Aon Risk Solutions

Cyber–the fast moving target

Benchmarking views and attitudes by industry

2016

Risk. Reinsurance. Human Resources.

Empower Results®

Table of Contents

Introduction

Two days before Christmas 2015, hackers attacked the power grid in the Ivano-Frankivsk region of Ukraine with a virus that had erased the programs engineers use to monitor equipment. For six hours, 103 cities were hit with power outages and another 186 cities were left partially in the dark because devices that route power and change voltages had been disconnected from the grid.

This attack on the power grid and control systems of energy suppliers has sent shockwaves around the world, fueling concern over the mounting capacities of hackers to cause massive physical and financial damage. The incident, one of the most disruptive in scale, added to a long list of other high-profile breaches in 2015, which journalists and IT experts called "the year of cyber attacks ".

The rapidly changing nature of cyber threats confounds many. As the security industry strives to protect companies with new, powerful tools, hackers invariably deploy even more damaging cyber attack techniques. Furthermore, they are not limiting the focus of the attacks to network and privacy data; rather, it extends to cars, airplanes, power grids and the "Internet of Things" (IoT).

Disruptions or exploited vulnerabilities in integrated IoT systems have the potential to cause business interruption, tangible property damage, supply chain shut down, and bodily injury.

While criminals are predominantly aiming at financial gain by stealing personal and company data, ideologically motivated groups also exploit cybercrime techniques to sabotage the operations and reputation of corporations and governments by stealing and publishing confidential information. Additionally, the persistent concern of insider threats and employee negligence further highlights the wide-ranging organizational challenges presented by cyber risk.

Concerns for the rising scale and frequency of cyber attacks are reflected in Aon's 2015 Global Risk Management Survey. For the first time, surveyed companies have ranked computer crimes, hacking, viruses, and malicious code as one of the top ten risks facing businesses today and in the next three years.

However, despite such urgency past studies conducted by Aon have shown that a majority of organizations have neither completed a cyber risk assessment nor bought cyber cover.

These results have given us pause, prompting Aon to undertake a detailed study of what large companies across various industries are doing to mitigate such threats.

We hope that the findings, presented in both aggregation and by industry, will allow organizations to gain insight into this mounting threat, benchmark their risk management practices, and identify approaches that may increase their preparedness.

With our global footprint—Aon operates in more than 120 countries staffed by 72,000 colleagues—we strive to provide our clients with such fact-based analytics that can assist in developing forward-thinking strategies and gaining a competitive edge .

If you have any questions or comments about the survey or wish to discuss the survey further, please contact your Aon account executive or visit **aon.com/cyber**.

Research Profile

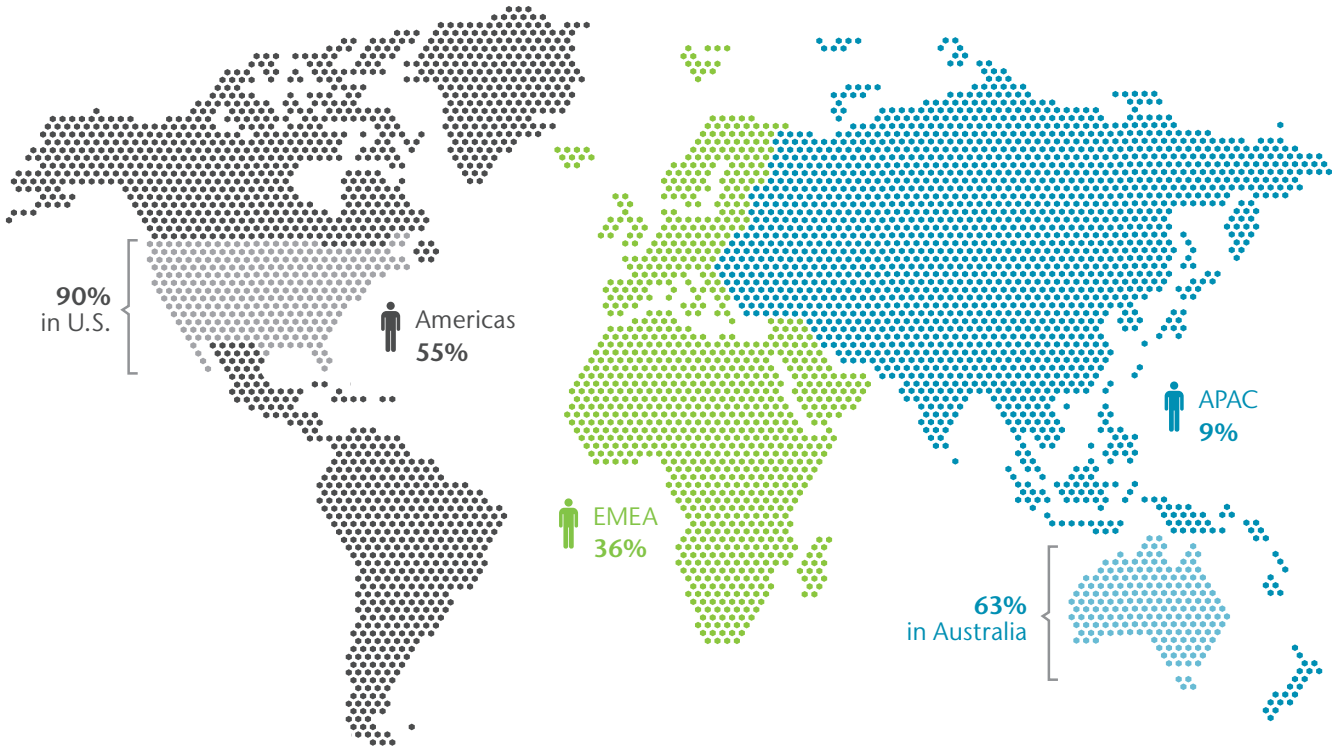
Aon's first cyber captive survey, conducted in fall 2015, has gathered input from 128 of Aon's captive clients, which represent a broad range of industries and geographical regions.

These clients currently have an established captive managed by Aon Captive and Insurance Management. Through the survey, we aim to gain a better understanding of our clients' current thinking and practices relating to cyber threats, identify their cyber needs, and explore a captive or retail market cyber solution.

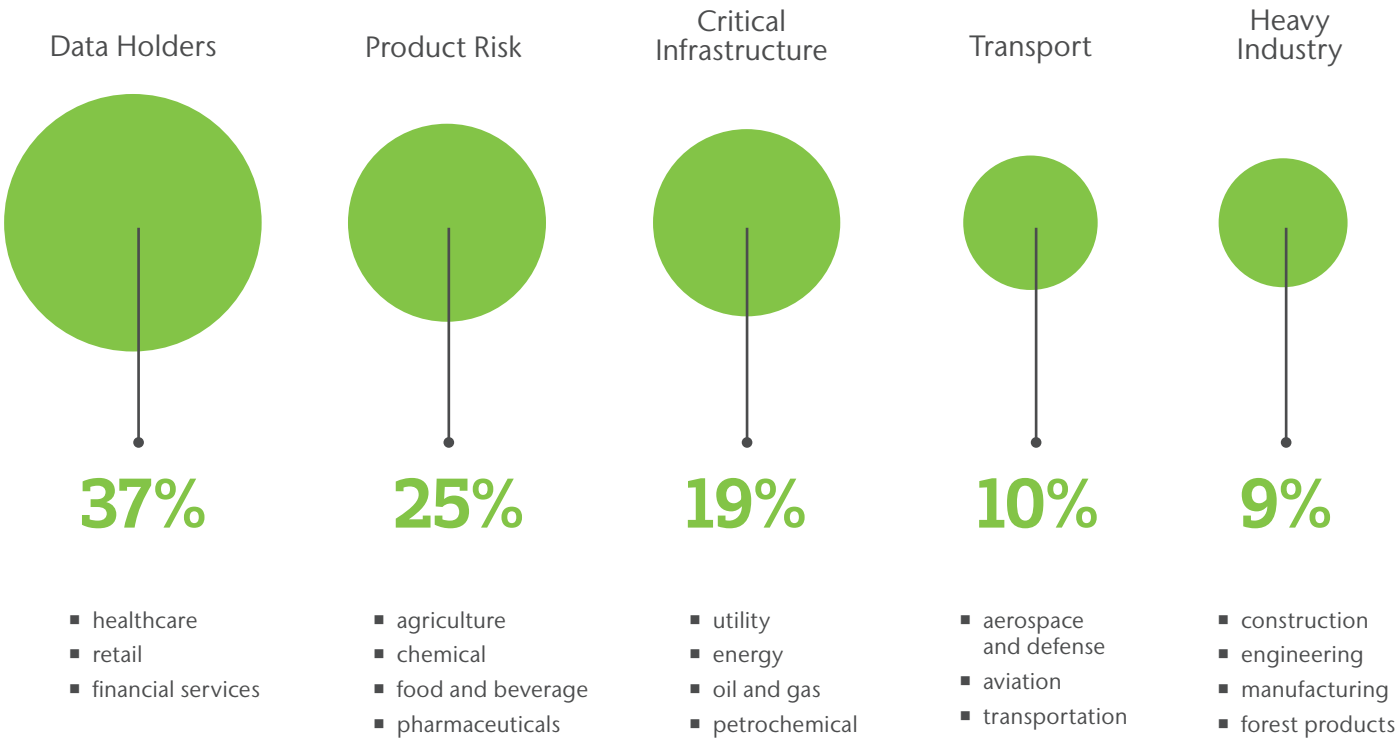
For the purpose of analysis, we have divided the surveyed clients by size according to revenue—greater than USD 5 billion and less than USD 5 billion. The findings are presented both in aggregation and by industry sector.

Research respondents by revenue

Research Respondents (Risk Managers and Directors of Captive Insurance Companies) by Region



Survey respondents by industry categories



Executive Summary

As the Fourth Industrial Revolution progresses, driven by widespread use of mobile technologies, cloud computing, corporate bring-your-own-device policies, big data analytics, and 3D printing, cyber has emerged as one of the fastest growing risks for governments and companies across the globe. Equally or perhaps even more important is the growing realization that cyber risk, in some instances more pervasive than traditional exposures, is present wherever organizations use technology to touch people, suppliers, customers, and governments.

In light of these developments, we wanted to find out what large forward-thinking companies around the globe think about cyber risk and ascertain their attitude towards managing it. In the following survey which is structured in four main sections—**cyber risk concerns, risk assessment, attitudes toward cyber insurance**, and **policy cover and structure**, respondents have shared with us their thinking and the steps they have taken to cope with the fastly evolving cyber risks.

As the overall insurance market is designing innovative solutions to address the uncertainties, these key findings have revealed some valuable answers.

Cyber risk concerns

Business interruption, both during a breach and post breach was rated as the top cyber risk concern by survey respondents, whereas bodily injury/property damage (first and third party) was rated as their lowest concern.

The results align to the growing dependency of companies on IT infrastructure to support mission critical business operations and an understanding of the significant disruptive impact that cyber attacks can have on business processes. While media coverage of cyber risk incidents tends to focus on data privacy and regulatory fines, across the board clients' number one risk concern is business interruption, both during and after a breach. With continued digital transformation, we see this risk remaining at the top of executives' cyber risk concerns across all industry groups.

Furthermore, we have seen losses move from the intangible world of data, into the physical world, resulting in direct property damage from cyber events. Although property damage/bodily injury is currently rated as the lowest concern, with the "Internet of Things" we are beginning to see the link between digital and physical losses increasing, resulting in growing concern amongst both corporations and insurance providers. Typically, physical loss is not addressed by a cyber policy and property policies do not consistently respond to these types of losses either, hence this evolving area of risk needs to be watched carefully and companies should stay ahead of it by regularly connecting with their risk management expert and cyber insurance broker.

Cyber risk assessment

Only 59% of companies have used a formal risk assessment process to help inform their insurance buying decision, and a mere 51% of companies would value an independently administered cyber risk assessment.

The stated use of cyber risk assessments to inform insurance strategy remains surprisingly low given the evolving nature and complexity of cyber exposures and the lack of historical loss data. Companies with comparative risks in other lines of insurance typically approach the property insurance market following for example a detailed engineering report on their risks as this is a crucial step for them when distinguishing their exposures from inferior risks.

A formal risk assessment process will help inform risk retention, transfer and mitigation strategies as it serves to identify, assess and quantify exposures. ERM frameworks are advised to adopt new approaches to analytics and techniques to include cyber risk, and this maturity should occur across all industry verticals. Given the divide between cyber risk concerns and insurance cover we believe that 59% is too low a number and highlights that many businesses might not know the appropriate starting point to conduct a meaningful cyber risk assessment.

Only 51% of respondents would value an independently administered risk assessment. This finding is also lower than we would expect, given that 75% of companies are concerned about the loss adjustment process where claim disputes involving coverage interpretation and quantum could potentially be mitigated by a formal risk assessment and quantification report obtained at inception.

Only 25% of companies are sure they comply with international best practices and standards for information security governance.

This finding, which is consistent throughout all industry sectors, reflects what we call the "great digital divide" in organizations in regards to cyber risk. Without benchmarking to an accepted best practice or standard, risk managers rely on internal IT managers to determine whether their information security standards are sufficient.

Effective cyber risk management is the result of having the appropriate people, tools and processes in place. It includes knowing who is doing what and when—and practicing and communicating that process.

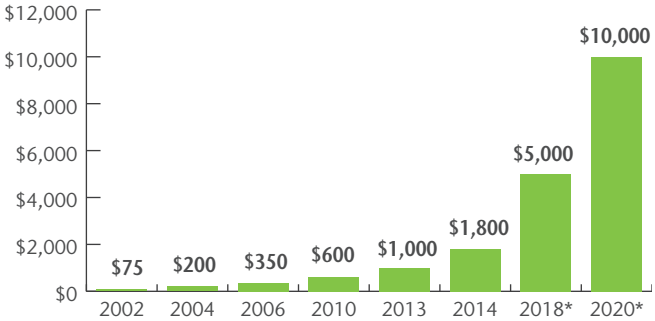
Attitudes toward cyber insurance

68% of companies buy cyber for balance sheet protection, closely followed by ensuring due diligence comfort for the board.

Buying cyber insurance for balance sheet protection is not surprising. What is more revealing however is the motivation to purchase cover to ensure board comfort. For those who buy cover, 75% have concerns about the loss adjustment process and almost 99% suggest that policy terms and conditions need to be clearer. This leads us to believe that companies are unsure of the value of their cyber insurance purchase and may in some cases have been buying inadequate coverage in an effort to satisfy their board's need for having cover in place.

60% of large companies don't buy cyber insurance.

Cyber Insurance: Global Gross Written Premium



*2018 *: estimated by PWC*
*2020 *: estimated by ABI research*

Despite the growing frequency and scale of cyber attacks and increasing management focus, more than half of the surveyed companies do not buy cyber insurance. There are marked differences by industry with 70% of companies who are classed as "data holders" buying coverage versus 17% of critical infrastructure companies at the low end. Cyber insurance currently appears to have a much longer sales cycle than many other lines of cover as we have seen many clients exploring cyber insurance for a number of years without making a purchase. As cyber insurance has only been available for the last 15 years, it has not yet developed into a mature product. There is a great deal of variation in coverage triggers, definitions and exclusions. In line with other experts and industry bodies, we do however predict a material uplift in cyber insurance purchases over the next 5 years as cyber coverage develops.

Policy cover and structure

61% of clients who buy insurance buy limits in the USD 10m–USD 25m range.

The most frequently selected limit range is extremely low relative to the exposures. Only 17% of respondents buy limits in excess of USD 100m and most of these are companies in the critical infrastructure sector. Cyber has been around for 15 years and insureds are still seeking to determine the appropriate limit to purchase. As such, peer benchmarking has limitations. As more sophisticated analytic modeling becomes available (like Aon's recently released Cyber Insight model) we anticipate a greater understanding of the exposure particular to any one organization.

Nearly 95% of companies state clear policy wording as the most important issue in the cyber risk market and 75% of large companies express concerns about the loss adjustment process.

This result is not surprising given the evolving nature of the risk. Cyber insurance by its nature is a "gap" coverage addressing those risks not covered by standard P&C policies. As the risk evolves with new sources of claims and the insurance market adjusts its response, coverage analysis of cyber policies and how they dovetail, or not, with P&C policies will remain a priority and clear policy wordings are a must. Currently, even some traditional insurance experts are admitting that cyber risk developments are outpacing them, so the demand for clear policy wording is of vital importance for insurance carriers to help companies obtain the appropriate cover.

The high rate of concern regarding claims handling reflects understandable uncertainties regarding the ability of cyber insurers to meet buyer expectations and is directly connected to the clear policy wording issue. This is to be expected with a relatively "new" coverage, especially given cyber coverages' potential breadth and significance in terms of first and third party exposures. We expect to see coverage disputes, increased use of cyber claims management experts and further similar developments with more and more involvement from legal teams.

One possible solution to curtail these developments from spiraling out of control is an insurance carrier cross-function approach from the beginning—allowing underwriters, brokers, and claims experts to work alongside each other to better understand the emerging coverage needs and to create policies that are clear, fair and fit for purpose.

94% of companies said they would share risk with others in their industry as part of a captive facility writing cyber

Given the prior findings, it is highly conceivable that large companies would consider an industry type mutual which gave them some control over underwriting, coverage scope and claims adjustment, whilst providing an opportunity to share best practices, experience and data in a private setting. Larger clients in particular who see limited value in the current industry risk transfer options may start to explore this route. The extent to which these alternative risk transfer options are pursued will depend on the market's ability to keep pace with client needs.

Key Findings Comparison by Industry

Topics	Data Holders	Product Risk	Critical Infrastructure	Transportation	Heavy Industry
Top Cyber Risk Concern	Post Breach Business Interruption	Business Interruption	Business Interruption	Business Interruption	Business Interruption
Lowest Cyber Risk Concern	Bodily Injury/ Property Damage	Bodily Injury/ Property Damage	Data & System Restoration	Loss of IP	Bodily Injury/ Property Damage
Use of Risk Assessment to inform Coverage/Limits	51%	75%	59%	70%	56%
Rationale for buying cover	Board Due Diligence (80%)	Balance Sheet Protection (58%)	Balance Sheet Protection (71%)	Balance Sheet Protection (64%)	Board Due Diligence (56%)
Who is buying?	70%	17%	29%	33%	33%
Limits (m)	USD 10-25	USD 10-25	>USD 100	USD 10-25	USD 10-25
Budgeted for Cyber Cover	74%	31%	41%	9%	33%

Key Findings

Cyber Risk Concerns

Which elements in cyber risk give you the greatest cause for concern?

Not surprisingly, the inability to conduct business tops respondents' concerns in the case of a cyber-induced business interruption, followed by post-breach loss—continuing loss of revenue in the immediate aftermath of resuming business as usual, abnormal turnover of customers, reputational damages, and diminished goodwill.

In the past, when thinking of business interruption insurance, natural disasters such as fires, floods, and earthquakes came to mind. However, as day-to-day operations rely more on IT systems and data delivered over the Internet, cyber attacks can be a leading driver of business interruption loss. As technology continues to drive efficiencies in productivity and creates new commercial opportunities, it equally creates exploitable opportunities for security breaches. Whether causing physical damage to property, equipment failures, supply chain disruptions, or simply the inability to use revenue-generating systems such as e-commerce sites, cyber disruptions can put revenue and profit streams at great risk. And without adequate breach response and business continuity plans in place, the disruption could potentially severely damage an organization's brand and reputation.

Smaller companies, with less than USD 5 billion in revenue, put post-breach extended business interruption as a close second. This is typically because large companies have the prowess and financial wherewithal to recover from reputational losses caused by a cyber-related business interruption, whereas smaller companies are more vulnerable, especially when cyber attacks cause lengthy disruptions.

