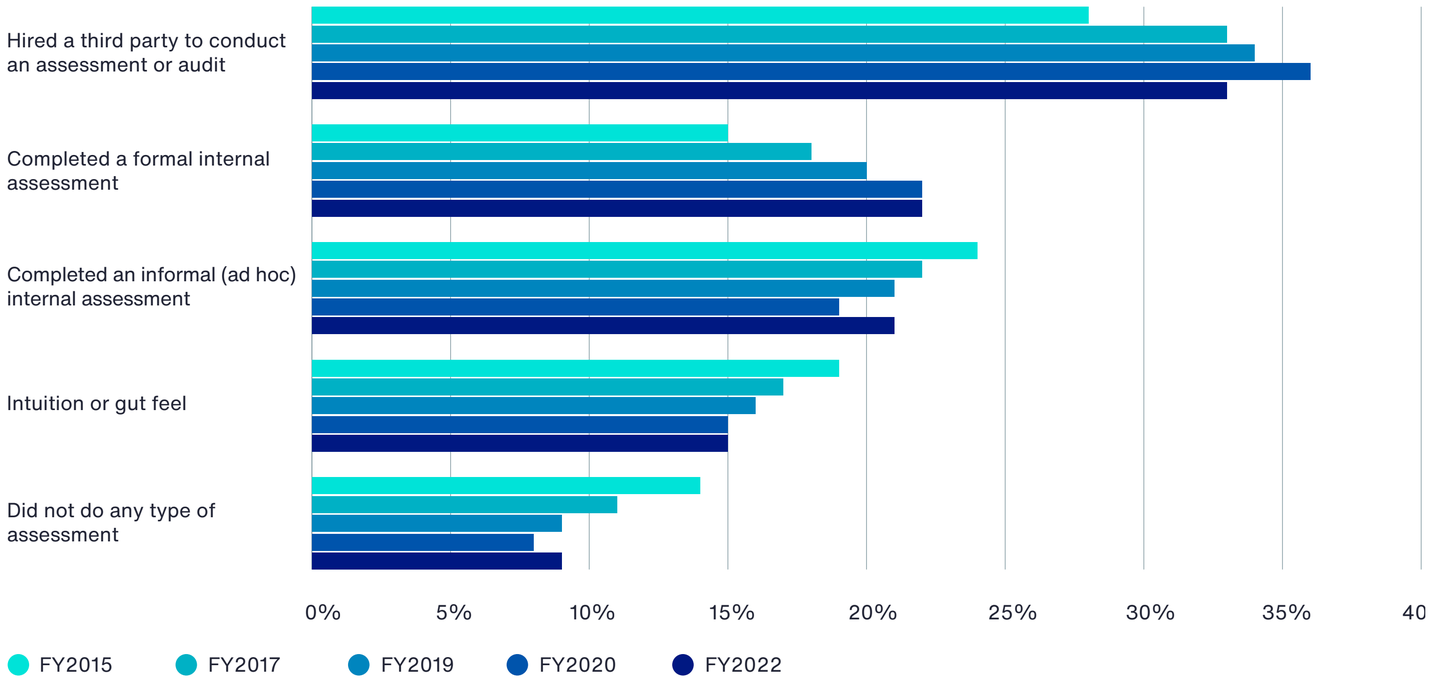
Cyber liability and IP risks rank in the top 10 of all business risks facing companies. According to Figure 17, 86 percent of respondents consider cyber risk as the number one or two business risk (20 percent of respondents), among the top five (35 percent of respondents) and among the top 10 business risks (31 percent of respondents). Similarly, 82 percent of respondents rate the risk to their company's IP among the top 10 of all business risks.

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



To assess cyber risk, third party and formal internal assessments are conducted. To determine the cyber risk to their company, 33 percent of respondents say the company hired a third party to conduct an assessment or audit and 22 percent of respondents say their organization completed a formal internal assessment. Twenty-one percent of respondents say their organizations did an informal (ad hoc) internal assessment (Figure 18). Only 15 percent of respondents say it was based on intuition or gut feel.

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



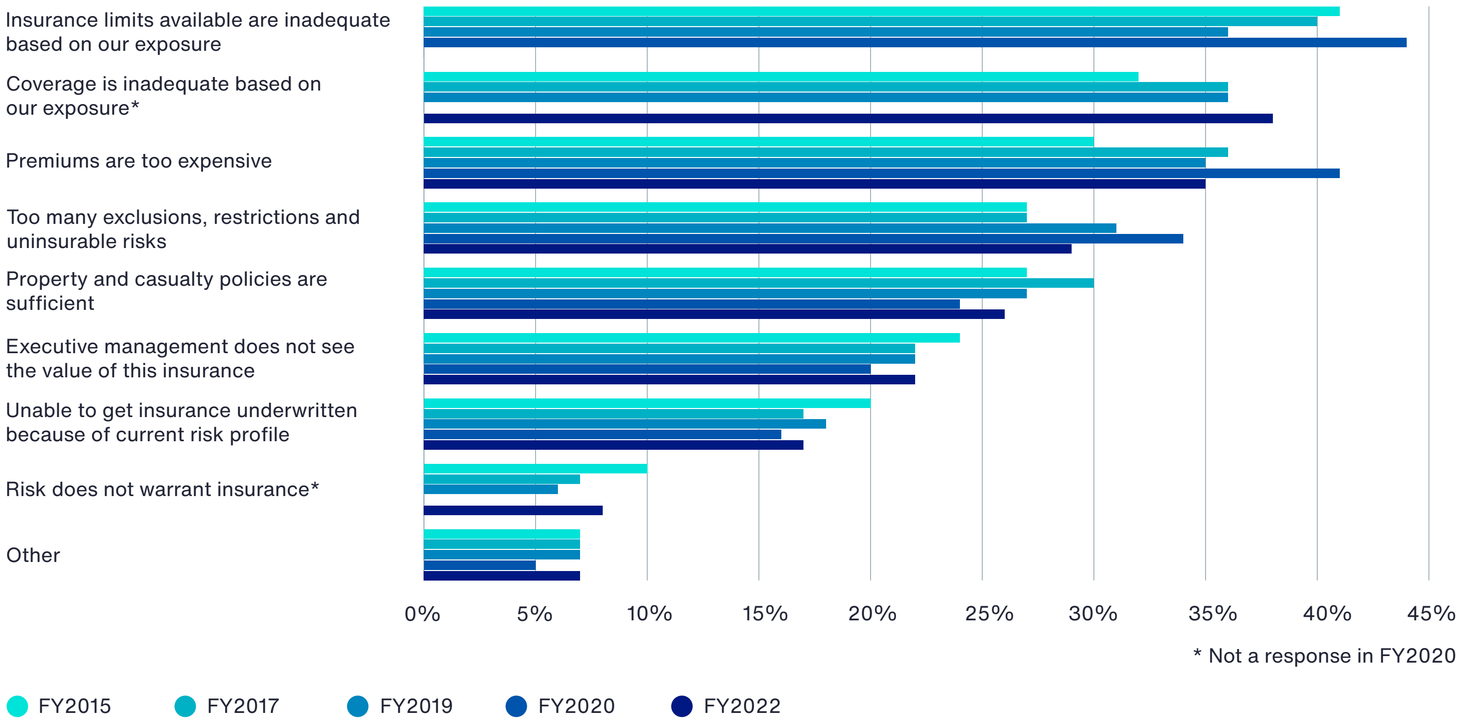
Most companies are postponing the purchase of a standalone cyber insurance. Of the 70 percent of companies that do not have cyber insurance, 37 percent of respondents say their company has no plans to purchase a standalone cyber insurance. Only 16 of respondents say their company will purchase cyber insurance in the next 12 months. Almost half of respondents (47 percent) say they will purchase cyber insurance in the next 24 months (26 percent) or more than 24 months (21 percent).