Moreover, the unpredictable nature of reputational crises in an age of 24-hour news cycles and social media channels poses additional challenges. Companies must now operate under the assumption that any cyber-induced business interruption could potentially harm their reputation and brand, and that such threats are real. The two risks seem not only interconnected but intrinsically linked, and companies who operate in heavily regulated and extremely consumer-focused industry sectors are well advised to be concerned about these risks, and to mitigate them.

At present, current data relating to the long-term negative impact on a company's reputation are mixed. While a few extreme cases have led to reductions in market capitalization and management changes, the majority of companies have gradually recovered from measurable reputational losses.

Surprisingly, business interruption caused by a breach of third-party systems is rated relatively low. The recent cyber incidents involving third-party vendors for major international retailers and hospitals serve as stark reminders of the rising frequency and costly impact of third-party breaches on large companies.

For a simple illustration of this interconnectivity of risks, please visit **www.aon.com/2015GlobalRisk** and watch our interactive video to learn more.

When a company suffers a cyber breach, the immediate losses are most commonly related to the loss of customer or employee data, all of which could trigger lawsuits by victims for inappropriate access to private information, or fines and customer redress brought on by regulators.

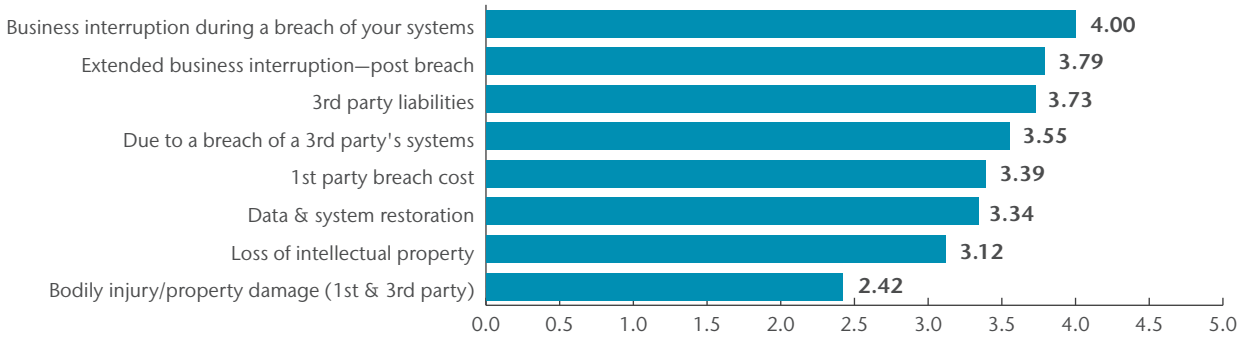
In terms of intellectual property, a survey conducted by security firm Kaspersky Lab shows that more than one in five large manufacturing firms reported a loss of intellectual property through a cyber attack in 2014. Large organizations worldwide lose five percent of their revenue to fraud, much of it attributable to the theft of intellectual property. The United States Commission on the Theft of American Intellectual Property estimates that cyber espionage and other forms of intellectual property theft from foreign countries account for annual losses of USD 300 billion for U.S. companies.

The former chief of the National Security Agency (NSA) stated as early as 2012 that "cybercrime constitutes the greatest transfer of wealth in history."

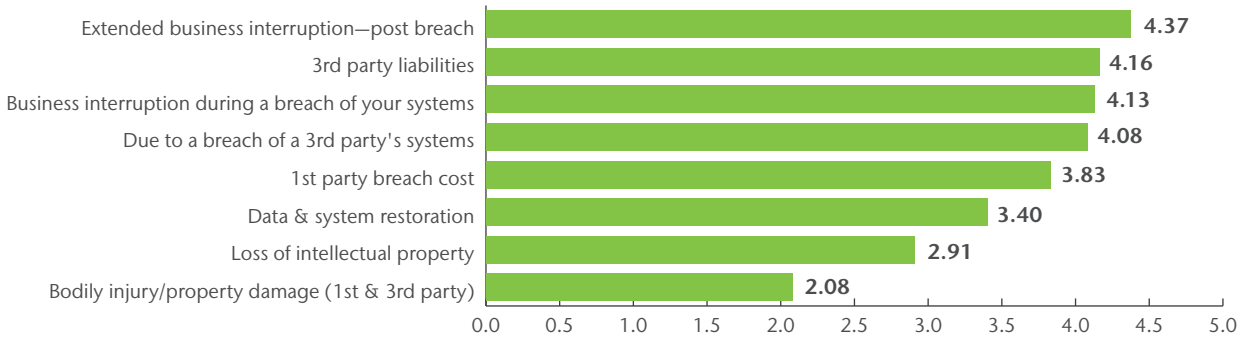
Cyber Loss Spectrum

Which elements in cyber risk give you the greatest cause for concern?

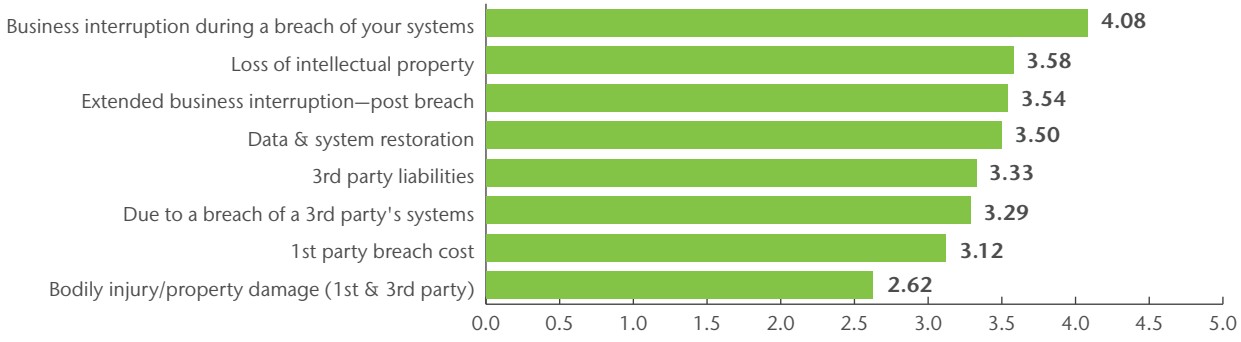
Overall



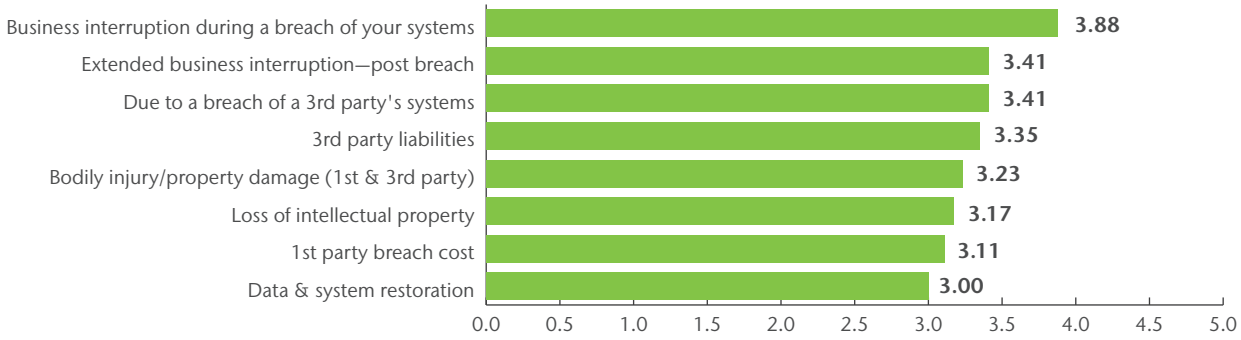
Data holders



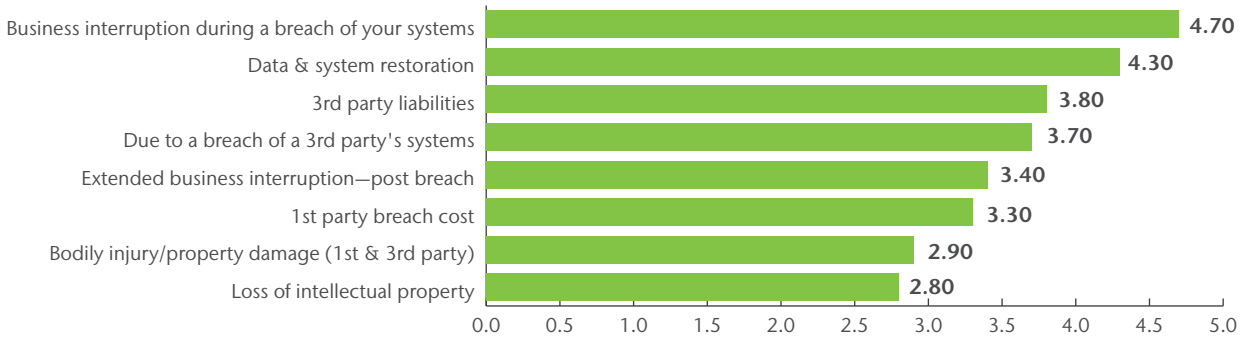
Product risk



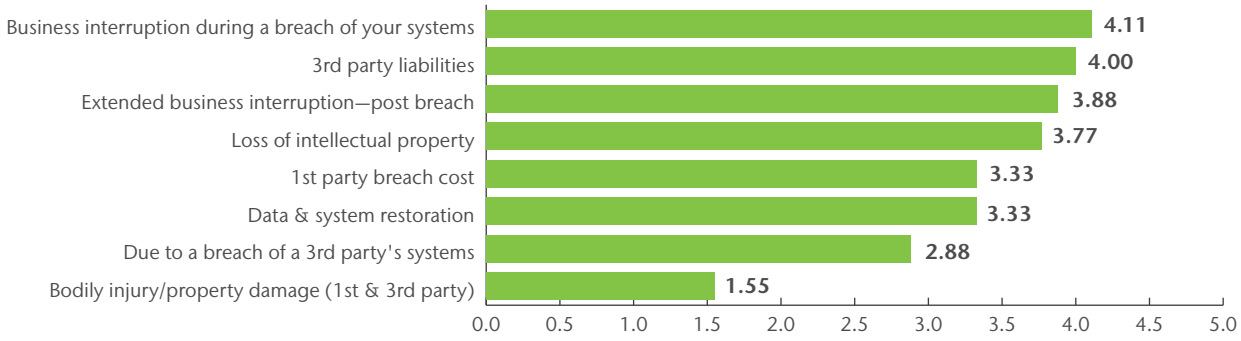
Critical infrastructure



Transport



Heavy industry



Risk Assessment

Factors that influence total limits decisions

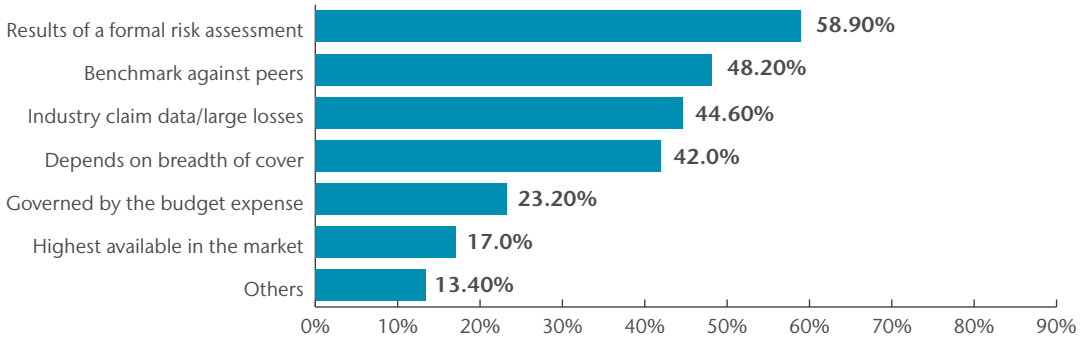
When deciding on total limits to insure, which factors influence the decision ?

About 59% of respondents go through a formal risk management process to arrive at the limits decision, which suggests that they not only value the advice of risk management professionals, but also take a thoroughly holistic and analytical approach to determining the protection needed. Aon believes this remains surprisingly low given the nascent nature and complexity of the risk. ERM frameworks are advised to adopt new approaches to data analytics and techniques to include cyber risk, and this maturity should occur across all industry verticals.

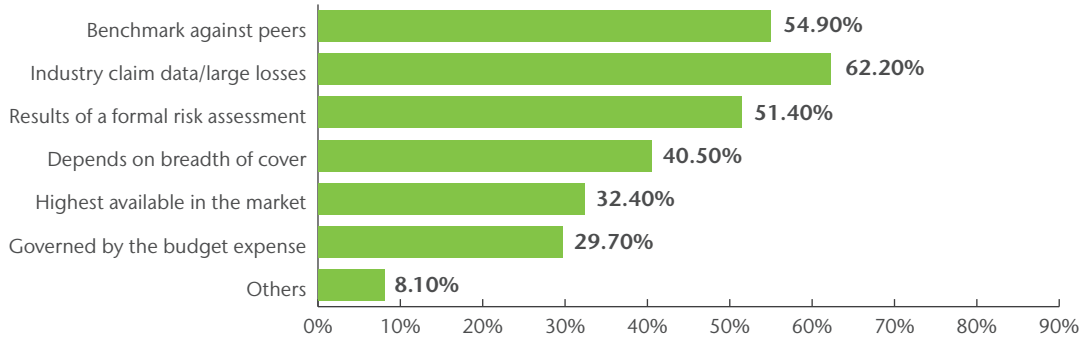
For companies with revenues above USD 5 billion, a higher percentage (67.2%) has chosen results of formal risk assessment as a key factor in deciding total limits, followed by industry claims data/large losses (44.8%) and dependence on breadth of cover (43.3%).

On the other hand, smaller companies (57.8%) use benchmarking against their peers to make total limits decisions, followed by results of formal risk assessment (46.7%) and industry claims data (44.4%). Given the fast pace of change companies should not be relying on lagging indicators to inform their views on the emerging cyber risk. Instead, they are advised to undertake forward looking cyber risk assessments to help stay ahead of the curve.

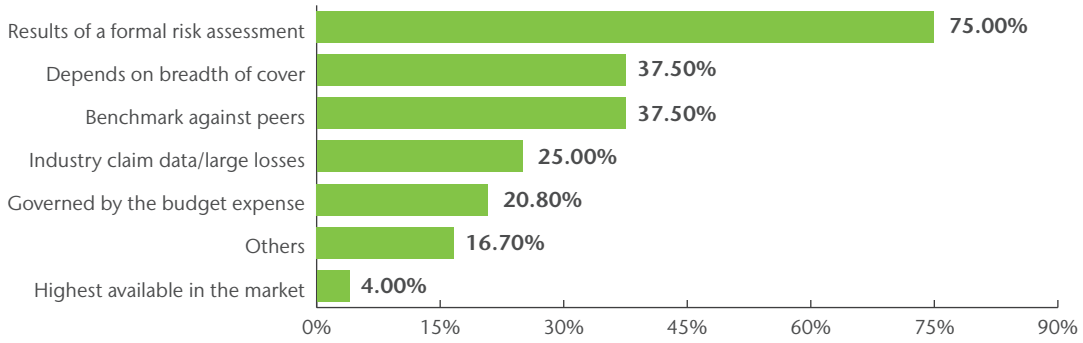
Overall



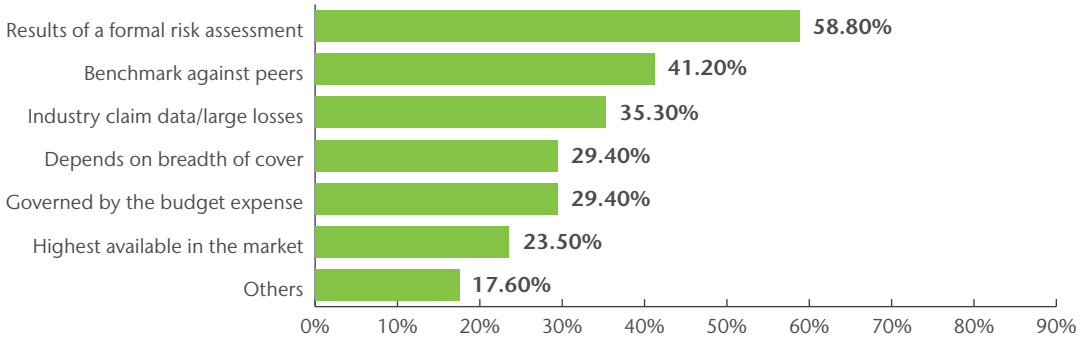
Data holders



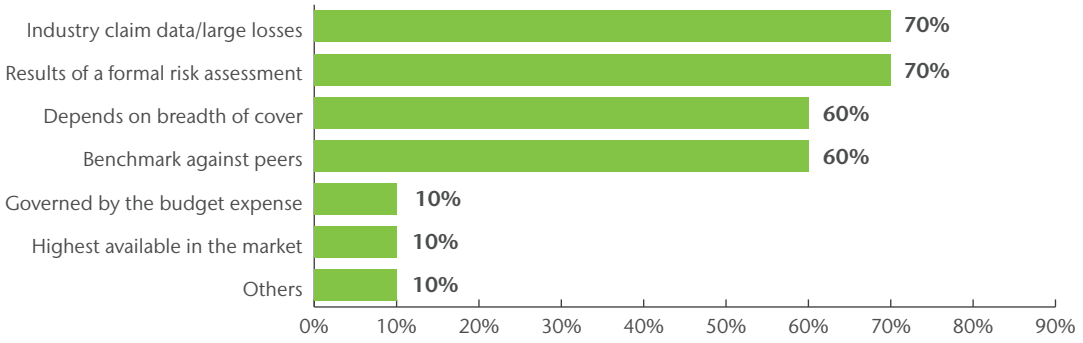
Product risk



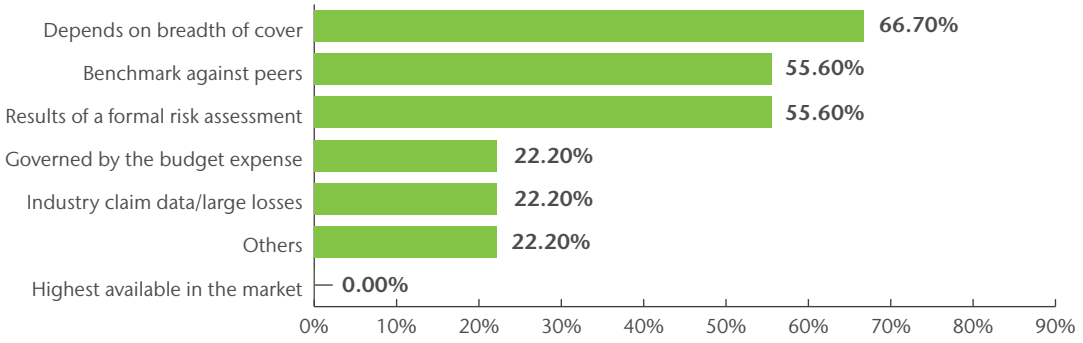
Critical infrastructure



Transport



Heavy industry



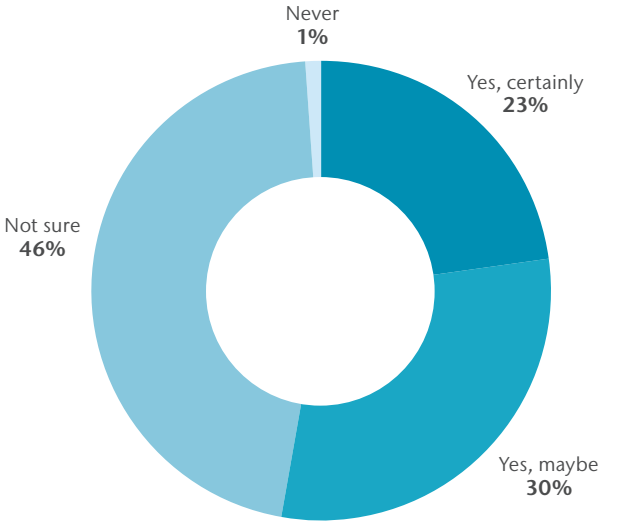
International best practices and standards

Based on the information currently available to you, do you know if your company complies with international best practices and standards governing information security (e.g., ISO 27001/002, NIST, or similar)?

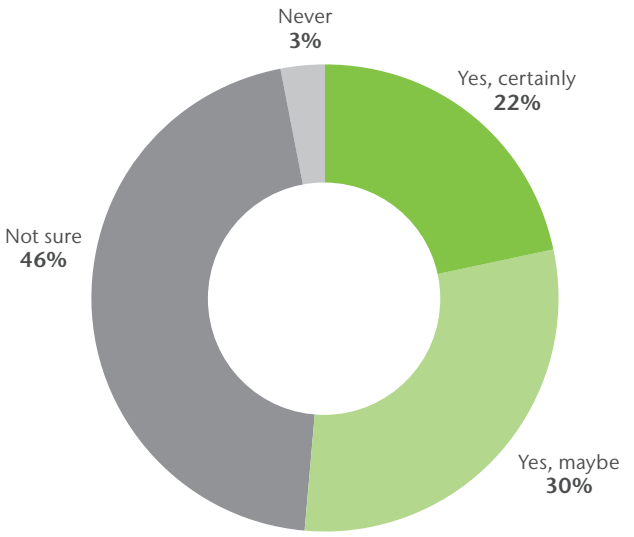
Nearly half of respondents are unsure if their companies comply with international best practices and standards for information security governance, such as ISO27001/002, NIST, or similar. A higher percentage of heavy industry participants (88%) say they do not know. This finding, which is consistent throughout all industry sectors, reflects what we call the "great digital divide" in organizations in regards to cyber risk.

Without benchmarking to an accepted best practice or standard, risk managers rely on internal IT managers to determine whether their information security standards are sufficient. Some choose to rely on industry peer comparisons, and while this may be satisfactory on one level, any favorable comparison is hollow if industry peers are themselves unprotected. But without an independent assessment of IT security effectiveness, risk managers may lack control and insight into an important enterprise-wide risk.

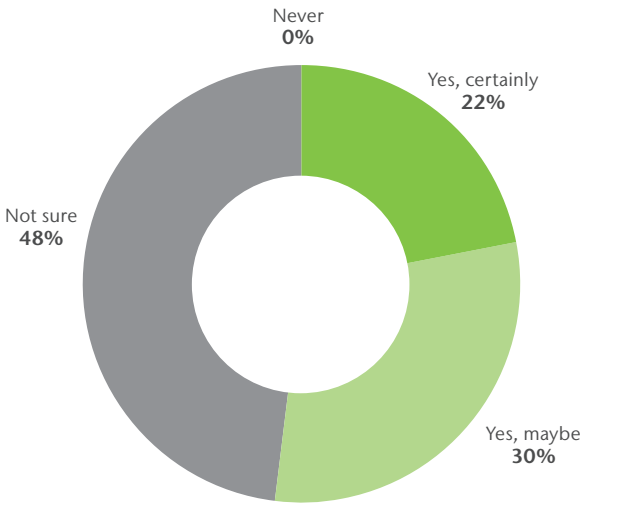
Overall



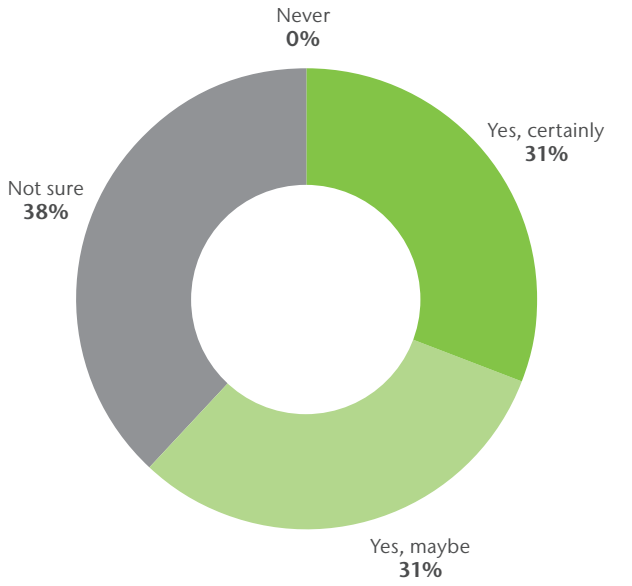
Data holders



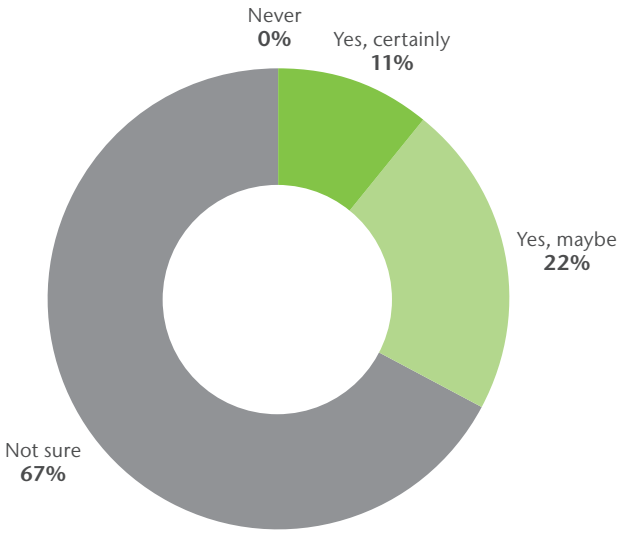
Product risk



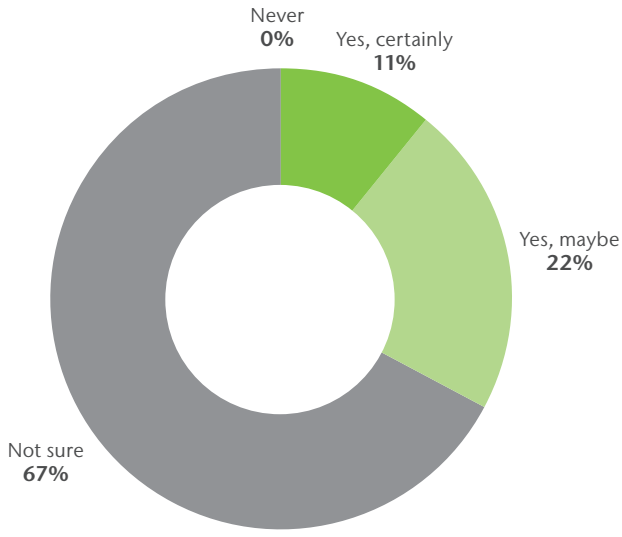
Critical infrastructure



Transport



Heavy industry



Independent cyber risk evaluation

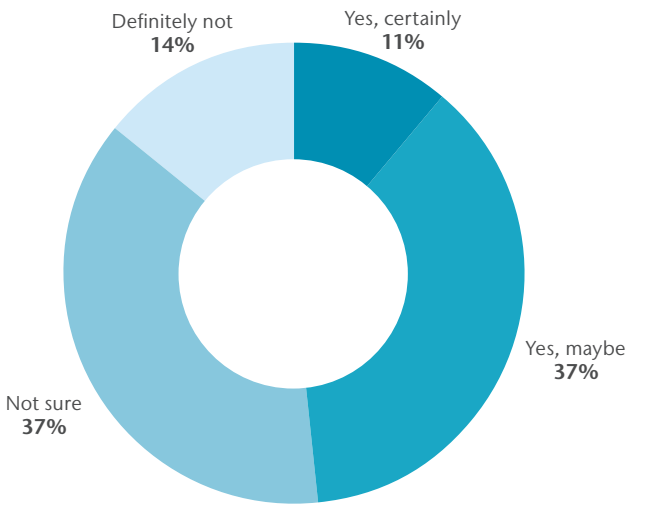
Would an independently administered cyber risk evaluation assist you in understanding and quantifying first and third-party cyber exposure?

Nearly half of respondents say that an independent cyber risk evaluation could help organizations understand and quantify first and third-party cyber exposure, establishing a benchmark standard for loss adjustment should a cyber event occur. About 34% say they are unsure.

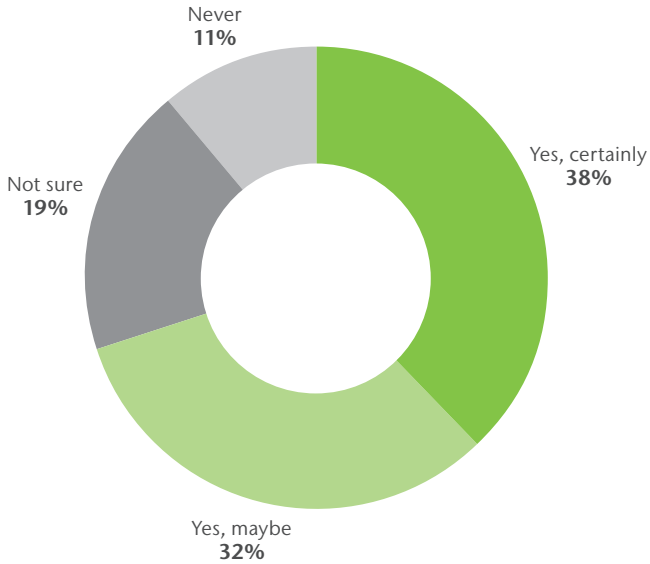
While 52% of larger companies agree with the statement, only 42.8% of smaller companies have indicated “yes, certainly” and “yes, maybe.”

It is interesting to note that the percentage of respondents who have selected the "definitely not" option was 9.5% in smaller companies vs. 17% in larger organizations. Almost half of the respondents did not express the need for a holistic cyber risk assessment, perhaps suggests a lack of visibility into the changing digital landscape and its inherent risks within their organization from their position within the risk function.

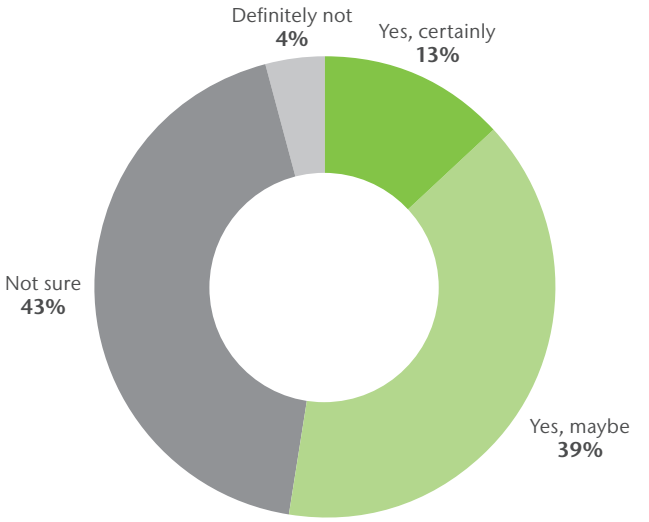
Overall



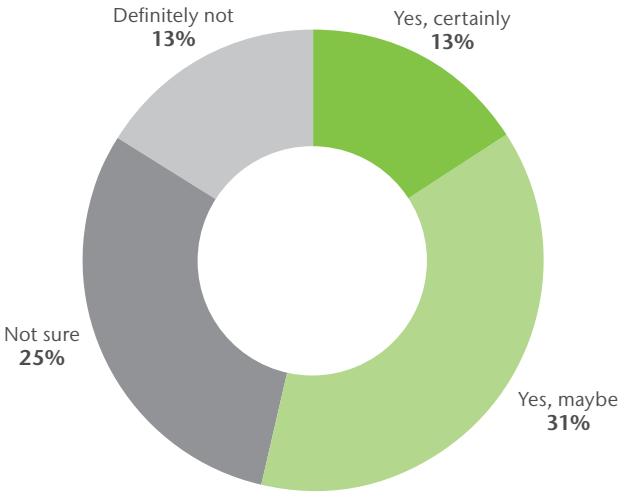
Data holders



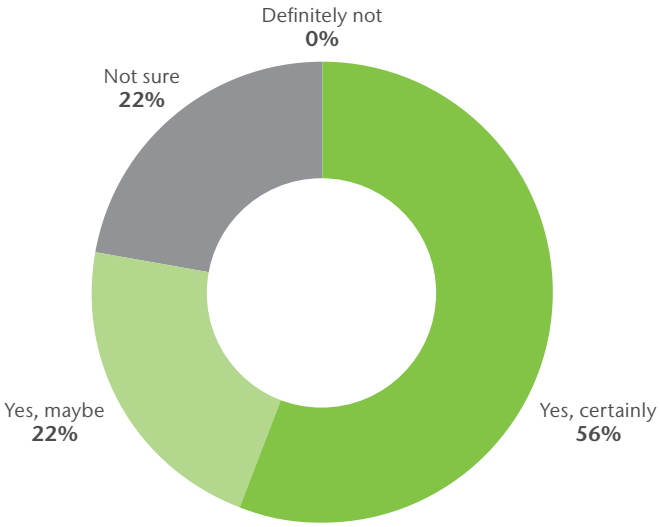
Product risk



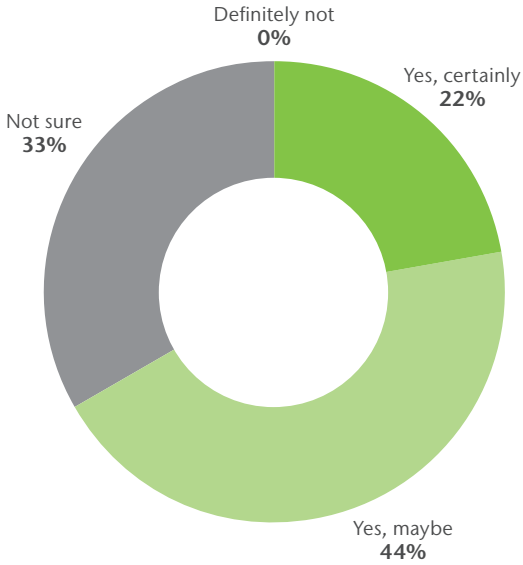
Critical infrastructure



Transport



Heavy industry



Attitudes toward Cyber Insurance

Main reasons for purchasing or considering cyber insurance

What are your main reasons for purchasing or considering cyber insurance?

With the average estimated cost of a data breach event reaching USD 3.8 million, and catastrophic breaches resulting in cyber insurance limits losses in excess of USD 100 million, it is not surprising that the majority of survey participants have listed balance sheet protection as the main reason for purchasing or considering insurance to cover catastrophic exposures.

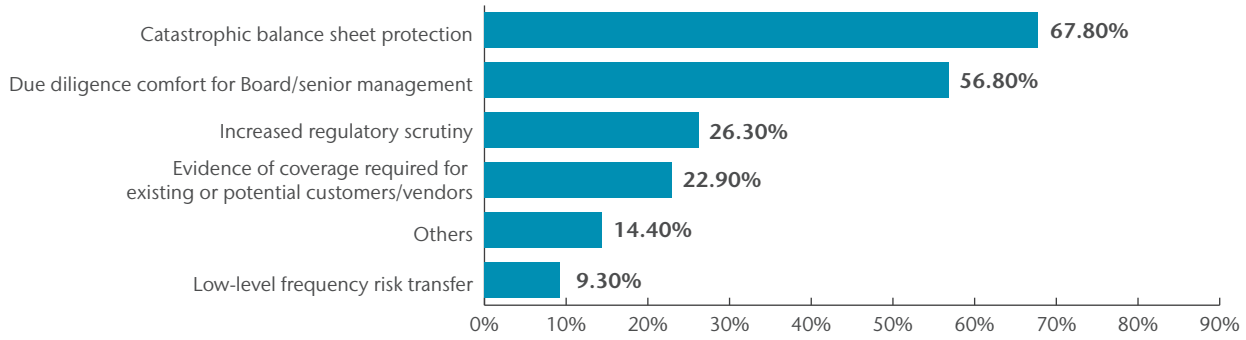
The increase in the number of directors and officers lawsuits, as well as senior management's rising awareness and cyber literacy, help explain why due diligence for board/senior management is ranked as the second most important reason. Corporate leadership has come to realize that cyber is not merely a technical issue relegated to the Chief Information Officer (CIO): it is an enterprise-wide business risk, and the ultimate responsibility to tackle cyber threats lies in the hands of the board and senior management.

While smaller companies see increased regulatory scrutiny as the third top reason, those with revenues greater than USD 5 billion rank evidence of coverage for existing or potential customers/vendors as the third most important reason.

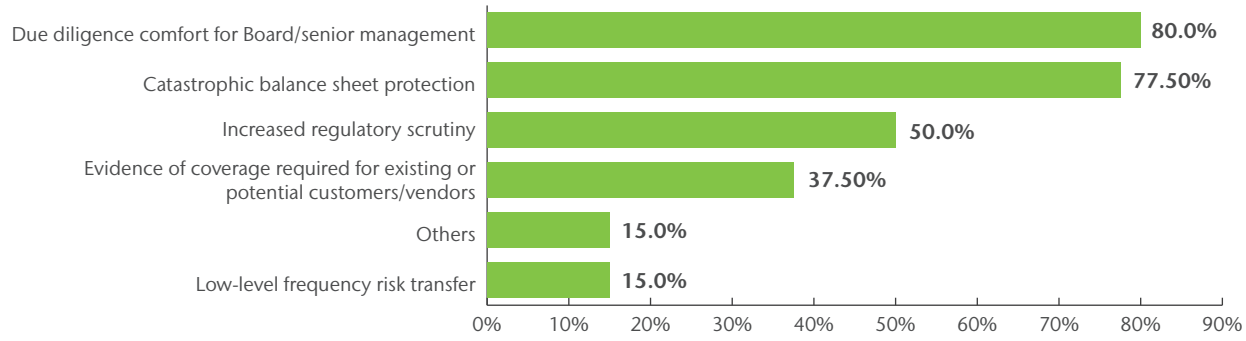
Based on our past research and experiences, clients have identified additional benefits of cyber insurance:

- Provide a baseline understanding of a company's information security program
- Satisfy customer and partner cyber insurance contract requirements (cyber insurance is often used as a tool to differentiate entities with partners, customers, and vendors in order to facilitate sales and to contractually allocate risk)
- Stabilize balance sheets
- Address regulatory guidelines and requirements
- Reduce the Total Cost of Risk
- Enable an organization-wide cyber risk management culture
- Align cyber insurance solution with Enterprise Risk Management