According to Figure 19, the main reasons for not purchasing a standalone cyber security insurance are: coverage is inadequate based on their exposure (38 percent of respondents), premiums are too expensive (35 percent of respondents) and there are too many exclusions, restrictions and uninsurable risks (29 percent of respondents).

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.

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

More than one response permitted



Risks to Intellectual Property (IP)[94]

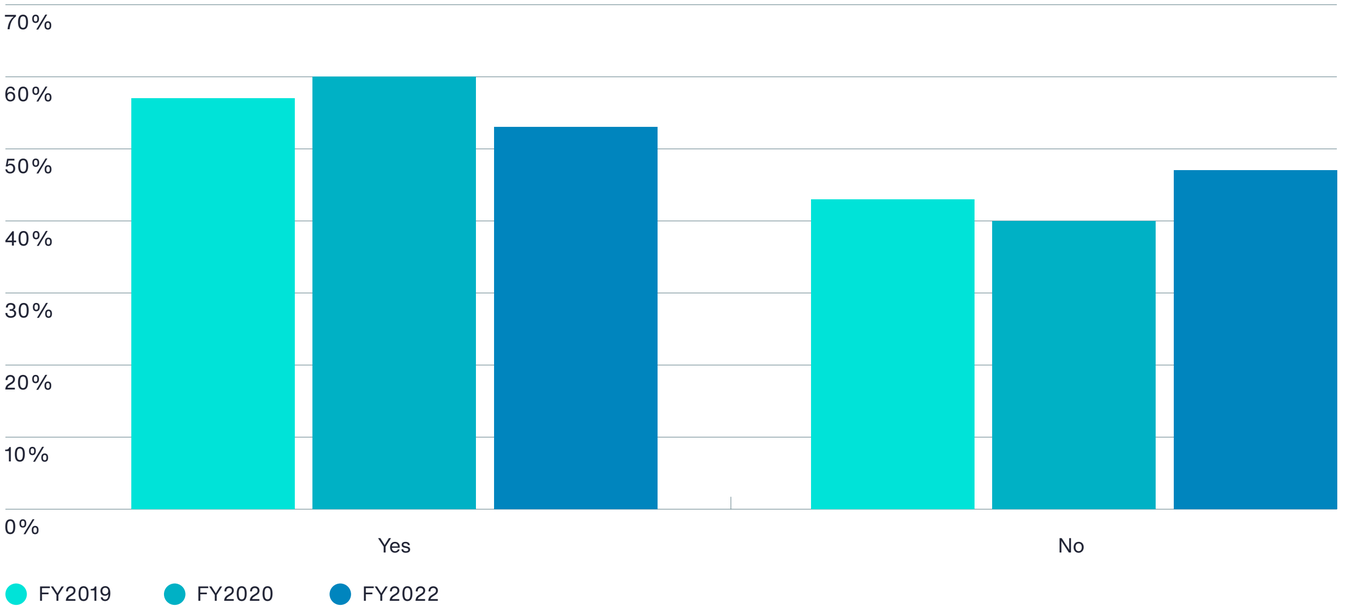
Intellectual Property Insurance: Scope and Gaps

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	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	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

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

The percentage of respondents that say their organizations have a strategy to manage risks to IP declines. Companies represented in this research estimate that the average total value of their IP assets such as trademarks, patents, copyrights, trade secrets and know-how is $597 million. As shown in Figure 20, 53 percent of respondents say their enterprise risk management activities include risks to their IP.[95]

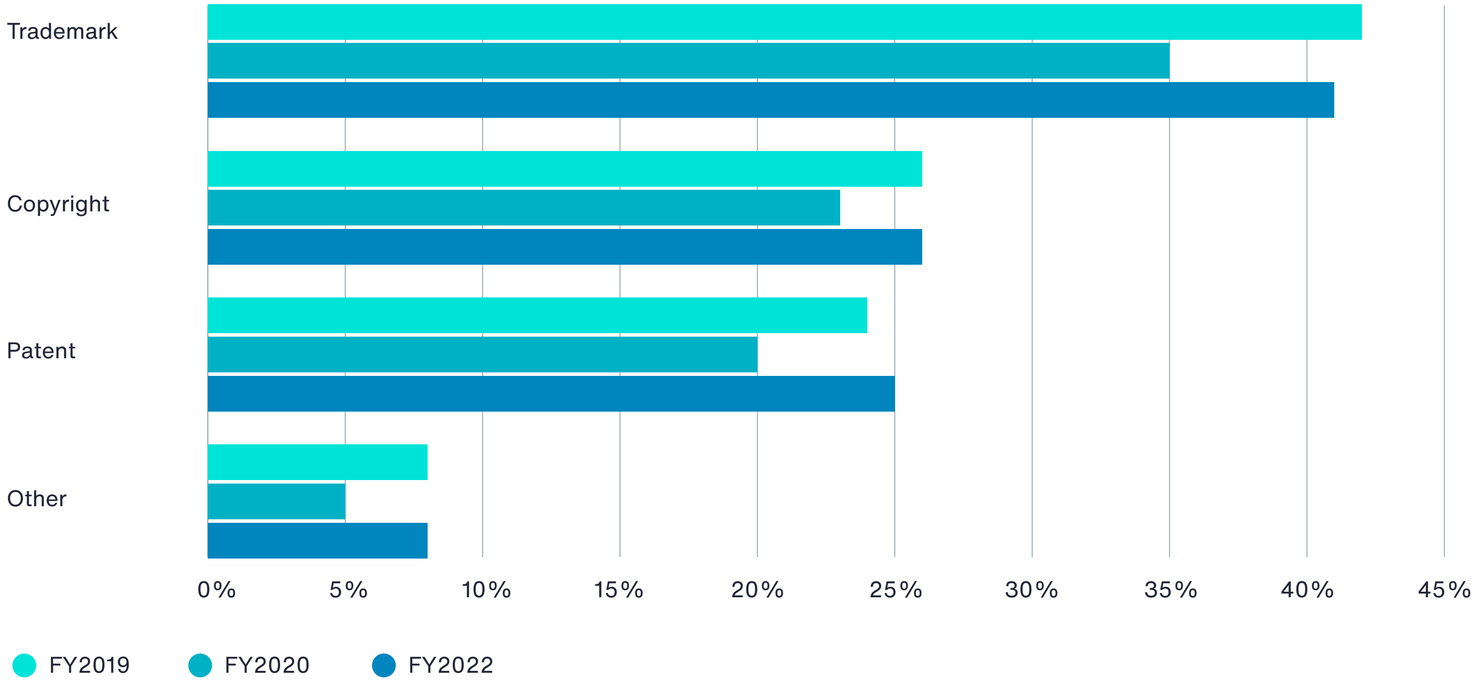
Figure 20. Do your company's enterprise risk management activities include risks to IP?