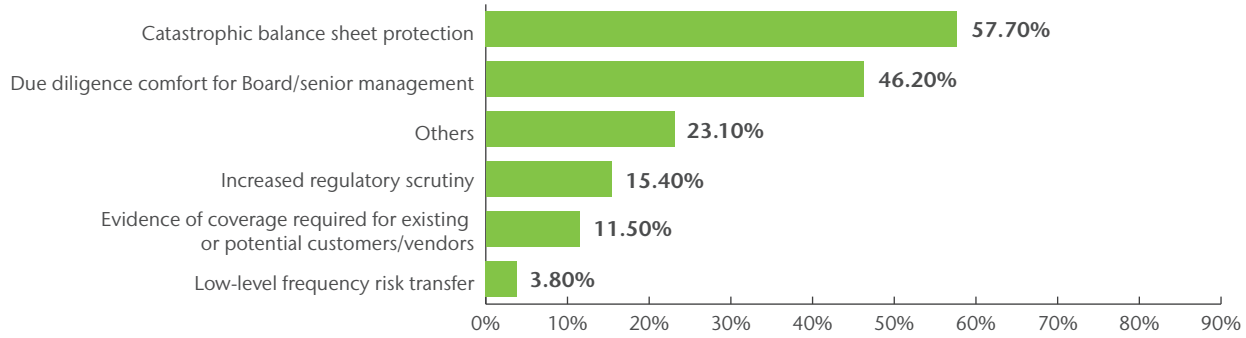
Overall



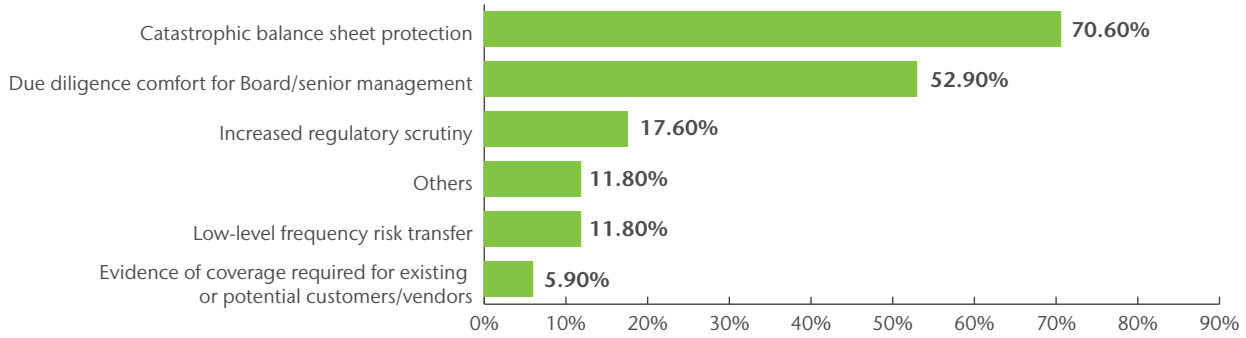
Data holders



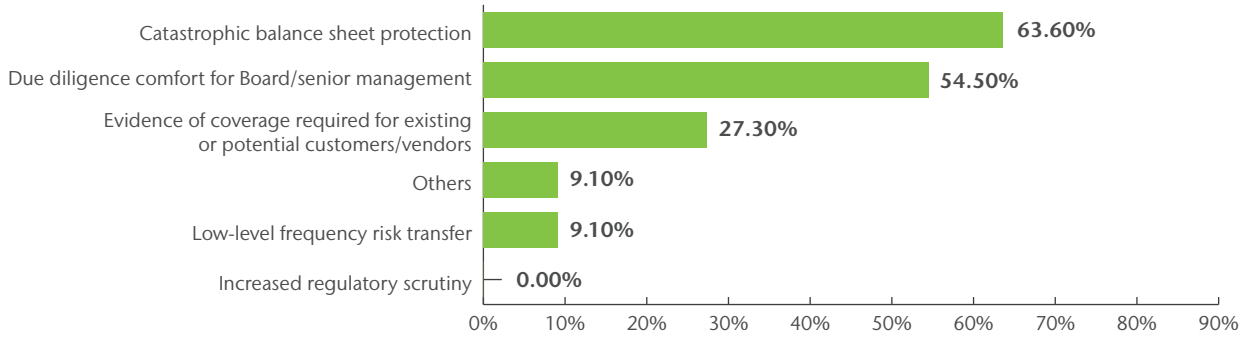
Product risk



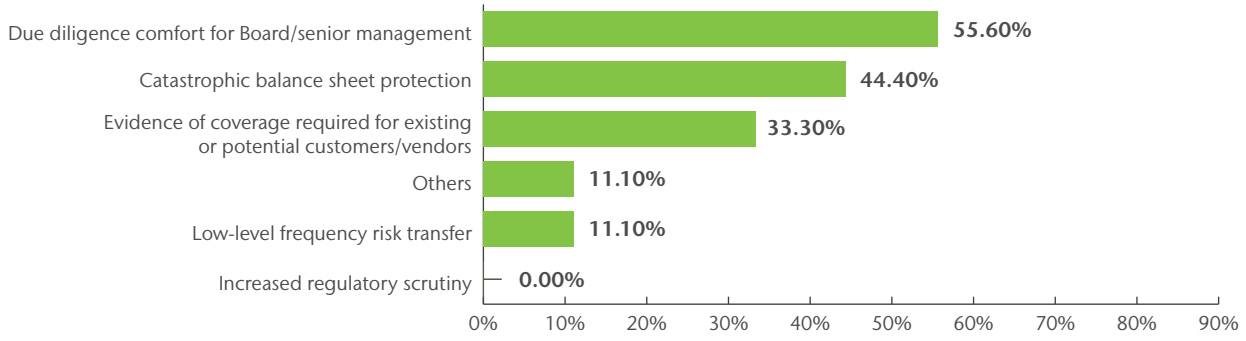
Critical infrastructure



Transport



Heavy industry



Cyber insurance purchase

Do you currently buy cyber coverage?

Despite the growing frequency and scale of cyber attacks and increasing management focus, more than half of surveyed companies do not buy cyber insurance. Of those, 40% of larger companies purchase cyber coverage. The situation is relatively better for smaller companies, with 55% buying cyber cover.

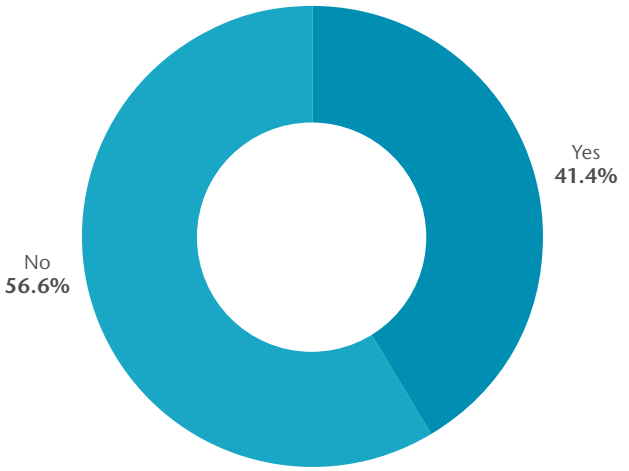
Such a discrepancy could be driven by the fact that large companies maintain well-funded IT security programs and leadership exhibits more confidence in their ability to effectively prevent cyber attacks.

Other factors leading to low take-up include the absence of meaningful capacity for larger companies, the inability to buy coverages most sought after (e.g. business interruption and contingent business interruption), pricing, and uncertainties surrounding the insurance industry's willingness to pay claims in untested waters.

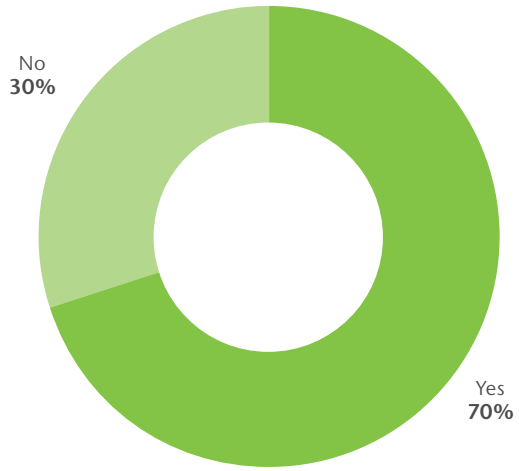
For smaller companies, a breach could have a more material impact. Of course, such purchasing patterns are evolving and reflect the correlation of cyber exposures to a frequency and severity analysis, which determines whether, and to what extent, cyber exposures impact the financial state of an organization.

Over the past two years, the healthcare, retail, and financial services industries have been targets of massive attacks by cyber criminals. That explains why 70% of respondents from these industries purchase cyber cover. This also corroborates other studies, which show that these three industries are more advanced in their understanding and risk management approach to cyber threats. Going forward, the healthcare, retail, and financial services industries could well be the leaders who influence coverage and limits.

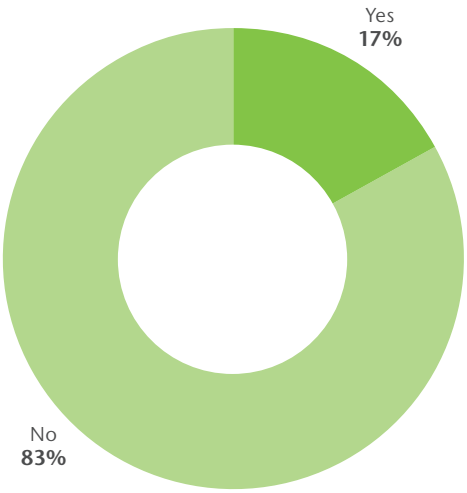
Overall



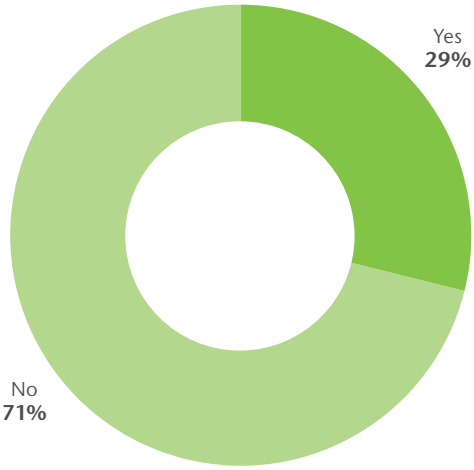
Data holders



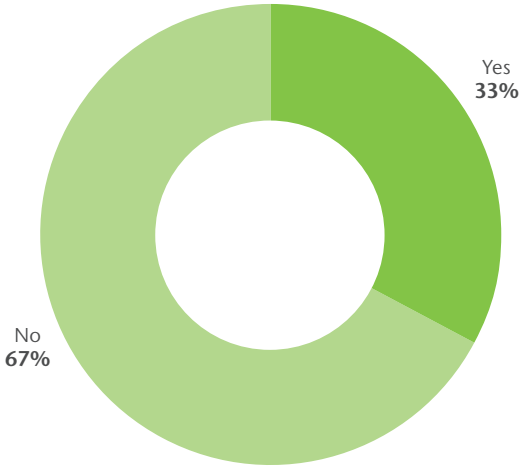
Product risk



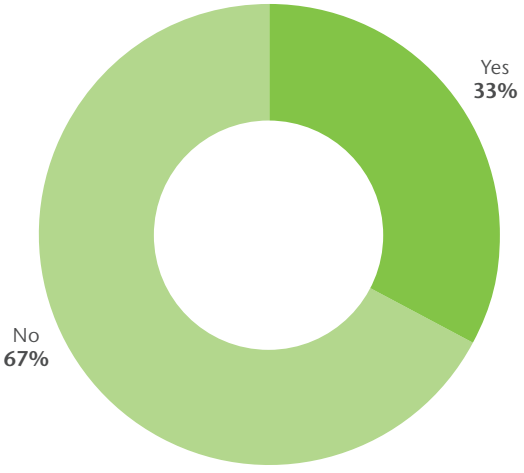
Critical infrastructure



Transport



Heavy industry



Budget considerations

Is the expense for cyber insurance currently in budget?

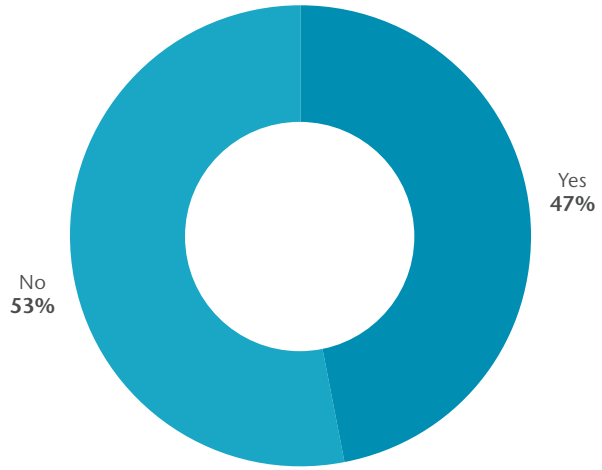
Only 47% have reported including cyber premium in their budget. As is consistent with the previous response, 40% of larger companies have budgeted for cyber insurance. Only nine percent of the transport respondents say they budget for cyber insurance, the lowest among all groups.

This may be due to the fact that because a large percentage of surveyed companies with revenue size of above USD 5 billion fall in the categories of pharmaceutical, chemical, energy, aviation, and food and beverage, their chances of exposure to cyber attacks are currently smaller than those for the healthcare, retail and financial services industries . Moreover, the larger the revenue size, the greater the ability to absorb any risk management cost. Therefore, many of these companies have not yet determined a need to buy cyber insurance.

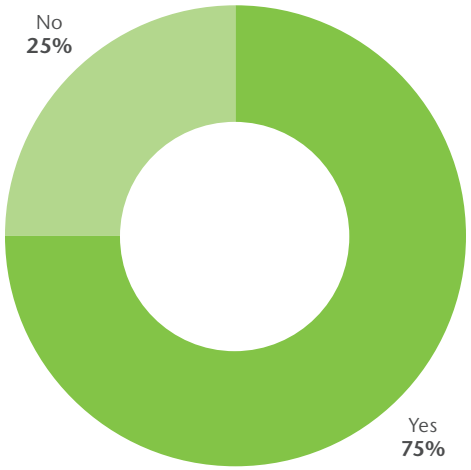
However, the lack of budget for cyber-related expenses could suggest a concerning level of unpreparedness for the company. The massive, well-publicized attacks against large companies over the past two years show that false complacency could lead to tremendous damage to a company's bottom line. As hackers and IT professionals remain locked in a fierce arms race, this risk, which is still not fully understood, will keep growing.

Other factors leading to low take-up include the absence of meaningful capacity for larger companies, inability to buy coverages most sought after (e.g. business interruption and contingent business interruption), pricing, and uncertainties surrounding the insurance industry's willingness to pay claims in untested waters.

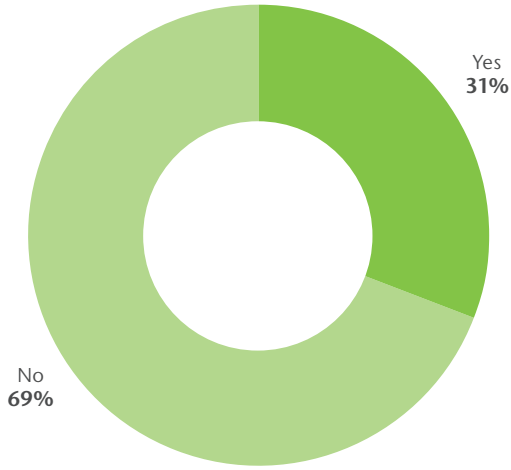
Overall



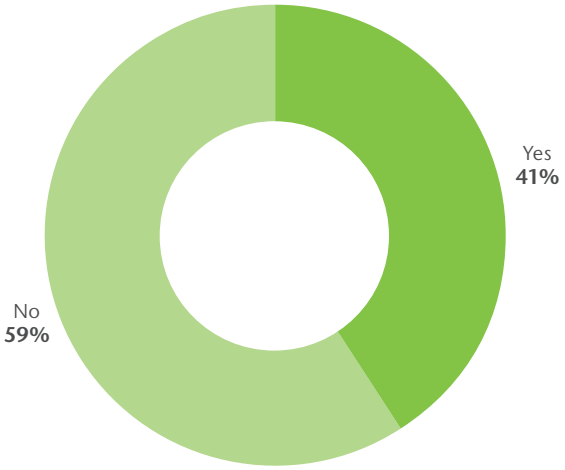
Data holders



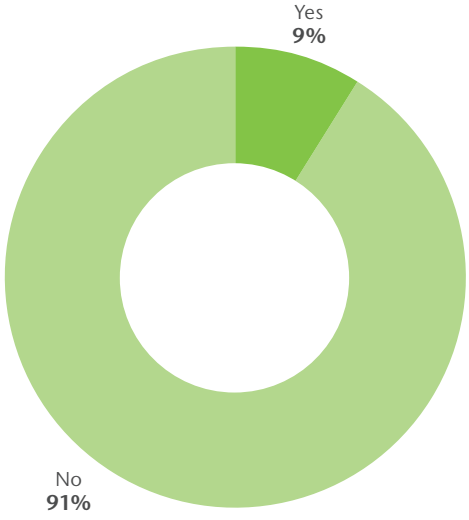
Product risk



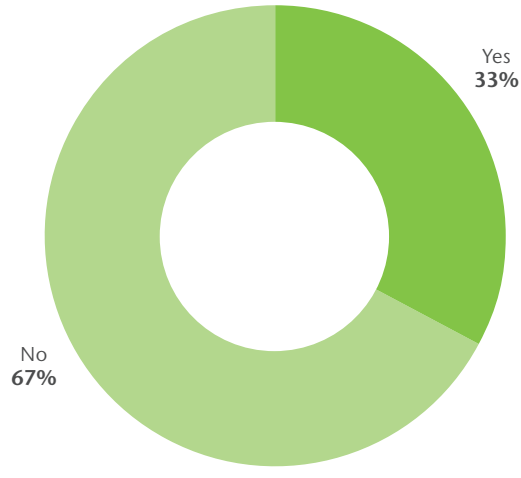
Critical infrastructure



Transport



Heavy industry



Policy Cover and Structure

Cyber Risk in the market place

What do you perceive as the greatest issues in the cyber risk market place?

About 71% of surveyed companies have listed terms and conditions as their most important issue in the cyber risk market place, followed by pricing (48%).

It is unsurprising that terms and conditions are listed as the greatest issue in the cyber risk market place, due to lack of consistency among markets and the immaturity of the product.

There are over 60 different cyber insurance carriers, all with different cyber insurance policy terms and conditions. As cyber insurance has only been available for the last 15 years, it has not yet developed into a mature product. There is a great deal of variation in scope of coverage, policy triggers, definitions and exclusions.

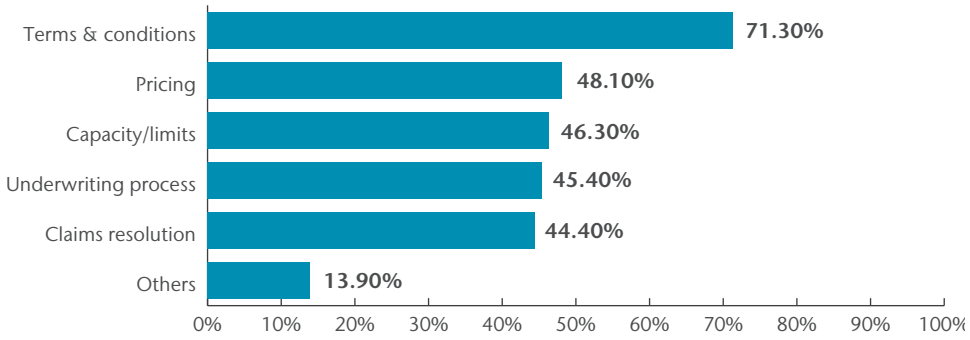
Given the "gap" nature of a cyber insurance policy, it is important to understand what coverages are available to address cyber risk, while also understanding what elements of cyber coverage may be available under in force policies. While generally cyber insurance policies do not address property damage or bodily injury perils, these coverages may be addressed by an organization's property or general/excess liability policies. However, there is a great deal of inconsistency in how property and general/excess liability insurance carriers address (or do not address) losses arising from a network security breach. The insurance industry has yet to provide a comprehensive "all-risk" cyber insurance solution.

Similarly, concerns around pricing are understandable. Pricing varies widely by industry and continues to rise in the wake of significant breaches. While double-digit increases are being experienced across the board, more significant increases are being experienced in loss affected industries. Renewal premiums continue to increase even for insureds with no change in exposure profile.

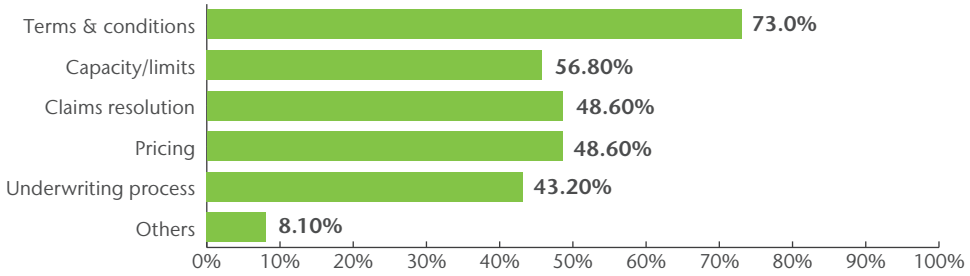
Larger companies see capacity limits as their third most important issue, whereas smaller companies are more concerned about the underwriting process.

The underwriting process for cyber insurance requires a deep-dive into network security controls for an organization. In addition to completing an application, companies may need to engage with underwriters in a conference call or meeting in order to discuss key areas of risk such as network security controls, vendor management, business continuity and incident response planning. In addition to the Risk Manager, multiple stakeholders within the organization may need to be involved in the underwriting process, including individuals from Information Technology / Security, as well as the Legal Department.

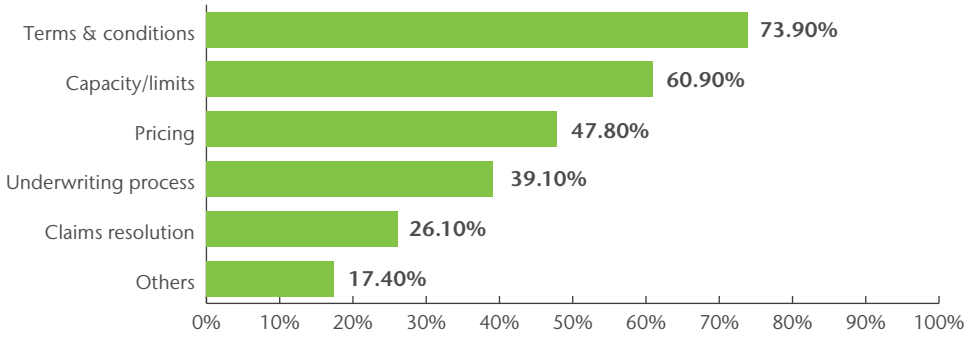
Overall



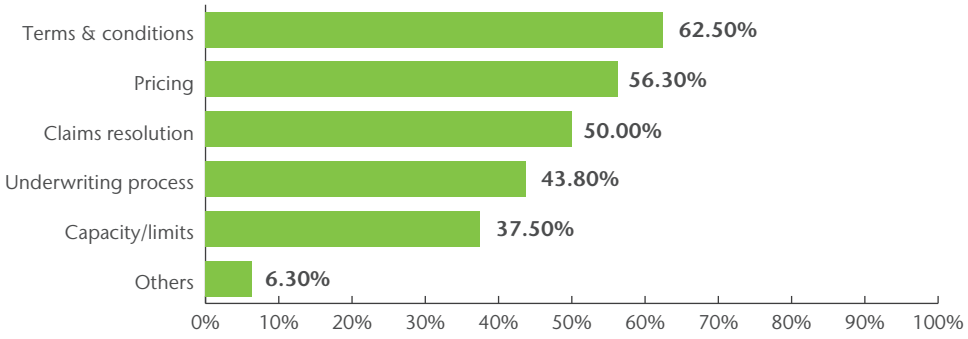
Data holders



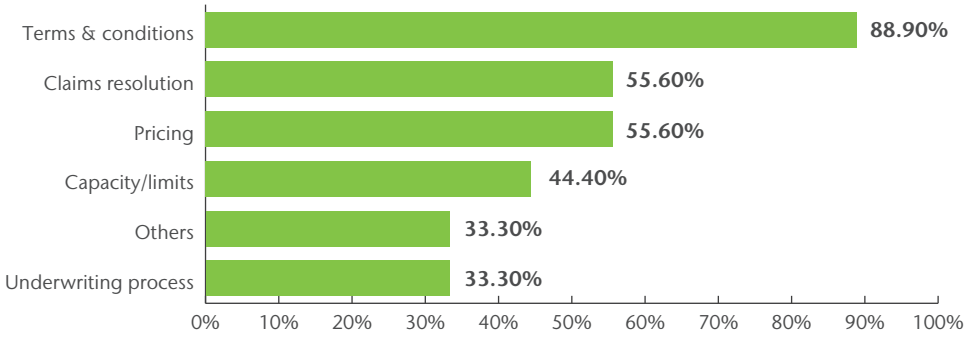
Product risk



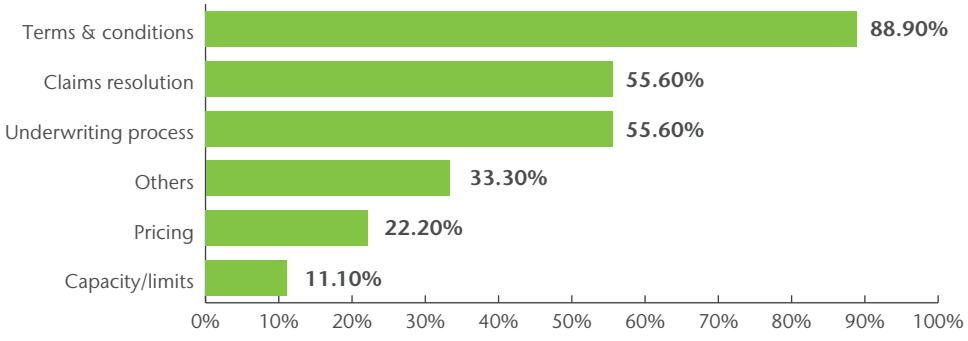
Critical infrastructure



Transport



Heavy industry



Most frequently cited limit range

Cyber cover limit ranges selected by all respondents

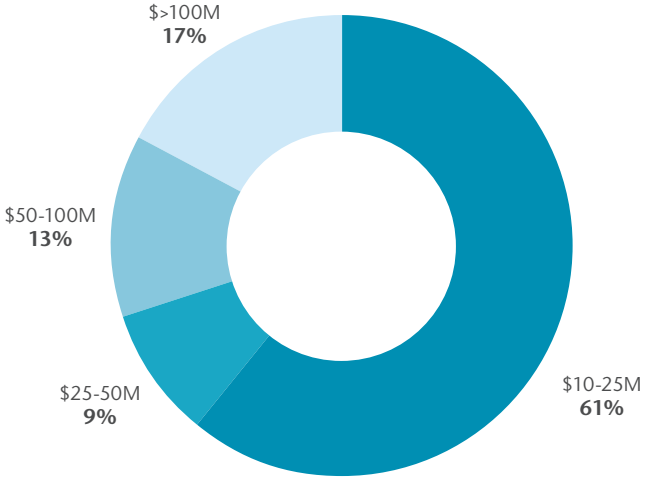
For all respondents, the most frequently chosen limit range stands at USD 10 million–25 million (61%). However, in the large company group, there is no clear majority. About 36.3% of respondents have chosen the USD 10 million–25 million range, while 17% have picked the above USD 100 million category.

By industry, 80% of the critical infrastructure respondents who represent large utility, energy, oil and gas, and petrochemical companies say they have purchased limits of above USD 100 million.

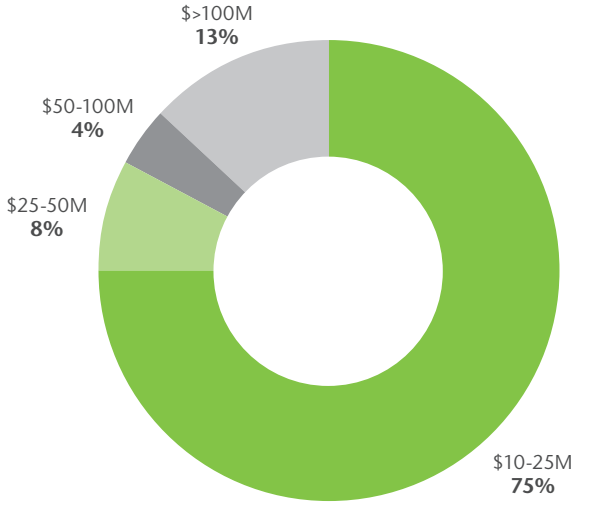
Cyber limits are available between USD 200 million–USD 300 million through the traditional insurance markets. While the majority of entities purchase USD 1–5 million or USD 20–50 million, we can see a trend for dramatically higher limits in 2016 as more breaches are reported. The demand for an alternative limits solution is growing fast.

As the complexities of cyber risk increase, the insurance industry could face the potential danger for a cyber hurricane—an event that could potentially impact multiple lines of business, geographies, and industry sectors. This could signify major challenges, since we may see the first multi-billion dollar cross- class cyber event, which will emphasize the need for higher limits.

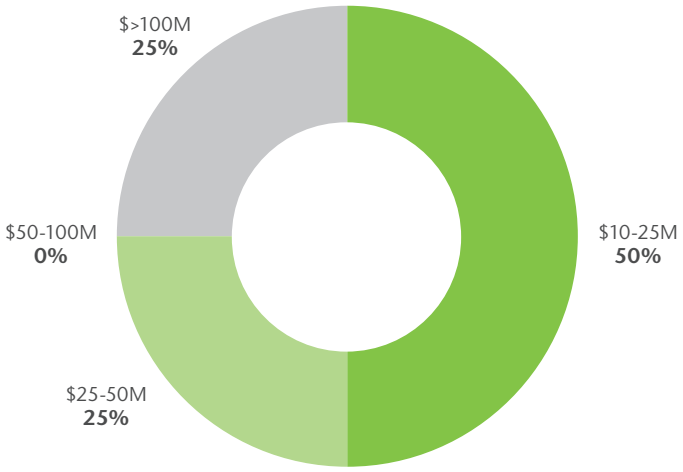
Overall



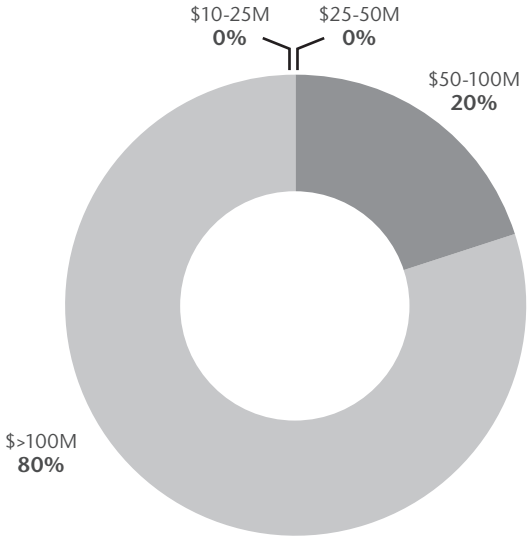
Data holders



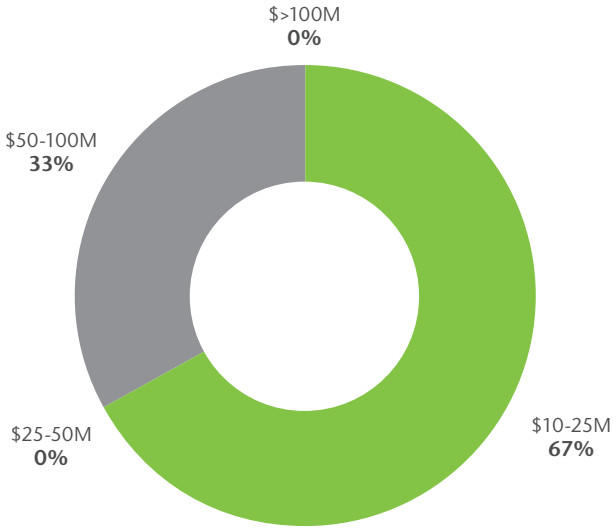
Product risk



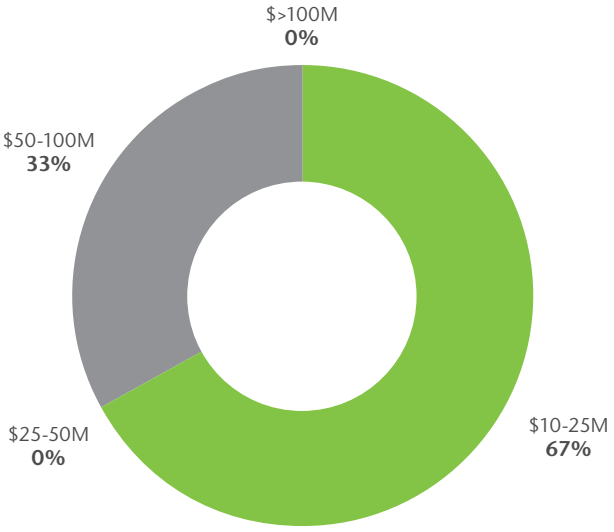
Critical infrastructure



Transport



Heavy industry



Retention levels

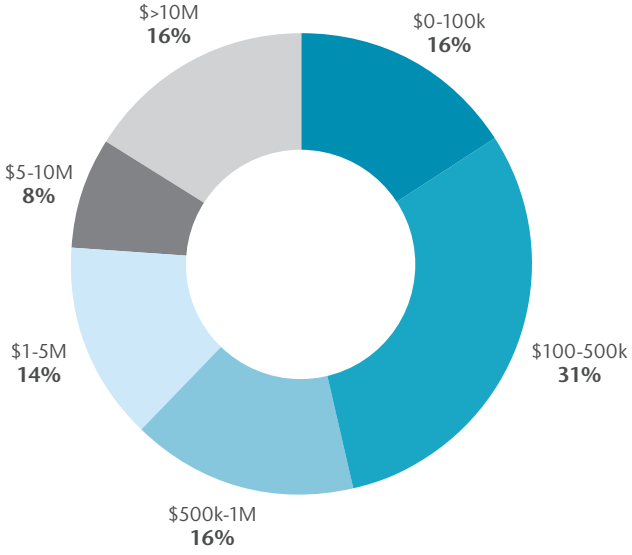
Retention limits selected by all respondents

On average, the most frequently selected retention level for all companies ranges from USD 100,000 to USD 500,000. Understandably, a high percentage of smaller companies, 46%, have picked this range. The indication for larger companies is not clear: 28% have chosen the above USD 10 million range; and 24% have selected the USD 1 million–USD 5 million level.

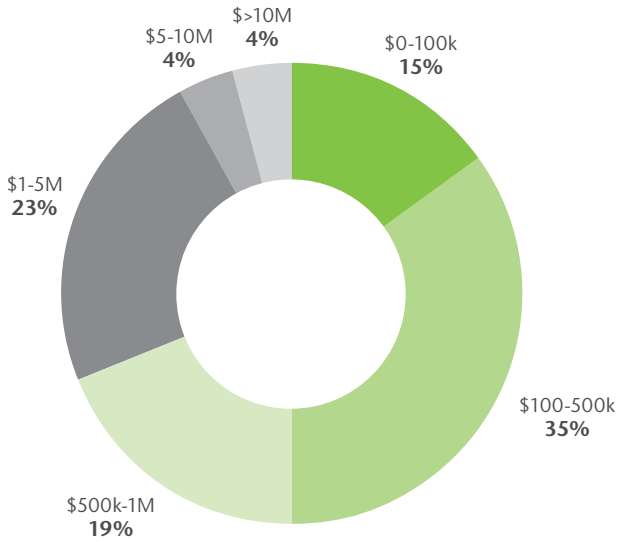
As inconclusive as they are, the data have highlighted the uncertainties relating to the possible impact of cyber risk. Organizations need to consider cyber assets and exposures in the context of financial statement impact as compared to historical tangible assets and exposures. While a cyber attack often causes disruption to business and IT operations, catastrophic cyber losses can also result in potential directors' and officers' liability allegations.

With cyber risk constantly evolving, insurance carriers might also require a higher retention amount in the near future. It seems, though, that insurers are greatly restricting coverage at lower retention levels by introducing exclusions and sub-limits. Due to the fact that wording details are critical to having a claim paid, there is often a trade-off of higher retention in order to maximize coverage—otherwise there could be critical coverage shortfalls.

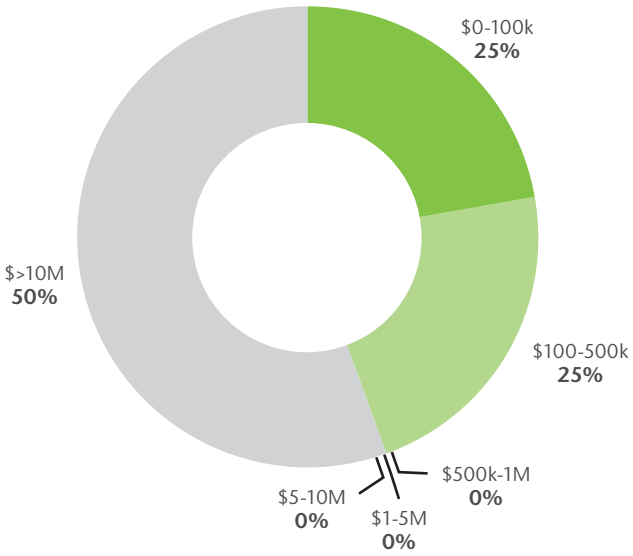
Overall



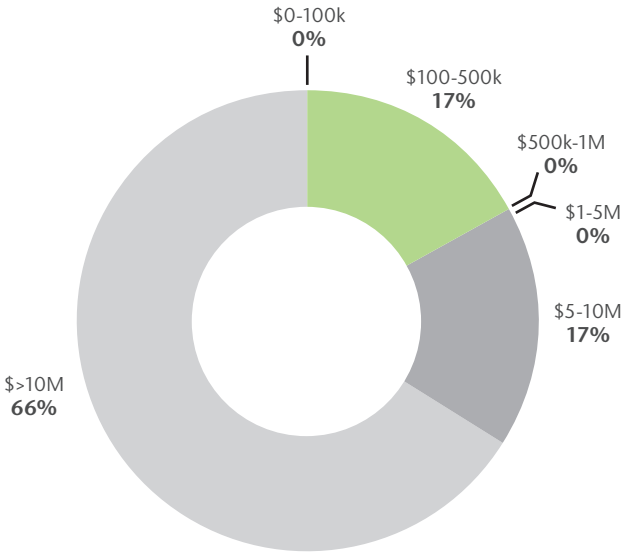
Data holders



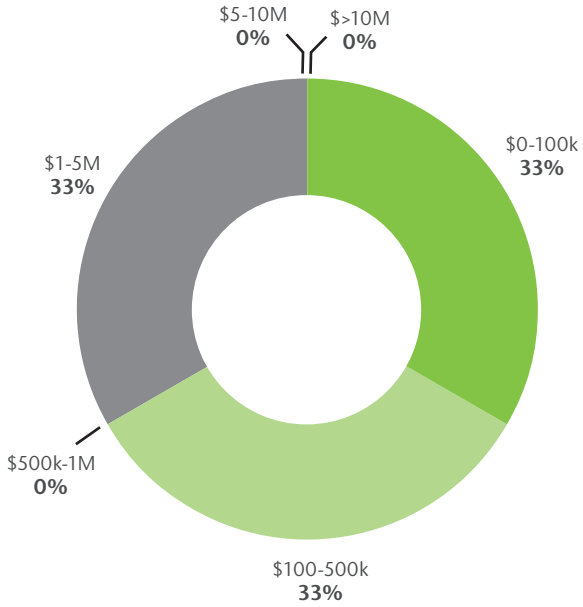
Product risk



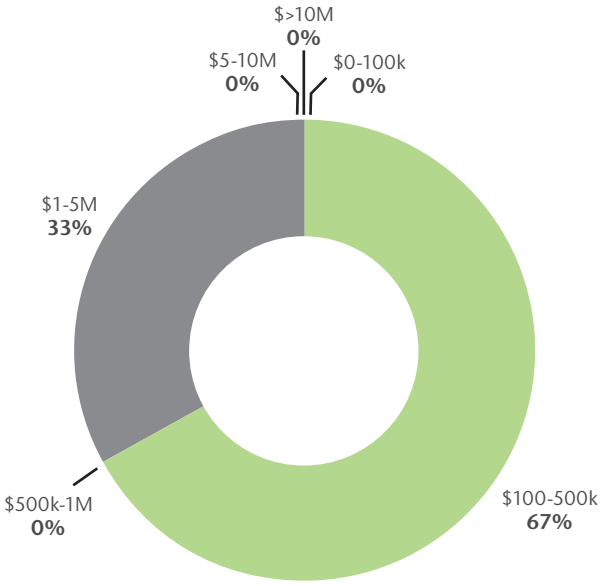
Critical infrastructure



Transport



Heavy industry



Estimating premium

How did you arrive at the quantum for cyber risk?