[95] ***It's All About the Intangibles: Intellectual Property Risk Management***. Professional Liability Underwriters Society Annual Conference. November 12, 2019. Washington, D.C.

In the past two years, 35 percent of respondents say their company experienced a material IP event. According to Figure 21, most of these incidents involved trade secrets (41 percent of respondents). Fewer events involved copyrights, patents and trademarks, service mark or trade dress (26 percent and 25 percent of respondents, respectively).

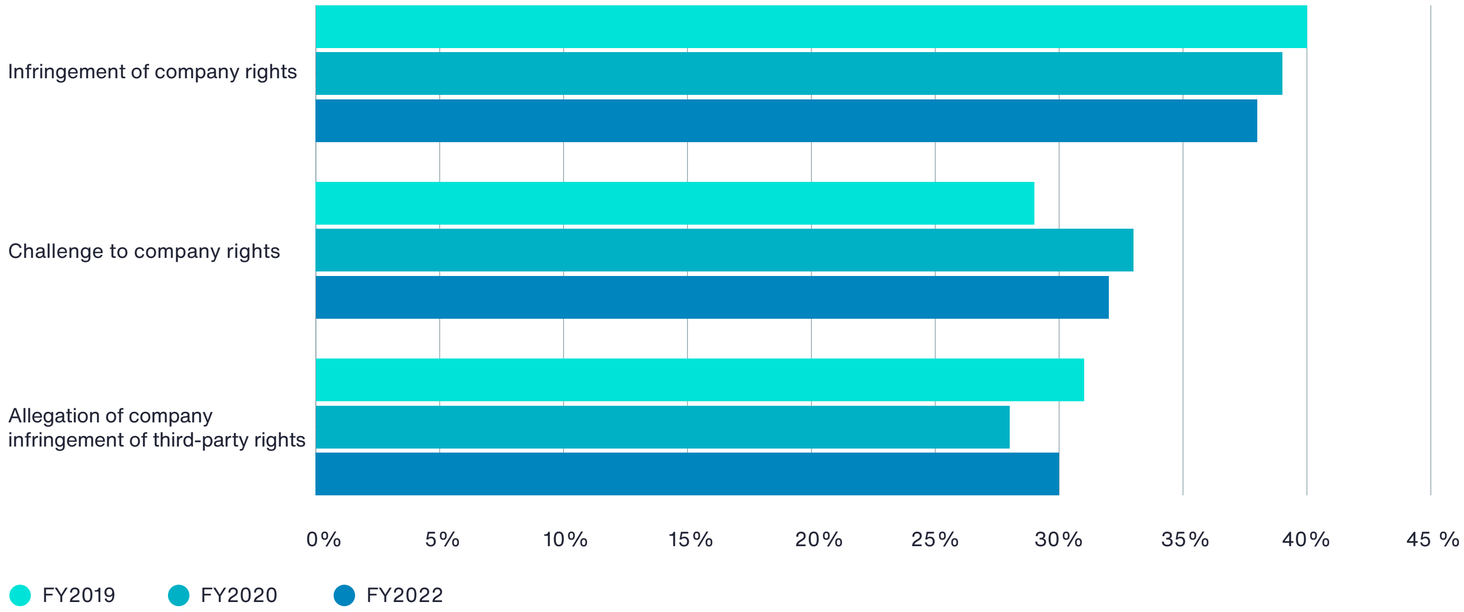
Figure 21. What type of IP assets were involved in a material IP event?



According to Figure 22, the event can be described as an infringement of company rights (38 percent of respondents), challenge to company rights (32 percent of respondents) or an allegation of company infringement of third-party rights (30 percent of respondents).

Figure 22. What best describes the IP material event?