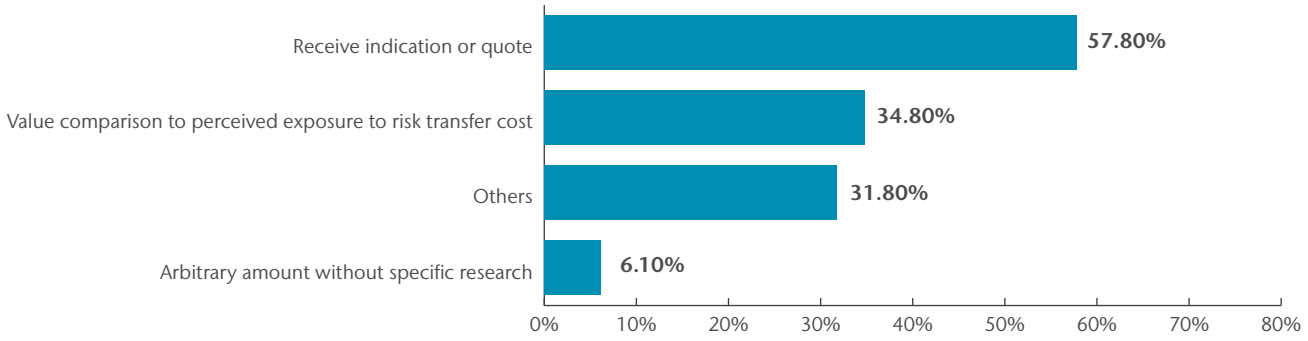
Across all industry groups, the majority of respondents (59%) have arrived at the premium estimate by receiving market quotes.

If broken down by revenue size, a higher percentage of smaller companies (77%) put market quotes as the most frequent means in estimating premiums, followed by value comparison of perceived exposure to risk transfer.

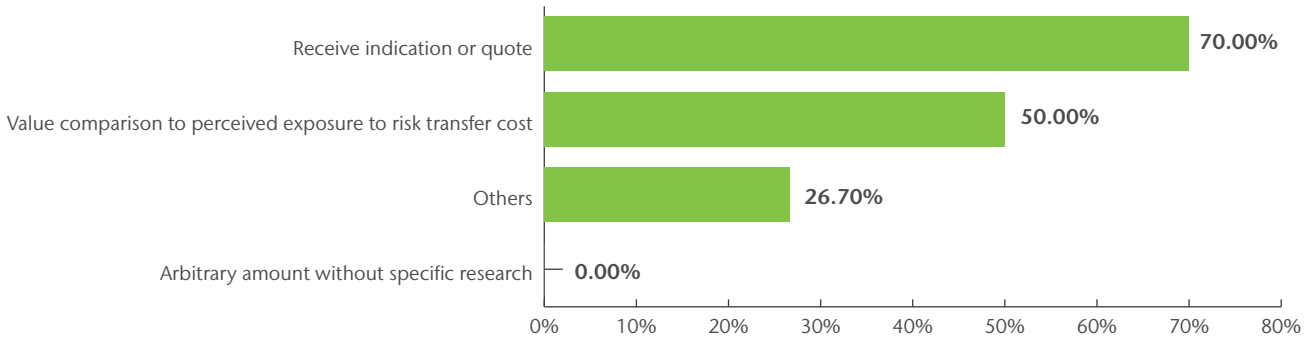
As historical data on cyber exposures and necessary limits are not readily available, particularly with respect to cyber-driven business interruption, it is no surprise there is no clearly preferable method of arriving at the quantum for larger companies, which estimate their premiums by utilizing peer benchmarking, receiving market quotes, and/or completing a value comparison of perceived exposure to risk transfer. However, as actuarial data is currently being collected, cyber benchmarking is improving.

Furthermore, risk management specialists, including Aon, are now partnering with internal modeling resources and third parties to conduct cyber evaluation and risk quantification assessments that can produce more accurate models for retentions, limits, and pricing. Organizations will be able to analyze the financial statement impact of various retention, limits, and pricing options from a Total Cost of Risk standpoint.

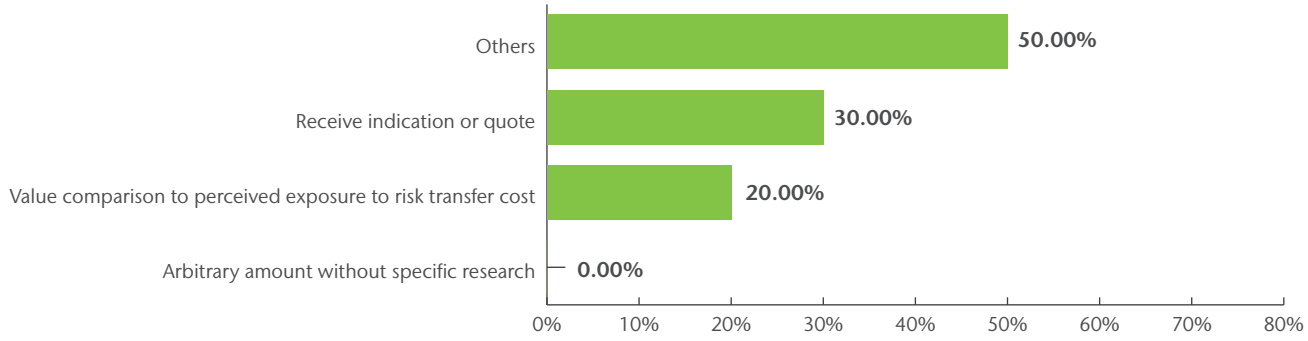
Overall



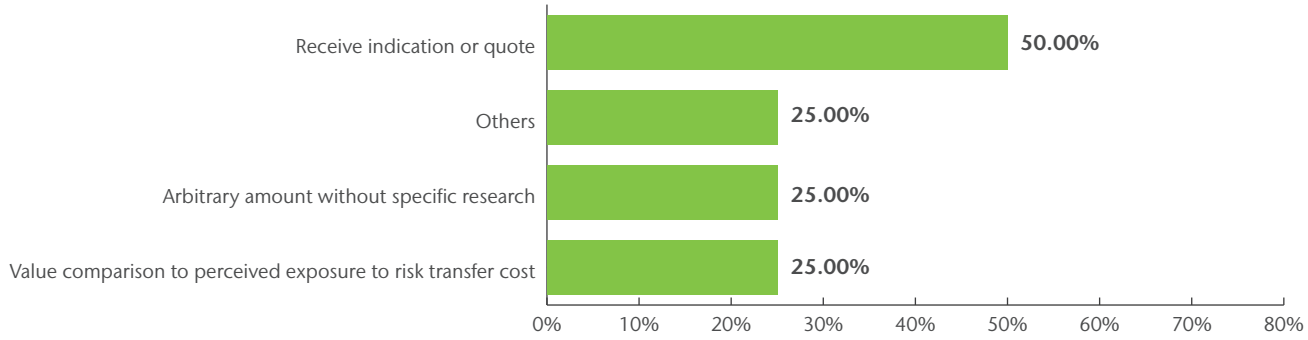
Data holders



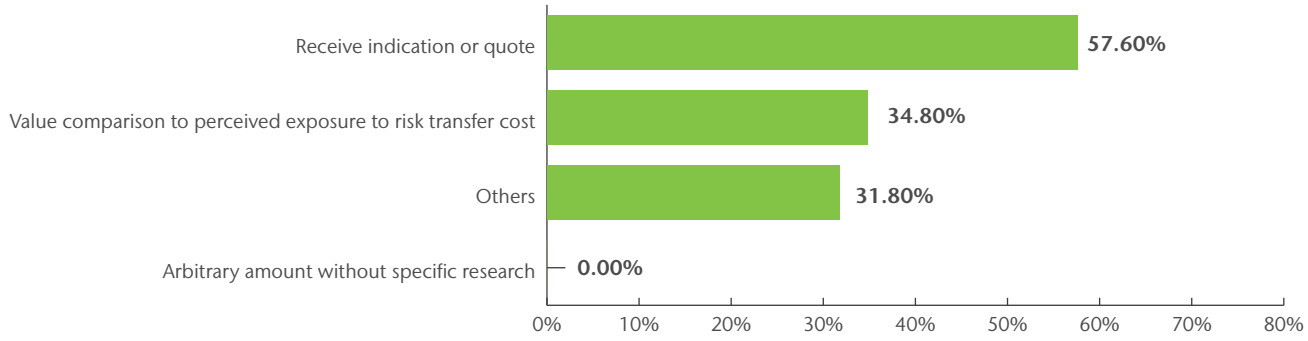
Product risk



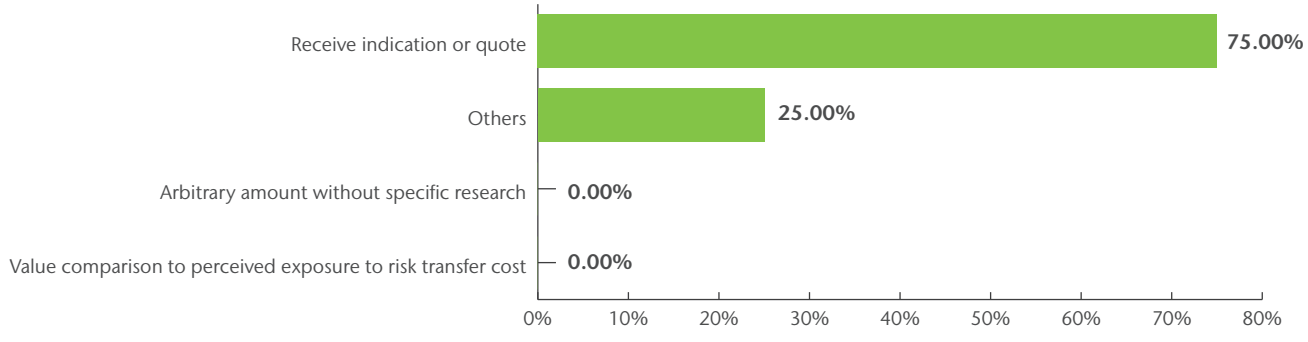
Critical infrastructure



Transport



Heavy industry



Retaining cyber risk in a captive

Assuming the availability of capacity through a dedicated captive facility, would you be willing to retain the self-insured layer in your captive?

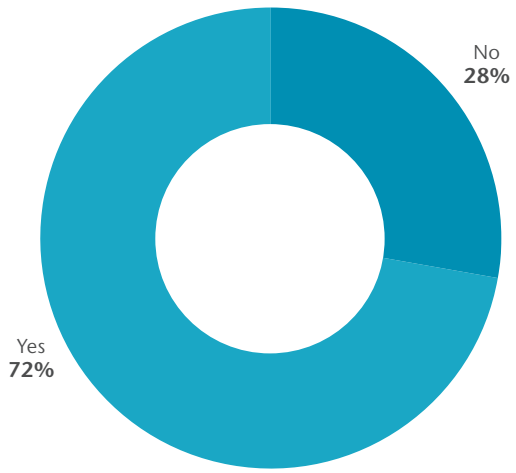
Historically, captive insurance companies have most often been used to underwrite property damage, workers' compensation, medical malpractice, and third-party liability risks. In **Aon's 2015 Global Risk Management Survey**, 8% of respondents have indicated interest in underwriting cyber risk in a captive, and that trend is projected to increase threefold in the next 5 years.

By including cyber risk in a captive, rather than simply self insuring the risk, the company has an opportunity to see how the risk will behave in a formal insurance structure subject to underwriting and claims adjustment disciplines. Over time, that experience and data can be used to negotiate program structure with insurance carriers and inform cost allocations of cyber loss.

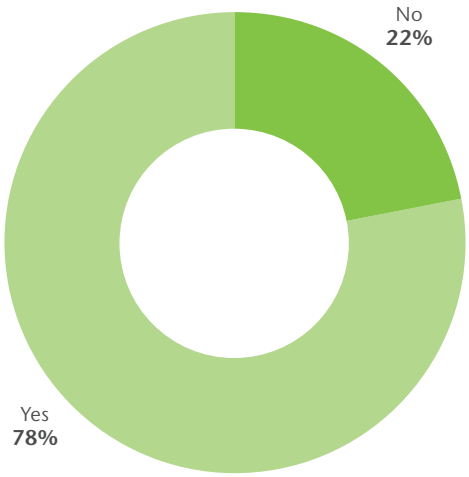
Insureds place cyber exposures in captives for four different reasons:

- In-fill program for high deductible cyber or professional indemnity program
- Using the captive to retain the primary layer of risk
- Using the captive to access re-insurance capacity
- Using the captive to incubate where broad coverage is currently unavailable

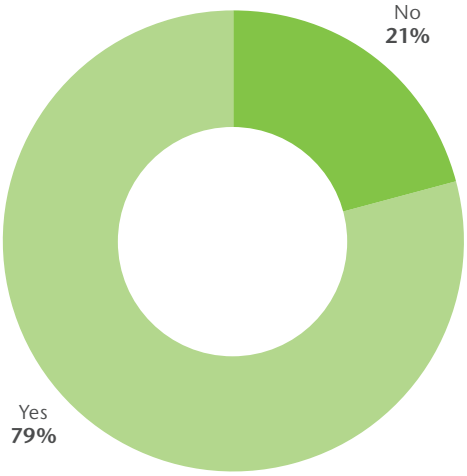
Overall



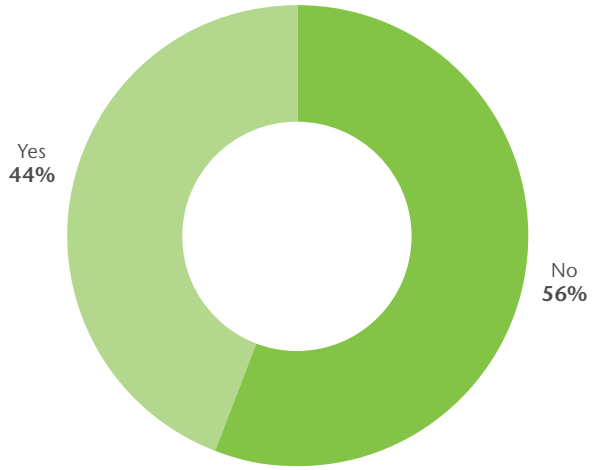
Data holders



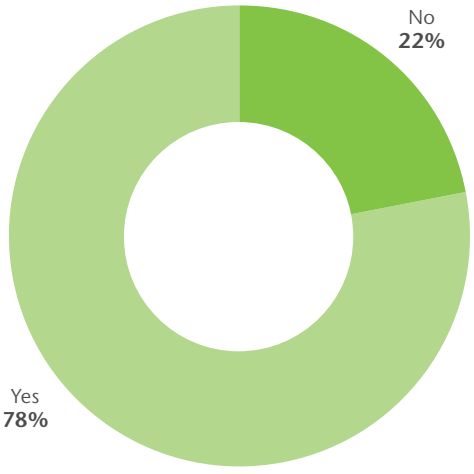
Product risk



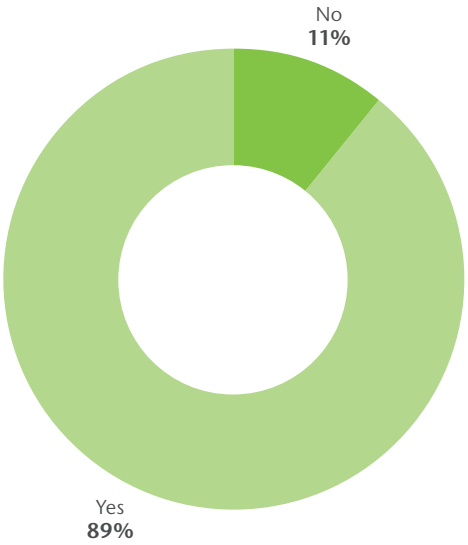
Critical infrastructure



Transport



Heavy industry



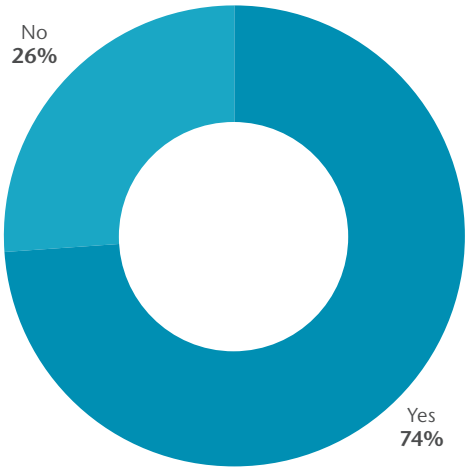
Risk sharing/pooling

Would you be willing to share risk with other companies in your industry as part of a captive facility dedicated to writing cyber risk, assuming you were comfortable with the underwriting process?

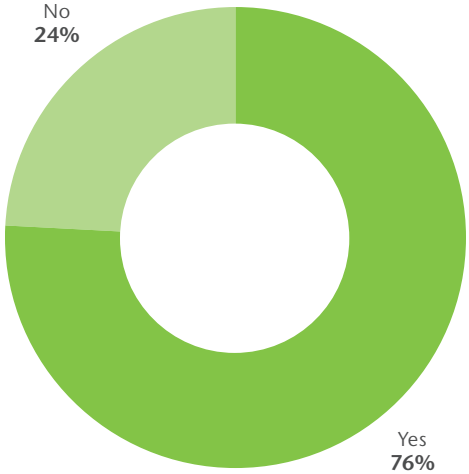
Regardless of company sizes, an overwhelming majority of respondents (94%) have said "yes" to the question, depending on the scope of coverage (56%) and limit size (37.6%).

At the same time, one-third of participants have indicated they would never share risk. At a time when governments are pushing for centralized information-gathering databases, such as the U.S. Information Sharing and Analysis Centers, many organizations are reluctant to join up and voluntarily share critical vulnerability information in the wake of the Edward Snowden revelations relating to the US government's overarching surveillance programs.

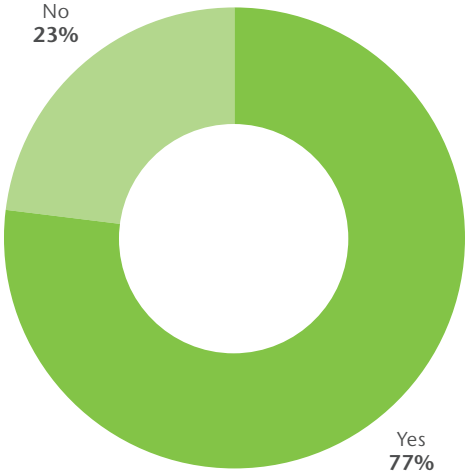
Overall



Data holders

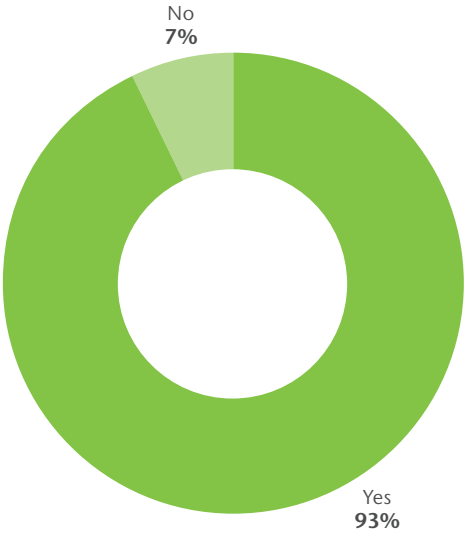


Product risk

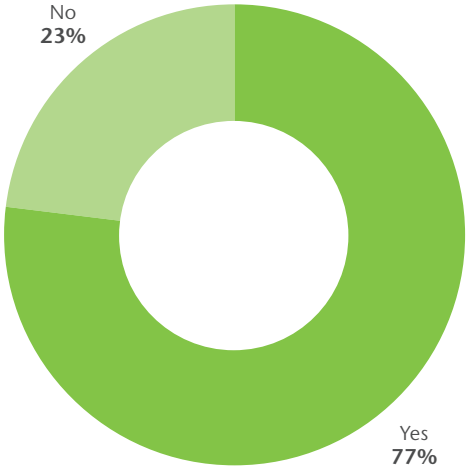


Critical infrastructure

Transport



Heavy industry



Loss adjustment process

Are you concerned that claims arising from cyber coverage will be adjusted and paid fairly?

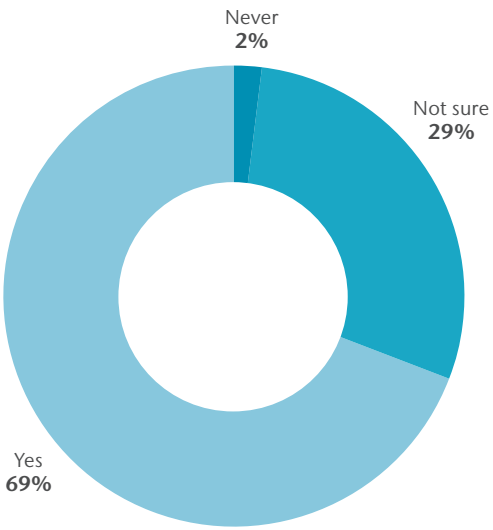
Across industry, 67% of surveyed companies (75% of larger companies) have expressed concern about the existing loss adjustment process and the capacity of the existing system being adapted to complex cyber risks. With disputes involving coverage interpretation and quantum often the rule rather than the exception, policyholders are confused and disappointed by a process that takes too long and does not live up to recovery expectations.

The high rate of concern regarding claims handling reflects understandable uncertainties regarding the ability of cyber insurers to meet buyer expectations. Where will first- and third-party cyber provisions fit in the existing portfolio of insurance? Will the cyber policy sit in a primary or excess position? Are coverage terms and conditions fully understood? In the absence of legal precedents, how will coverage provisions be interpreted in a loss adjustment? What will be required to establish causation and its nexus to actual damages, such as business interruption? Do cyber insurers employ or retain competent adjustment and quantum experts capable of sorting through complex IT, process, and financial issues? Will cyber insurers invoke a reasonable standard of proof for loss adjustment?

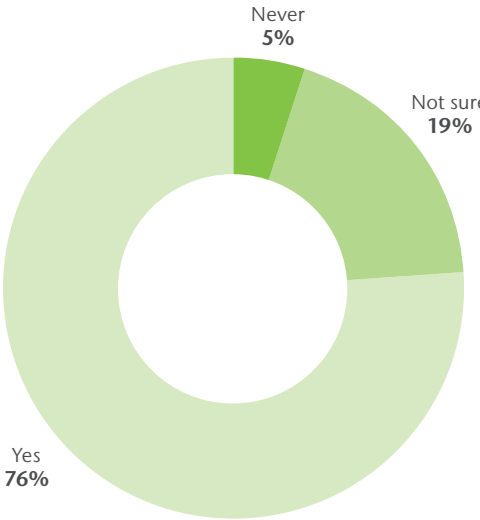
These questions should be expected with the introduction of any new insurance product; however, cyber coverage, given its potential breadth and significance in both first- and third-party realms, requires a more comprehensive inquiry. Risk managers need assurance that when a claim occurs, their coverage will respond fully and timely.

It is advisable for companies to engage an experienced claims management and settlement expert in the process.

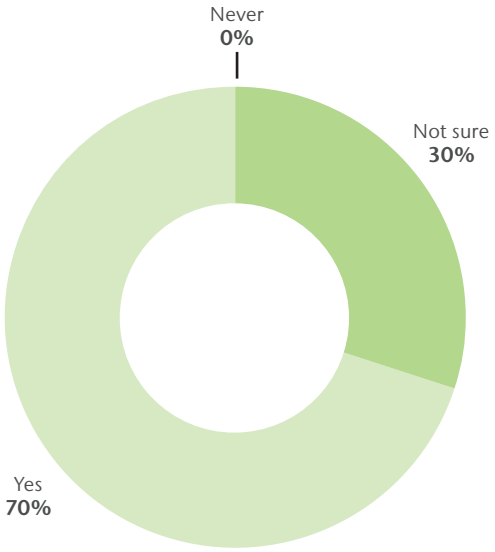
Overall



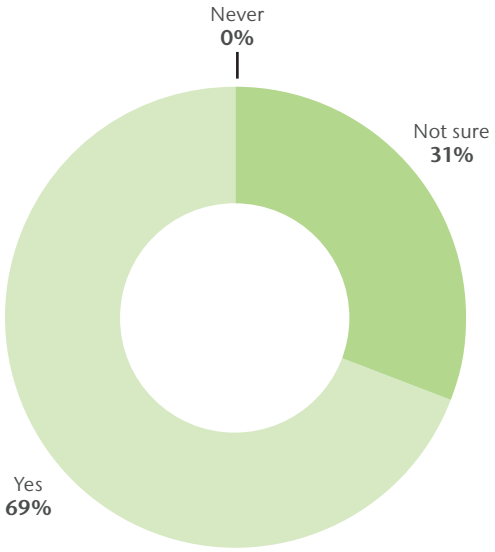
Data holders



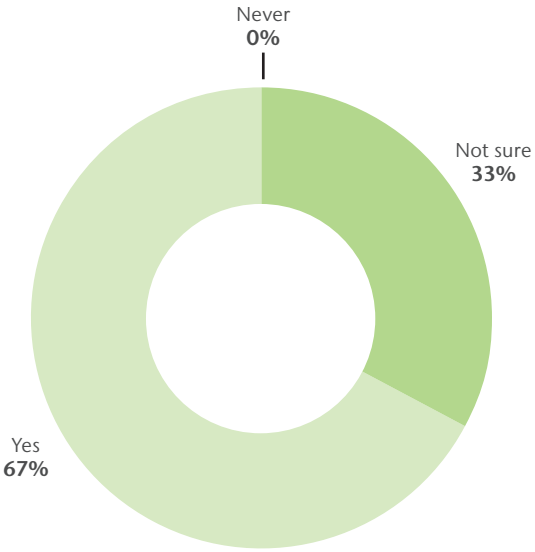
Product risk



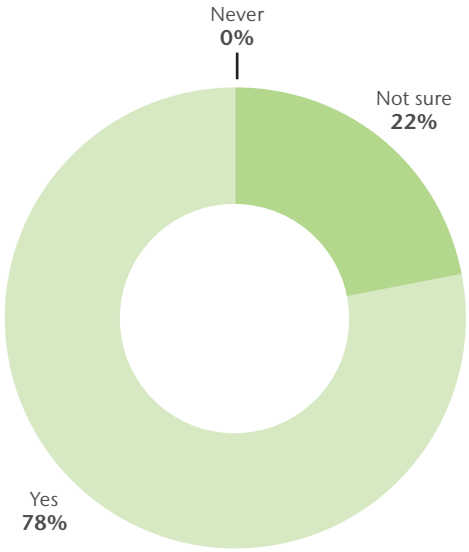
Critical infrastructure



Transport



Heavy industry



Steps to ensure a fair claims process

What steps should cyber underwriters take to ensure a fair claims process?

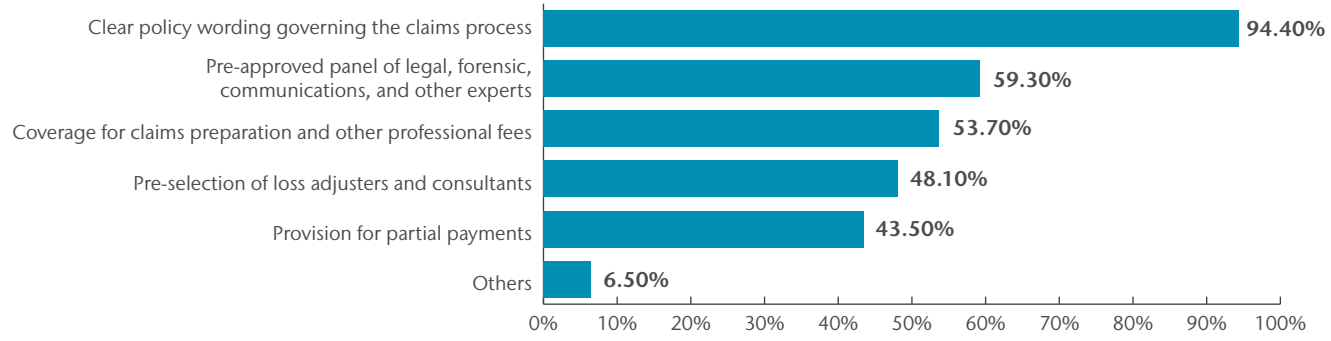
Unsurprisingly, 94.4% of respondents have listed clear policy wording governing the claims process as the number one-step for underwriters to ensure a fair claims process. The second most-selected option was a pre-approved panel of experts, at nearly 60%. For smaller companies, coverage for claims preparation ties for the second place. Larger organizations have listed pre-selection of loss adjusters and consultants as the third.

The results indicate that cyber insurance as presently constructed—containing elements of first- and third-party coverage—poses unique claims challenges. So far, there haven't been any over-arching solutions. While third-party liability claims understandably require the involvement of legal counsel, first-party claims are often resolved by adjusters and experts, who act without counsel. Yet with cyber, both types of claims can arise from the same event, which begs the question: Will attorneys run the cyber claims process?

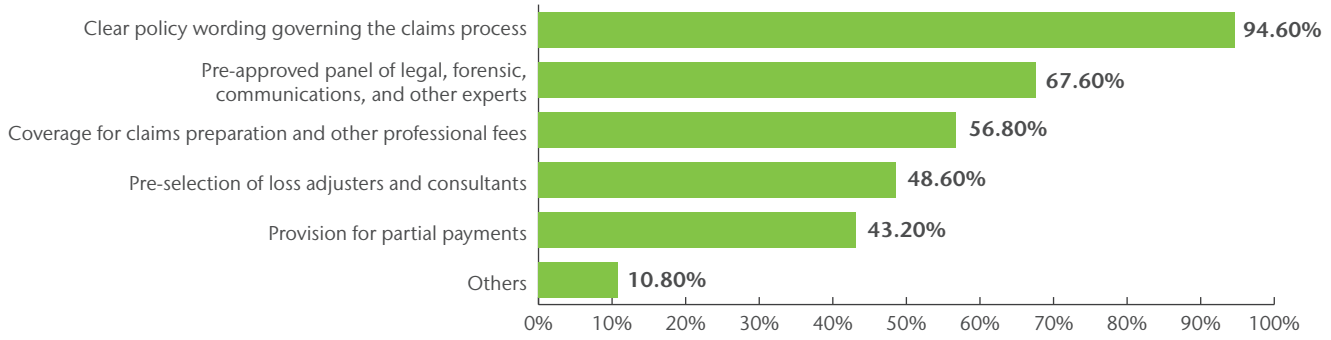
For the cyber insurance market to reach a fair claims process, reasonable claims protocols must be adopted. These protocols should address the fundamental roles and responsibilities of all parties, codes of communication and confidentiality, cover processes regarding the establishment of appropriate reserves and advance payments, and establish reasonable milestones and settlement timetables.

Although claims payment is ultimately the responsibility of underwriters, buyers and brokers alike play important roles in creating protocols that help achieve the expectations of all parties. This will likely take time, but establishing a claims-paying sensibility among cyber insurers now, built upon strong yet reasonable claims protocols, will go a long way toward alleviating the concerns currently exhibited by risk managers.

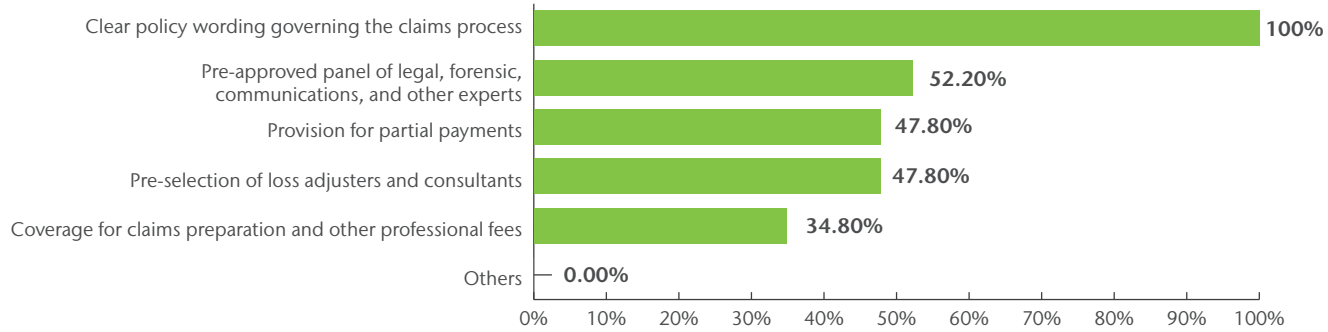
Overall



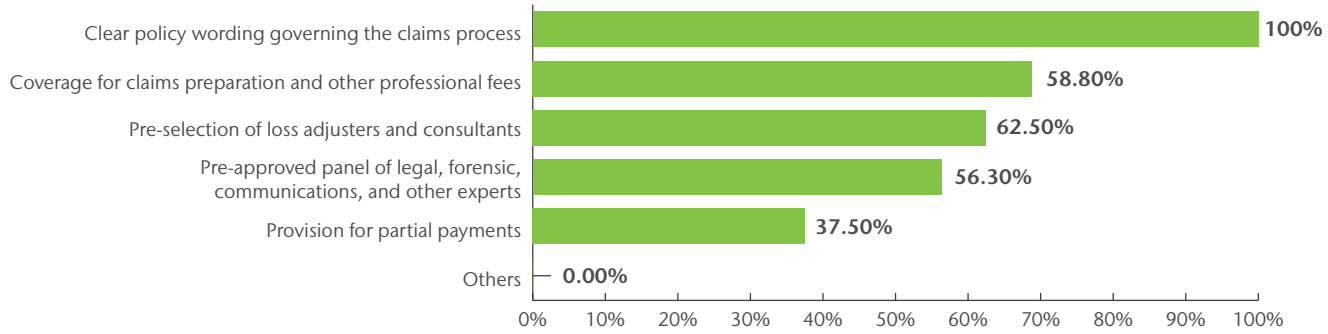
Data holders



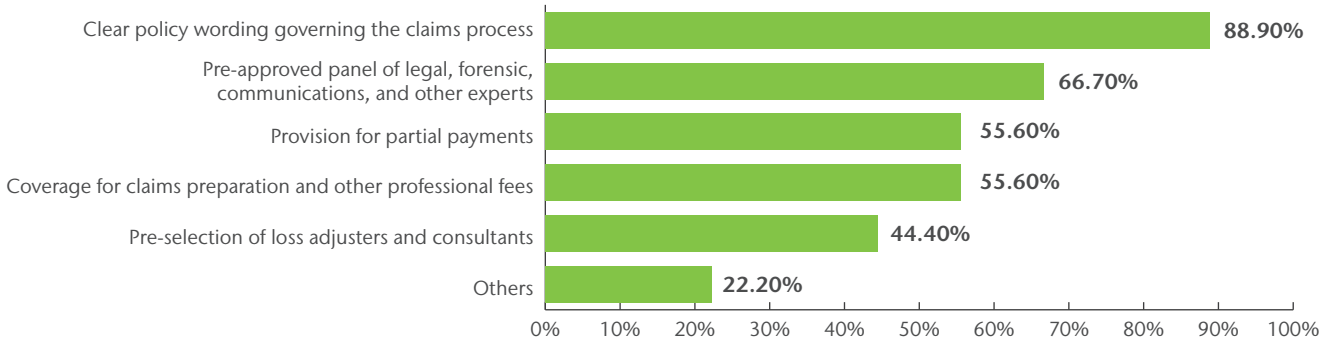
Product risk



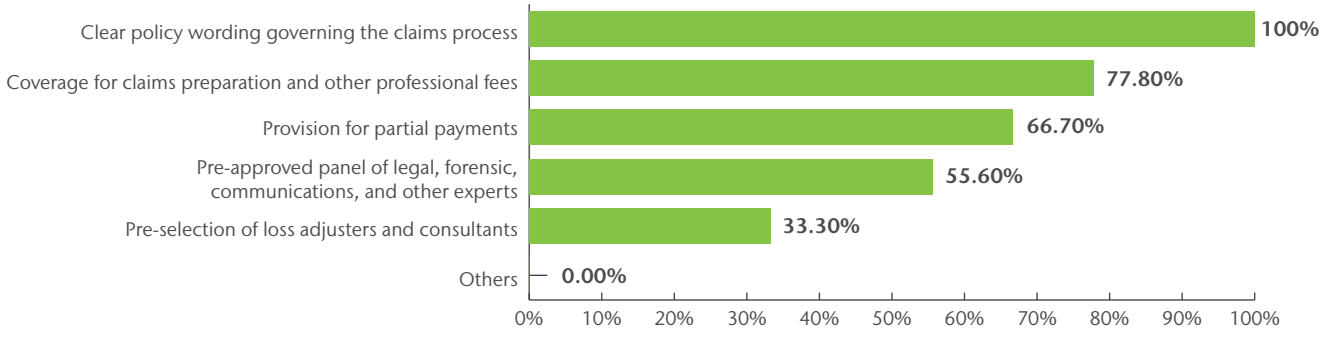
Critical infrastructure



Transport



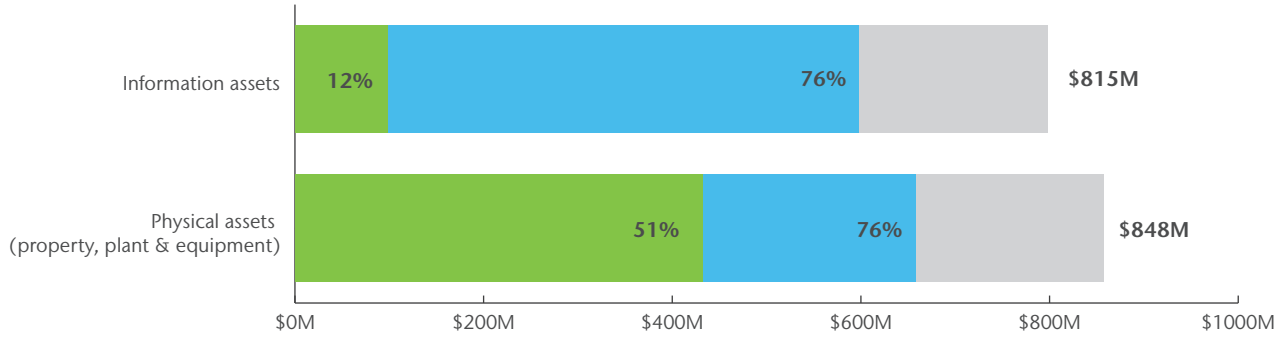
Heavy industry



Cyber Insurance Market Place

Snapshot in January 2016

Asset valuation, PML and insurance levels—Physical vs. information assets



In the wake of numerous publicly reported material incidents and analyses, cyber insurance sales are forecast to quadruple within four years. Insurance premium market size is currently estimated to be about USD 2.75 billion, of which about 90% will be in the U.S. In terms of growth, the premiums are expected to reach between USD 7.5 billion and USD 10 billion on an annual basis by 2020.

Currently, only about 12% of companies' information assets are covered by insurance, whereas 51% of their physical assets are covered. Such figures suggest significant room for the cyber insurance market to grow in the coming years.