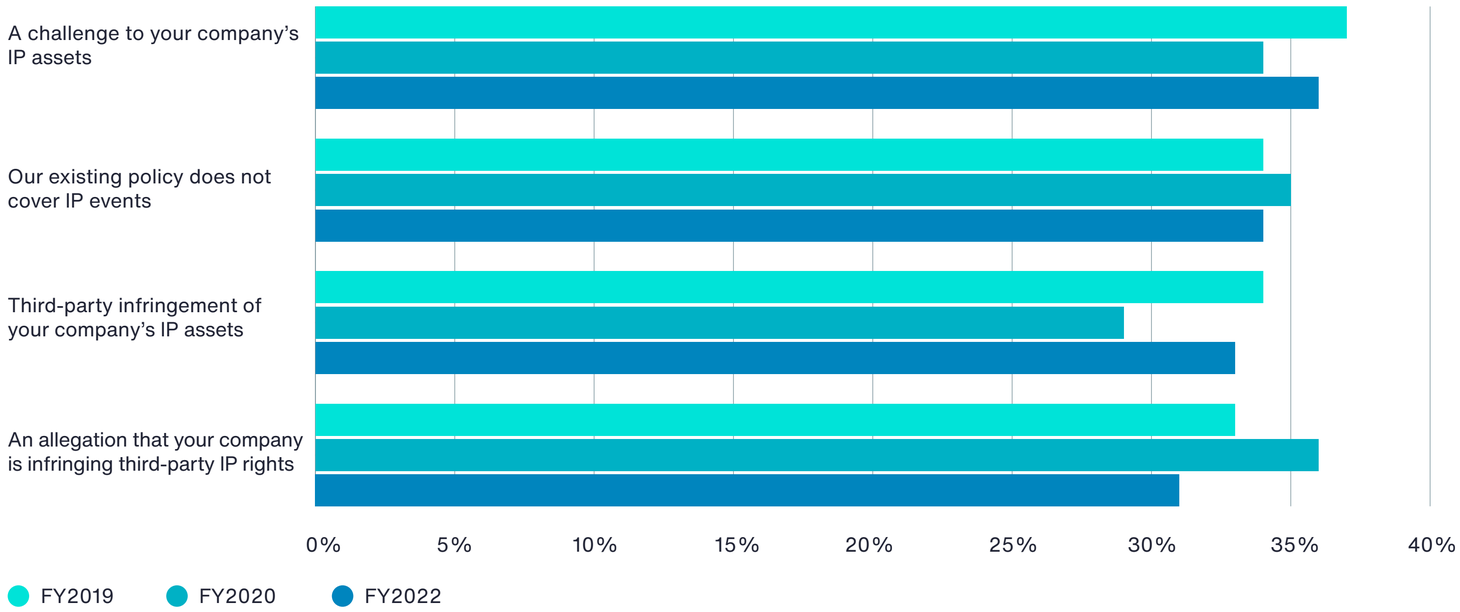
Only one response permitted



According to Figure 23, 66 percent of respondents say their organizations' existing insurance policy (e.g. property, general liability or crime) covers an IP event. Of these respondents, 36 percent of respondents say their companies' 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.[96]

Figure 23. Does your company's existing insurance policy cover any of the following IP events?

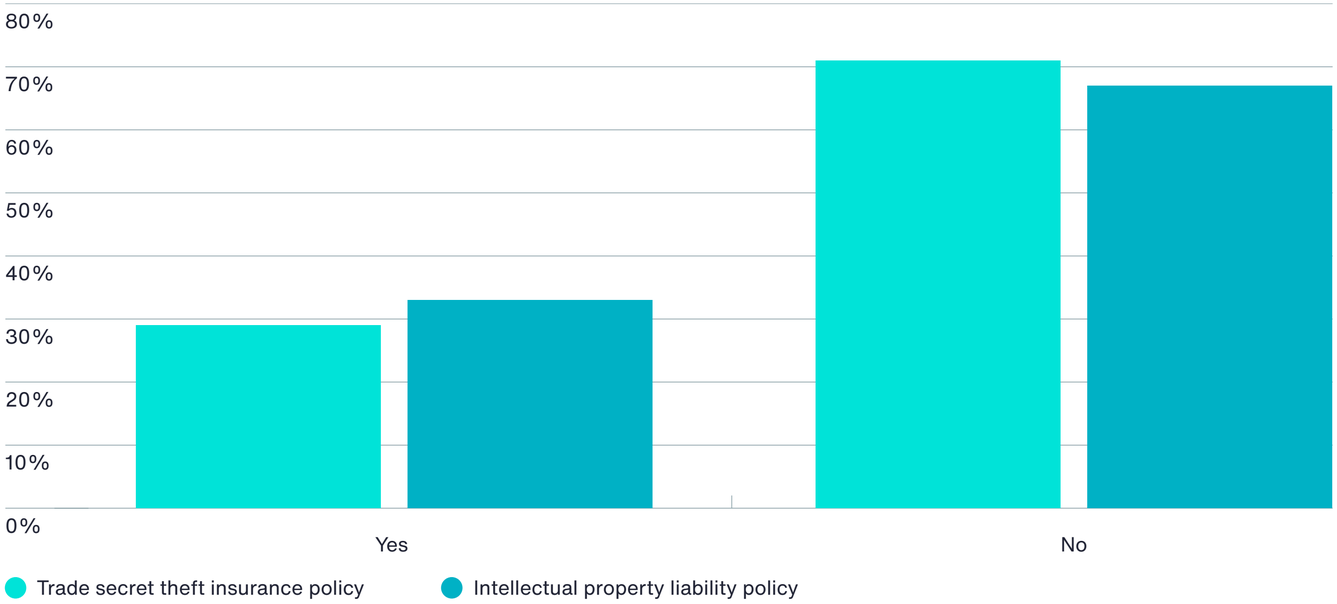
More than one response permitted



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

Few companies have a trade secret theft insurance policy and/or an intellectual property liability policy. As shown in Figure 24, only 29 percent of respondents say they have a trade secret theft insurance policy and a similar percentage of respondents (33 percent) have an intellectual property liability policy.[97]

Figure 24. Does your company have a trade secret and/or IP liability policy?

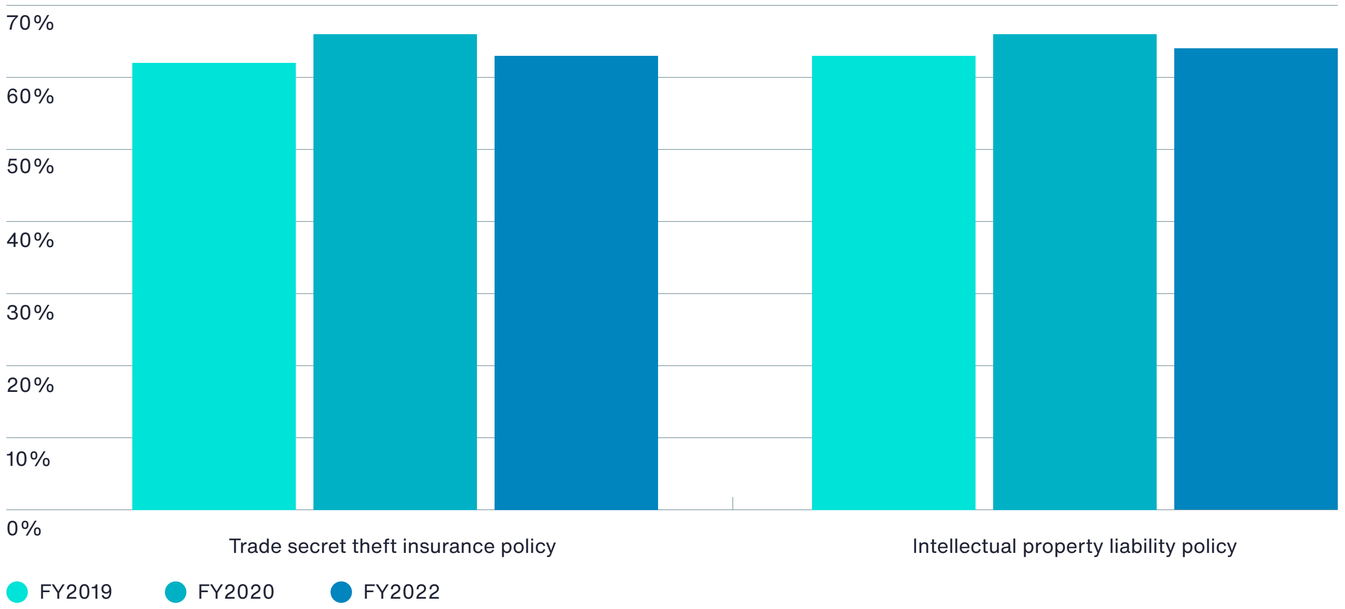


[97] A detailed review of insurance policies indicates that IP coverage is included in existing policies at a much lower rate than survey responses reflect – especially for patent infringement and trade secrets theft, which detailed reviews show less than 5% of organizations have insurance coverage for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

While most companies do not have specific IP insurance policies, there is significant interest in purchasing them. According to Figure 25, 63 percent of respondents are very interested or interested in purchasing a trade secret insurance policy and 64 percent say their organizations would purchase an intellectual property liability policy.

Figure 25. 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



3

Methods

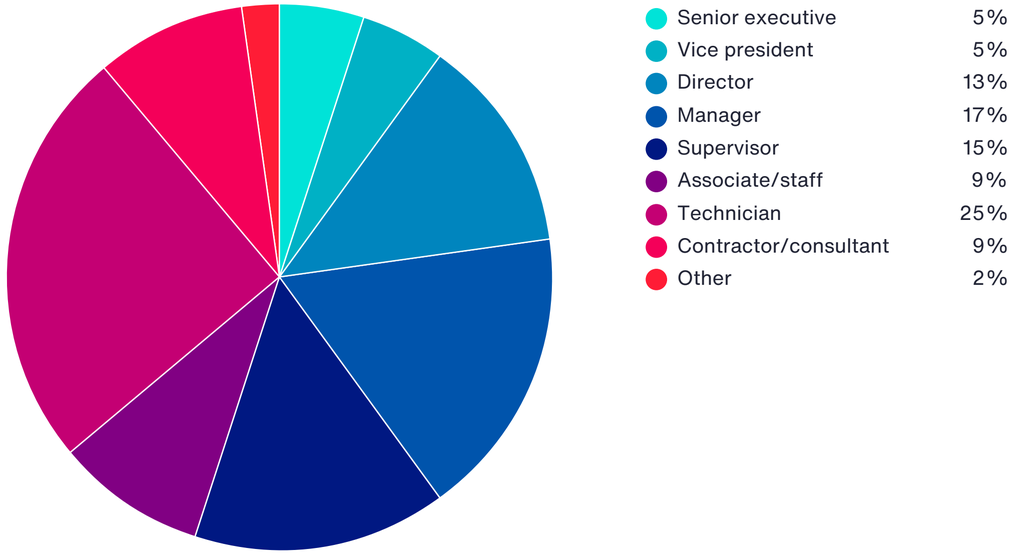
3 Methods

The consolidated sampling frame is composed of 61,073 individuals located in North America, Europe, the Middle East, Africa, Asia Pacific, Japan and Latin America. Respondents are involved in their company's cyber risk 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	61,073	100.0%
Total returns	2,671	4.4%
Rejected or screened surveys	290	0.5%
Final sample	2,381	3.9%

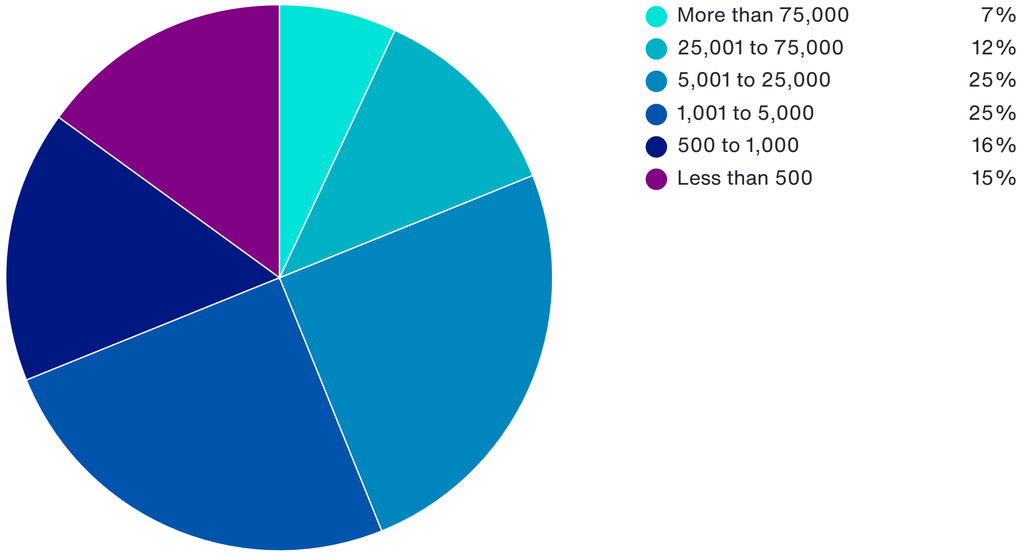
Pie Chart 1 reports the current position or organizational level of the respondents. More than half (55 percent) of the respondents reported their current position as supervisory level or above and 25 percent of respondents reported their current position level as technician.

Pie Chart 1. Current position or organizational level



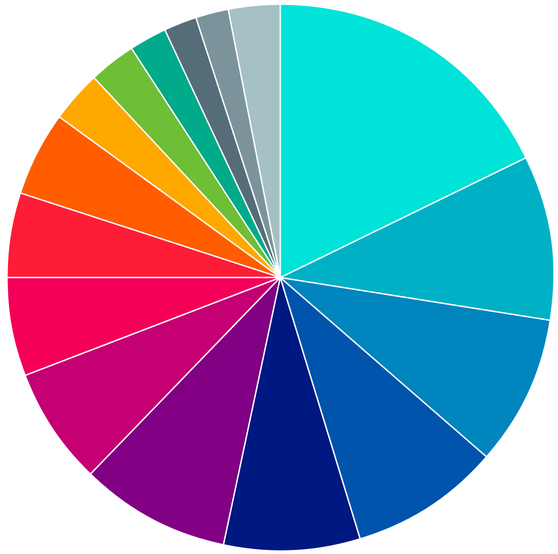
As Pie Chart 2 reveals, 69 percent of the respondents are from organizations with a global headcount of more than 1,000 employees.

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 industrial (11 percent of respondents), services (10 percent of respondents), retailing (9 percent of respondents), health and pharmaceuticals, technology and software, and public sector (each at 8 percent of respondents).[98]

Pie Chart 3. Primary industry focus



Financial services	18%
Retailing	10%
Public sector	9%
Services	9%
Industrial	8%
Technology & software	8%
Health & pharmaceuticals	7%
Manufacturing	6%
Consumer products	5%
Education & research	5%
Communications	3%
Energy & utilities	3%
Entertainment & media	2%
Hospitality	2%
Transportation	2%
Other	3%

[98] ***Cyber Insurance For Law Firms and Legal Organizations.*** Chapter 15 of The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals, Third Edition (americanbar.org) 2022

4

Caveats

4 Caveats

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

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

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

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

5

Appendix: Detailed Survey Results

5 Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in December 2021.

Survey response	FY2022
Sampling frame*	61,073
Total returns	2,671
Rejected surveys	290
Final sample	2,381
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?	FY2022
Very familiar	24%
Familiar	35%
Somewhat familiar	41%
Not familiar (stop)	0%
Total	100%

S2. Are you involved in your company's cyber risk management activities?	FY2022
Yes, significant involvement	35%
Yes, some involvement	65%
No involvement (stop)	0%
Total	100%

S3. What best defines your role?	FY2022
Risk management	26%
Finance, treasury & accounting	31%
Corporate compliance/audit	15%
Security/information security	12%
General management	9%
Legal (OGC)	7%
None of the above (stop)	0%
Total	100%

S4. Are you involved in your company's enterprise risk management activities?	FY2022
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).	FY2022
Less than $1 million	4%
$1 to 10 million	9%
$11 to 50 million	15%
$51 to 100 million	24%
$101 to 500 million	23%
$501 to 1 billion	13%
$1 to 10 billion	7%
More than $10 billion	5%
Total	100%
Extrapolated value (US$ millions)	$1,108.68

Q2a. What is the value of the largest loss (PML) that could result from damage or the total destruction of PP&E. Please assume the normal functioning of passive protective features – such as firewalls, nonflammable materials, proper functioning of active suppression systems, fire sprinklers, raised flooring and more.	FY2022
Less than $1 million	6%
$1 to 10 million	11%
$11 to 50 million	16%
$51 to 100 million	24%
$101 to 500 million	24%
$501 to 1 billion	10%
$1 to 10 billion	7%
More than $10 billion	3%
Total	100%
Extrapolated value (US$ millions)	$838.80

[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.	FY2022
Less than $1 million	13%
$1 to 10 million	24%
$11 to 50 million	27%
$51 to 100 million	19%
$101 to 500 million	13%
$501 to 1 billion	4%
$1 to 10 billion	1%
More than $10 billion	0%
Total	100%
Extrapolated value (US$ millions)	$142.65

Q3. What percentage of this potential loss to PP&E assets is covered by insurance, including captives reinsured but not including captives not reinsured?	FY2022
Less than 5%	0%
5% to 10%	3%
11%to 20%	5%
21% to 30%	7%
31% to 40%	8%
41% to 50%	11%
51% to 60%	17%
61% to 70%	14%
71% to 80%	14%
81% to 90%	11%
91% to 100%	10%
Total	100%
Extrapolated value	58%

Q4. What percentage of this potential loss to PP&E assets is self-insured, including captives not reinsured?	FY2022
Less than 5%	10%
5% to 10%	13%
11% to 20%	14%
21% to 30%	17%
31% to 40%	16%
41% to 50%	13%
51% to 60%	7%
61% to 70%	7%
71% to 80%	2%
81% to 90%	1%
91% to 100%	1%
Total	100%
Extrapolated value	30%

Q5. What is the likelihood that your company will sustain a loss to PP&E assets totaling no more than **50 percent** of PML over the next 12 months?	FY2022
Less than 0.1%	22%
0.1% to 0.5%	16%
0.6% to 1.0%	16%
1.1% to 2.0%	15%
2.1% to 3.0%	16%
3.1% to 4.0%	8%
4.1% to 5.0%	6%
5.5% to 10.0%	2%
More than 10.0%	1%
Total	100%
Extrapolated value	1.62%

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?	FY2022
Less than 0.1%	68%
0.1% to 0.5%	14%
0.6% to 1.0%	8%
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%	1%
More than 10.0%	1%
Total	100%
Extrapolated value	0.53%

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?	FY2022
Disclosure as a contingent liability on the balance sheet (e.g., FASB 5)	22%
Footnote disclosure in the financial statements	43%
Discussion in the management letter	19%
None – disclosure is not necessary	12%
Other	5%
Total	100%

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

Q8. What is the total value of your company's **information assets**, including customer records, employee records, financial reports, analytical data, source code, models, methods and other intellectual properties? Please assume a value based on full replacement cost (and not historic cost). Please note this value can be either a precise quantification or estimate.	FY2022
Less than $1 million	6%
$1 to 10 million	9%
$11 to 50 million	16%
$51 to 100 million	24%
$101 to 500 million	22%
$501 to 1 billion	13%
$1 to 10 billion	8%
More than $10 billion	5%
Total	102%
Extrapolated value (US$ millions)	$1,213.34

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.	FY2022
Less than $1 million	7%
$1 to 10 million	12%
$11 to 50 million	14%
$51 to 100 million	23%
$101 to 500 million	18%
$501 to 1 billion	12%
$1 to 10 billion	10%
More than $10 billion	4%
Total	100%
Extrapolated value (US$ millions)	$1,151.52

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.	FY2022
Less than $1 million	18%
$1 to 10 million	22%
$11 to 50 million	21%
$51 to 100 million	16%
$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)	$321.15

Q10. What percentage of this potential loss to information assets is covered by insurance, including captives reinsured but not including captives not reinsured?	FY2022
Less than 5%	33%
5% to 10%	29%
11% to 20%	13%
21% to 30%	7%
31% to 40%	6%
41% to 50%	4%
51% to 60%	4%
61% to 70%	2%
71% to 80%	2%
81% to 90%	1%
91% to 100%	1%
Total	100%
Extrapolated value	16.6%

Q11. What percentage of this potential loss to information assets is self-insured, including captives not reinsured?	FY2022
Less than 5%	1%
5% to 10%	2%
11% to 20%	3%
21% to 30%	3%
31% to 40%	7%
41% to 50%	12%
51% to 60%	18%
61% to 70%	22%
71% to 80%	18%
81% to 90%	10%
91% to 100%	5%
Total	100%
Extrapolated value	59.6%

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?	FY2022
Less than 0.1%	2%
0.1% to 0.5%	4%
0.6% to 1.0%	6%
1.1% to 2.0%	10%
2.1% to 3.0%	10%
3.1% to 4.0%	16%
4.1% to 5.0%	16%
5.1% to 10.0%	18%
More than 10.0%	18%
Total	100%
Extrapolated value	5.1%

Q13. What is the likelihood your company will sustain a loss to information assets totaling 100 percent of PML over the next 12 months??	FY2022
Less than 0.1%	9%
0.1% to 0.5%	9%
0.6% to 1.0%	12%
1.1% to 2.0%	12%
2.1% to 3.0%	16%
3.1% to 4.0%	15%
4.1% to 5.0%	16%
5.1% to 10.0%	9%
More than 10.0%	4%
Total	100%
Extrapolated value	3.0%

Q14. In your opinion, how would your company disclose a material loss to information assets that is not covered by insurance in its financial statements?	FY2022
Disclosure as a contingent liability on the balance sheet (FASB 5)	11%
Footnote disclosure in the financial statements	42%
Discussion in the management letter	10%
None – disclosure is not necessary	33%
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?	FY2022
Yes, fully aware	37%
Yes, somewhat aware	49%
Not aware	14%
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.	FY2022
Yes	50%
No [skip to Q17]	50%
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.	FY2022
Cyber attack that caused disruption to business and IT operations (such as denial of service attacks)	49%
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	37%
Negligence or mistakes that resulted in the loss of business confidential information	42%
System or business process failures that caused disruption to business operations (e.g., software updates)	45%
Other	7%
Total	210%

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.	FY2022
Zero	1%
Less than $10,000	8%
$10,001 to $100,000	9%
$100,001 to $250,000	16%
$250,001 to $500,000	20%
$500,001 to $1,000,000	17%
$1,000,001 to $5,000,000	12%
$5,000,001 to $10,000,000	8%
$10,000,001 to $25,000,000	6%
$25,000,001 to $50,000,000	3%
$50,00,001 to $100,000,000	2%
More than $100,000,000	0%
Total	100%
Extrapolated value US$	$4,976,960

Q16d. If yes, how has the above security exploit or data breach changed your company's concerns about cyber liability?	FY2022
More concerned	66%
Less concerned	13%
No change	21%
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?	FY2022
Increase	68%
Decrease	11%
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.	FY2022
Cyber liability is the number one or two business risk for my company	20%
Cyber liability is a top 5 business risk for my company	35%
Cyber liability is a top 10 business risk for my company	31%
Cyber liability is not in the top 10 of business risks for my company	14%
Total	100%

Q18b. How did you determine the level of cyber risk to your company?	FY2022
Completed a formal internal assessment	22%
Completed an informal (ad hoc) internal assessment	21%
Hired a third party to conduct an assessment or audit	33%
Intuition or gut feel	15%
Did not do any type of assessment	9%
Total	100%

Q19a. Does your company have cyber insurance coverage, including within a technology Errors & Omission or similar policy not including Property, General Liability or Crime policy?	FY2022
Yes	30%
No	70%
Total	100%

Q19b. If yes, what limits do you purchase	FY2022
Less than $1 million	8%
$1 million to $5 million	30%
$6 million to $20 million	50%
$21 million to $100 million	8%
More than $100 million	4%
Total	100%
Extrapolated value (US$ millions)	$16.34

Q19c. Is your company's cyber insurance coverage sufficient with respect to coverage terms and conditions, exclusions, retentions, limits and insurance carrier financial security?	FY2022
Yes	58%
No	29%
Unsure	13%
Total	100%

Q19d. How does your company determine the level of coverage it deems adequate?	FY2022
Formal risk assessment by in-house staff	14%
Formal risk assessment conducted by the insurer	15%
Formal risk assessment by third party	23%
Informal or ad hoc risk assessment	13%
Policy terms and conditions reviewed by a third-party specialist	16%
Maximum available from the insurance market	19%
Other	1%
Total	100%

Q19e. What types of incidents does your organization's cyber insurance cover? Please select all that apply.	FY2022
External attacks by cyber criminals	83%
Malicious or criminal insiders	80%
System or business process failures	41%
Human error, mistakes and negligence	28%
Incidents affecting business partners, vendors or other third parties that have access to your company's information assets	44%
Other	27%
Unsure	2%
Total	304%

Q19f. What coverage does this insurance offer your company? Please select all that apply.	FY2022
Forensics and investigative costs	63%
Notification costs to data breach victims	57%
Communication costs to regulators	46%
Employee productivity losses	51%
Replacement of lost or damaged equipment	59%
Revenue losses	35%
Legal defense costs	45%
Loss of asset value	49%
Regulatory penalties and fines	49%
Third-party liability	44%
Brand damages	20%
Other	21%
Unsure	23%
Total	561%

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.	FY2022
Access to cyber security forensic experts	82%
Access to legal and regulatory experts	80%
Access to specialized technologies and tools	50%
Advanced warnings about ongoing threats and vulnerabilities	41%
Assistance in the remediation of the incident	56%
Assistance in the notification of breach victims	46%
Identity protection services for breach victims	27%
Credit monitoring services for breach victims	47%
Assistance in reputation management activities	49%
Other	16%
Total	494%

Q20a. Does your company plan to purchase standalone cyber insurance?	FY2022
Yes, in the next 12 months	16%
Yes, in the next 24 months	26%
Yes, in more than 24 months	21%
No	37%
Total	100%

Q20b. If no, what are the **two** main reasons why your company is not planning to purchase standalone cyber security insurance?	FY2022
Premiums are too expensive	35%
Coverage is inadequate based on our exposure	38%
Too many exclusions, restrictions and uninsurable risks	29%
Risk does not warrant insurance	8%
Property and casualty policies are sufficient	26%
Executive management does not see the value of this insurance	22%
Unable to get insurance underwritten because of current risk profile	17%
Other	7%
Total	182%

Q21. Who in your company is most responsible for cyber risk management? Please select your two top choice.	FY2022
CEO/board of directors	3%
Chief financial officer	5%
Business unit (LOB) leaders	20%
Chief information officer	21%
Chief information security officer	16%
Risk management	17%
Procurement	8%
General counsel	7%
Compliance/audit	4%
Other	1%
Total	100%

Q22. Does your organization use or plan to use cryptocurrency or non-fungible token assets?	FY2022
Yes, currently use	64%
No, but planning to use within the next 12 months	20%
There are no plans to use	16%
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?	FY2022
Yes	53%
No	47%
Total	100%

Q24. What is the total value of your company's IP assets such as trademarks, patents, copyrights, trade secrets and know-how?	FY2022
Less than $1 million	0%
$1 to 10 million	8%
$11 to 50 million	18%
$51 to 100 million	24%
$101 to 500 million	29%
$501 to 1 billion	15%
$1 to 10 billion	5%
More than $10 billion	2%
Total	100%
Extrapolated value	$596.88

Q25a. Did your company experience a material IP event in the past 24 months?	FY2022
Yes	35%
No	65%
Total	100%

Q25b. If yes, what type of IP assets were involved in the event?	FY2022
Patent	25%
Trade secret	41%
Copyright	26%
Other	8%
Trademark, Service mark or trade dress	—
Total	100%

Q25c. If yes, what best describes the event?	FY2022
Challenge to company rights	32%
Infringement of company rights	38%
Allegation of company infringement of third-party rights	30%
Total	100%

Q26. How do IP risks compare to other business risks?	FY2022
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	32%
IP risk is a top 10 business risk for my company	31%
IP risk is not in the top 10 of business risks for my company	18%
Total	100%

Q27. Does your company's existing insurance policy (e.g., property, general liability or crime) cover any of the following IP events?	FY2022
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	31%
Our existing policy does not cover IP events	34%
Total	133%

Q28a. Does your company have a trade secret theft insurance policy as a complement to a cyber risk policy?	FY2022
Yes	29%
No	71%
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?	FY2022
Very interested	31%
Interested	32%
Somewhat interested	26%
Not interested	12%
Total	100%

Q29a. Does your company have an intellectual property liability policy?	FY2022
Yes	33%
No	67%
Total	100%

Q29b. If not, what is your company's level of interest in purchasing an intellectual property liability policy?	FY2022
Very interested	31%
Interested	33%
Somewhat interested	25%
Not interested	11%
Total	100%

Q30. Can an external cyber and intellectual property incident become a Black Swan for your firm?	FY2022
Yes	48%
No	45%
Unsure	7%
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?	FY2022
Yes	43%
No	46%
Unsure	11%
Total	100%

Part 4. Role & Organizational Characteristics

D1. What level best describes your current position?	FY2022
Senior executive	5%
Vice president	5%
Director	13%
Manager	17%
Supervisor	16%
Associate/staff	10%
Technician	25%
Contractor/consultant	9%
Other	2%
Total	100%

D2. What is the worldwide employee headcount of your company?	FY2022
Less than 500	16%
500 to 1,000	16%
1,001 to 5,000	25%
5,001 to 25,000	25%
25,001 to 75,000	12%
More than 75,000	7%
Total	100%

D3. What best describes your company's industry focus?	FY2022
Agriculture & food service	1%
Communications	3%
Consumer products	5%
Defense & aerospace	1%
Education & research	4%
Energy & utilities	6%
Entertainment & media	3%
Financial services	18%
Food service	0%
Health & pharmaceuticals	9%
Hospitality	4%
Industrial	11%
Public sector	8%
Retailing	9%
Services	10%
Technology & software	8%
Transportation	2%
Other	2%
Total	100%

5 Acknowledgements

The 2022 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:

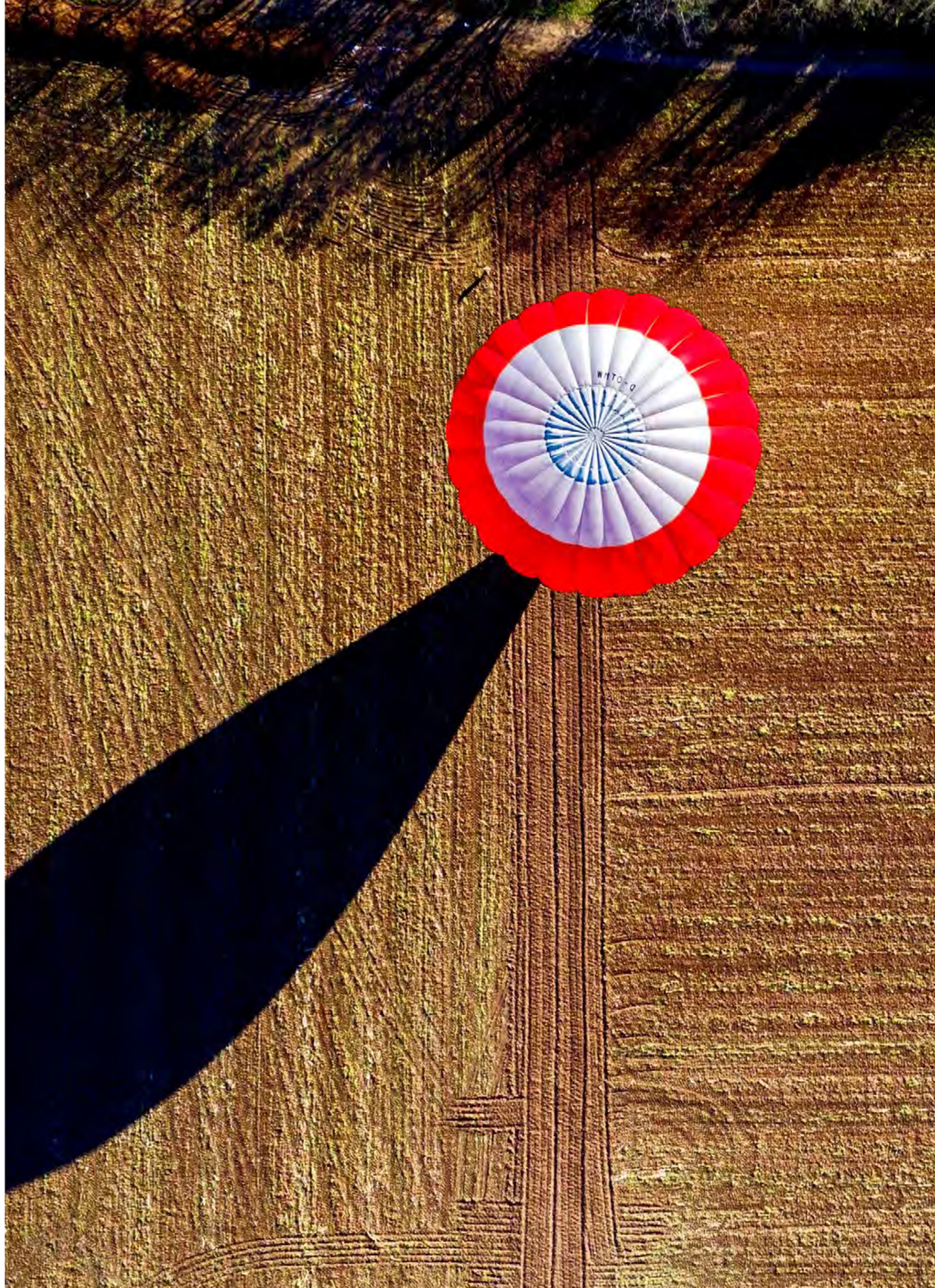
Jesus Gonzalez
Aon Intangible Assets Deputy Global Practice Leader

Carrie Yang
Aon AsiaPac Intangible Assets leader, Aon's Cyber Solutions

Christine Williams
Aon Global Specialty Products Leader
Global CEO Financial Services
Group & Professional Services Practice

Steve Keogh
Senior Advisor – Office of the President, Aon plc

Kevin Kalinich
Esq., Aon Intangible Assets Global Collaboration Leader



“

I discovered Buddha did not set out to found a world religion. He set out to understand why one suffers. I learned that only through living life’s ups and downs can you develop empathy; that in order not to suffer, or at least not to suffer so much, one must become comfortable with impermanence.

Satya Nadella
Executive Chairman and CEO of Microsoft

“

People should make use of every opportunity in life to practice benevolence, and one of the ten ways to do so is to help others succeed. Benefiting others is a virtue. We can do so by providing others assistance in what they do, saying a few good words about them or providing them with positive conditions.

Liao-Fan’s Four Lessons

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

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

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. Our colleagues provide our clients in over 120 countries with advice and solutions that give them the clarity and confidence to make better decisions to protect and grow their business.