Capacity has been fluctuating in 2015 both domestically and abroad

- While there are over 60 unique markets that can provide professional liability and/or cyber capacity, with new entrants in 2015, some markets have recently reduced capacity or have pulled out all together, while others have entered or increased their capacity
- Markets exist in the U.S. (primary and excess), the UK (primary and excess) and Bermuda (excess only)
- Of the available markets, there continue to be 4-5 Tier I markets for large complex accounts

Coverage continues to expand in both breadth and limit availability for middle market accounts, but not large accounts

- Carriers continue to differentiate their offerings with new/enhanced coverage components (Goodwill Coupon, Breach Response Services, PCI Coverage, etc.)
- Breach mitigation coverages continue to expand to meet clients' needs, including higher limits of coverage and the availability of coverage through a tower

Stronger data is being gathered as more breaches are reported

- There continue to be numerous reports of breaches as well as related additional data tracking costs
- Policies are responding, particularly to the breach mitigation, allowing better tracking of "claims" payments
- Heightened focus on IT security protocols and IT systems, especially relating to Point of Sale (POS)

Retentions remain stable and varied for middle market accounts, but some material increases for large accounts

- Retentions of all levels are available in the market, but vary based on industry class, revenue, and unique exposures, with recent market pressure to increase retentions, sometimes significantly
- Adjusting retentions can lead to more coverage/ sub-limit flexibility

Pricing continues to trend upwards

- Pricing continues to rise in the wake of significant breaches. While double-digit increases are being experienced across the board, pricing varies dramatically based on industry, size and scope of exposure
- Renewal premiums continue to increase even for insureds with no change in exposure profile

It is important to note that insurance carriers are limiting capacity and coverage and raising premiums for certain industry classes, such as large retail, healthcare, hospitality, and financial institutions.

Constraints in breadth of coverage and capacity for catastrophic cyber programs leave a gap in coverage that may require new or alternative risk transfer solutions. For example, catastrophic events could also lead to potential director and officer liability allegations, and these claims are generally not covered under standard cyber insurance policies.

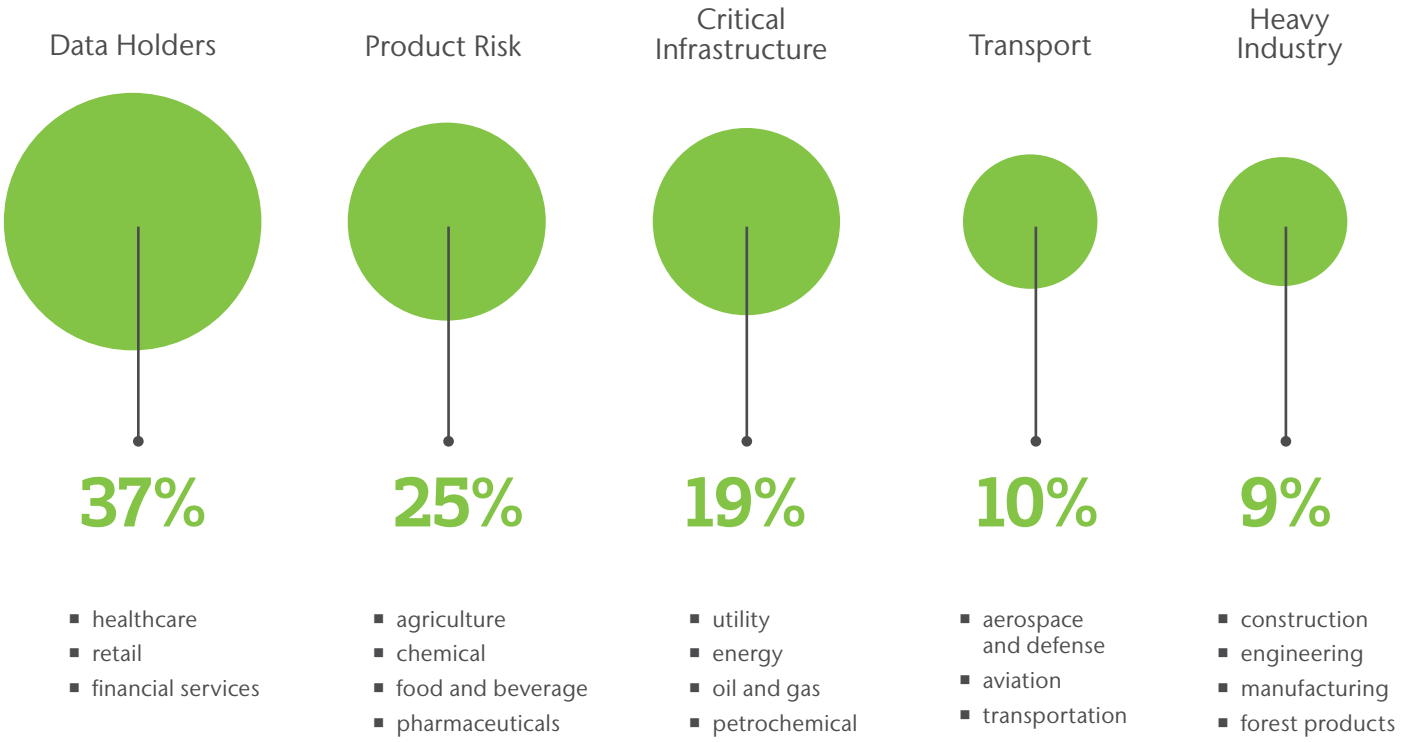
Brand and reputation, tangible property and bodily injury, all of which could be potential losses arising from a cyber incident, are also not addressed by many standard cyber policies. Moreover, the traditional cyber insurance markets run out of capacity at around USD 300 million. When new capacity becomes available, it often multiplies the pricing of existing coverage.

Key Findings by Industry

Key findings by industry

In an effort to provide insight and benchmarking tools for different industries, we have divided participants into five industry categories:

Survey respondents by industry categories

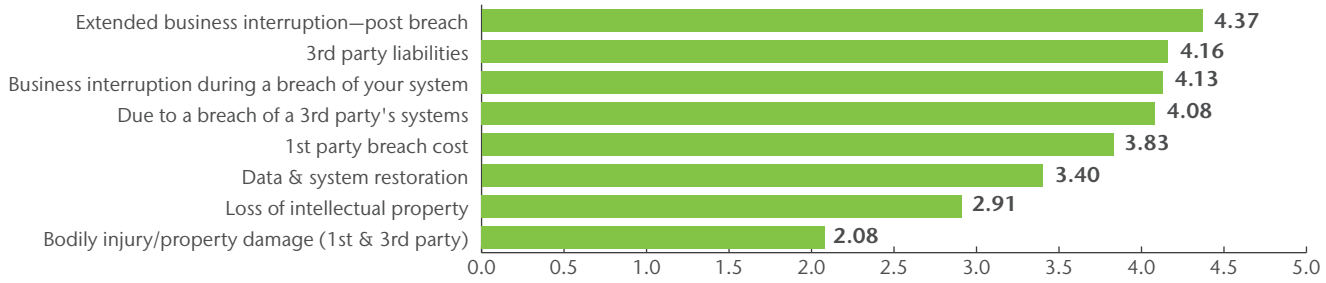


Data Holders

The data holders category, which has the largest number of participants, covers the healthcare, retail and financial services sectors. Half of the participants represent companies with revenues less than USD 5 billion and a quarter of the participants represent companies with revenues greater than USD 25 billion.

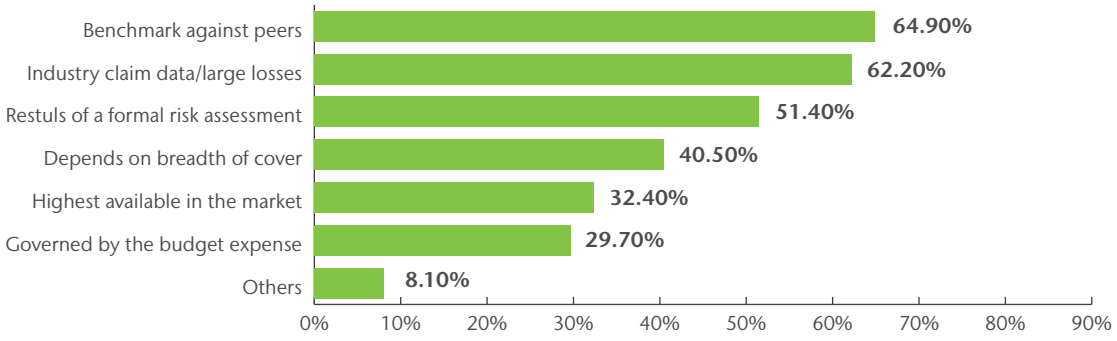
Cyber risk concerns

Which elements in cyber risk give you the greatest cause for concern?

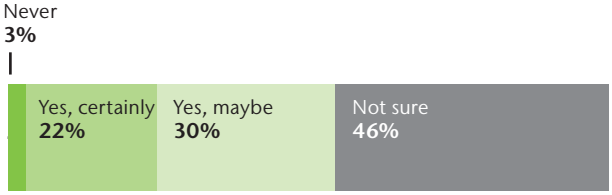


Risk assessment

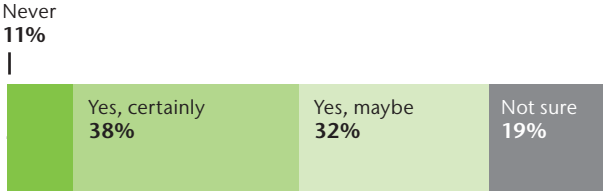
When deciding on total limits to insure, which factors influence the decision?



Based on the information currently available to you, do you know if your company complies with international best practices and standards governing information security (e.g., ISO 27001/002, NIST, or similar)?

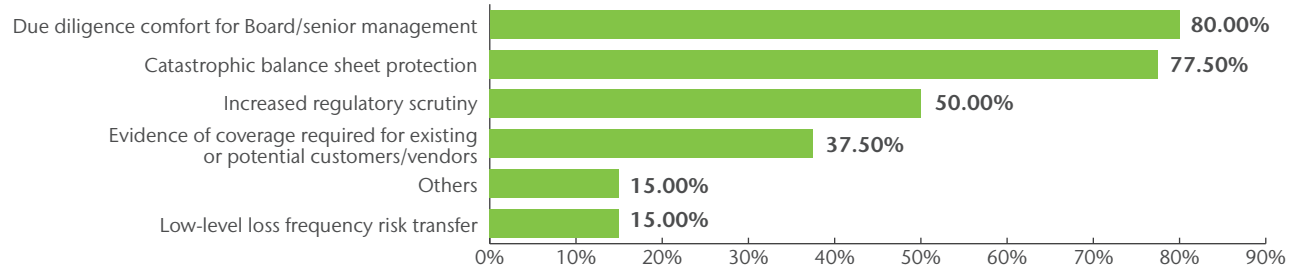


Would an independently administered cyber risk evaluation assist you in understanding and quantifying first and third party cyber exposure?



Attitudes toward cyber insurance

What are your main reasons for purchasing or considering cyber insurance?

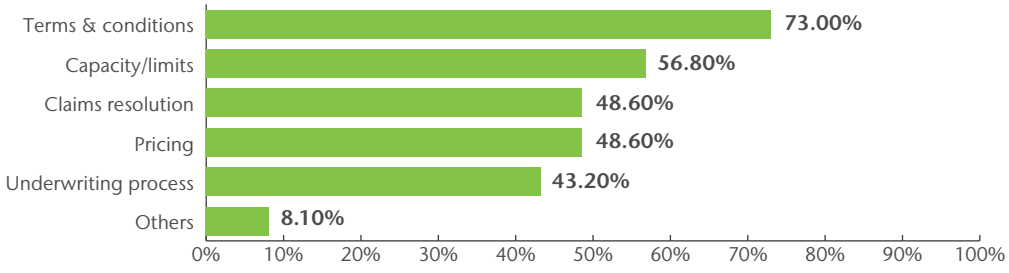


Do you currently buy cyber insurance?

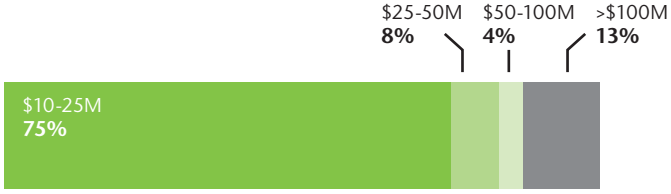
Is the expense for cyber insurance currently in budget?

Policy cover and structure

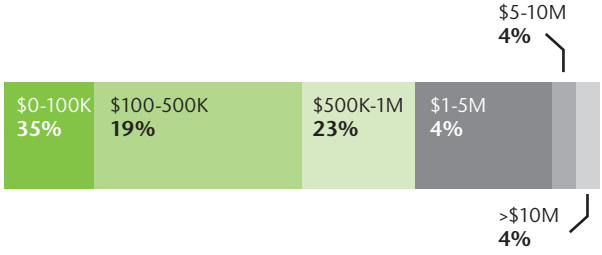
What do you perceive as the greatest issues in the cyber risk market place?



Limits

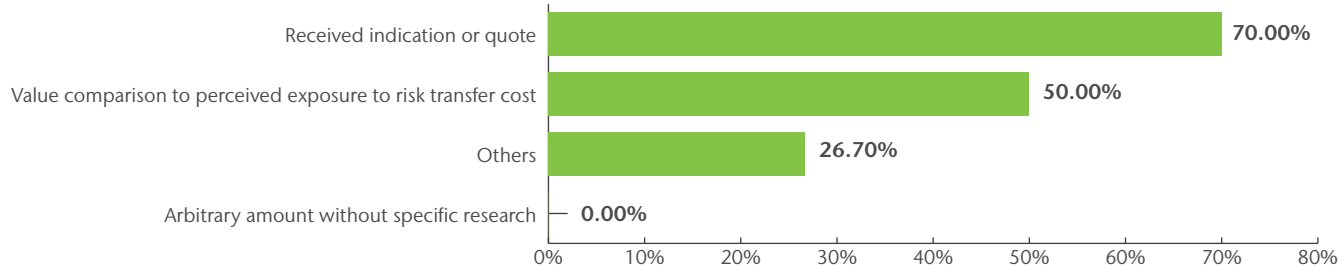


Retention levels



Estimating premium

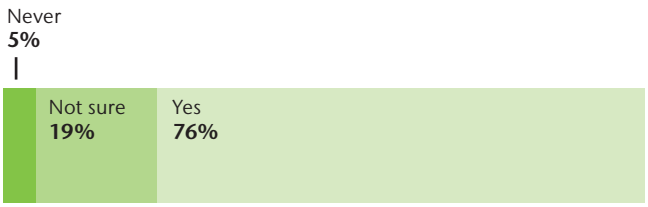
How did you arrive at the quantum for cyber risk?



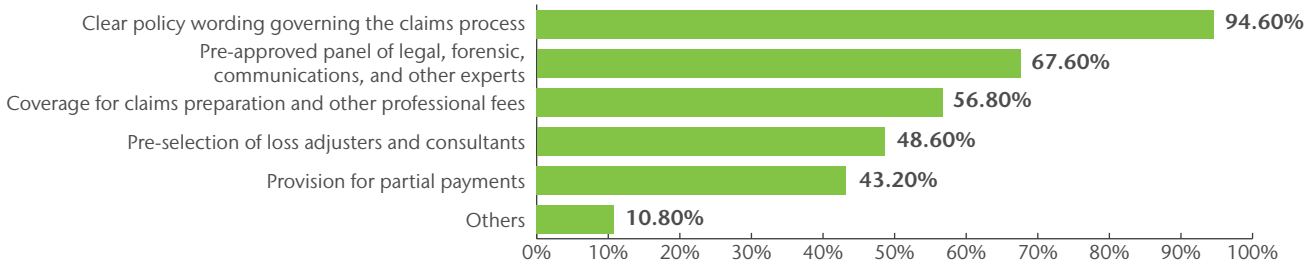
Assuming the availability of capacity through a dedicated captive facility, would you be willing to retain the self-insured layer in your captive?

Would you be willing to share risk with other companies in your industry as part of a captive facility dedicated to writing cyber risk, assuming you were comfortable with the underwriting process?

Are you concerned that claims arising from cyber coverage will be adjusted and paid fairly?



What steps should cyber underwriters take to ensure a fair claims process (indicate all that apply)?

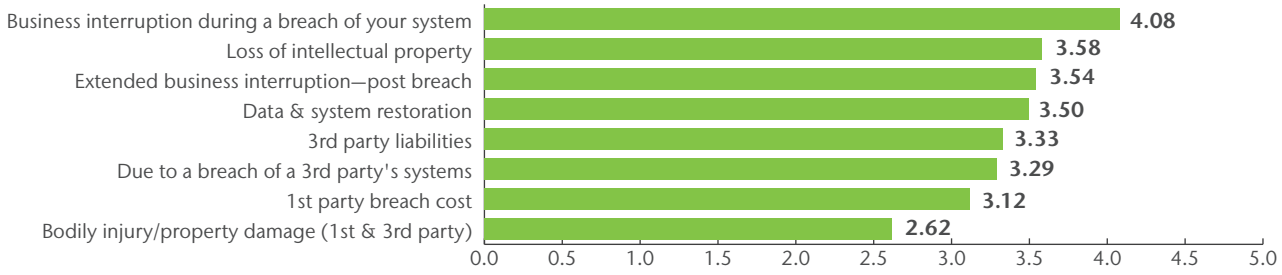


Product Risk

This category consists of participants from the agriculture, chemical, food & beverage, and pharmaceuticals sectors. About 74% of respondents represent companies with a revenue size of more than USD 5 billion.

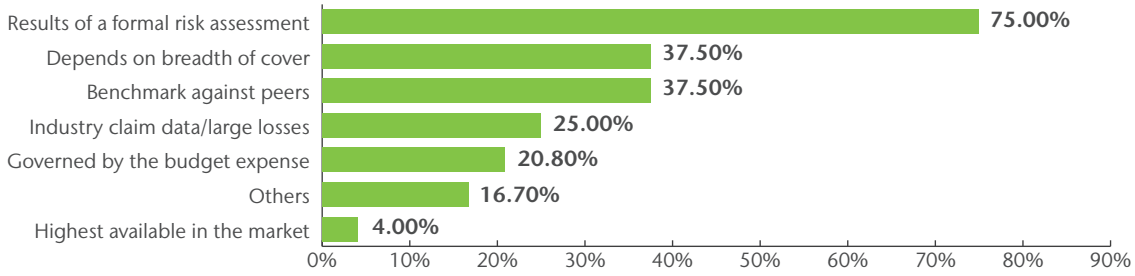
Cyber risk concerns

Which elements in cyber risk give you the greatest cause for concern?

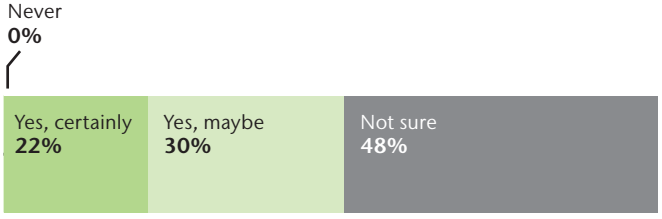


Risk Assessment

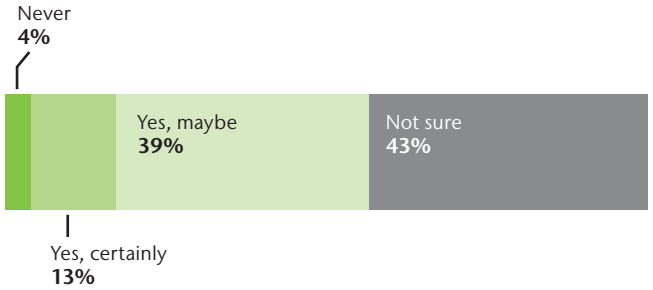
When deciding on total limits to insure, which factors influence the decision?



Based on the information currently available to you, do you know if your company complies with international best practices and standards governing information security (e.g., ISO 27001/002, NIST, or similar)?

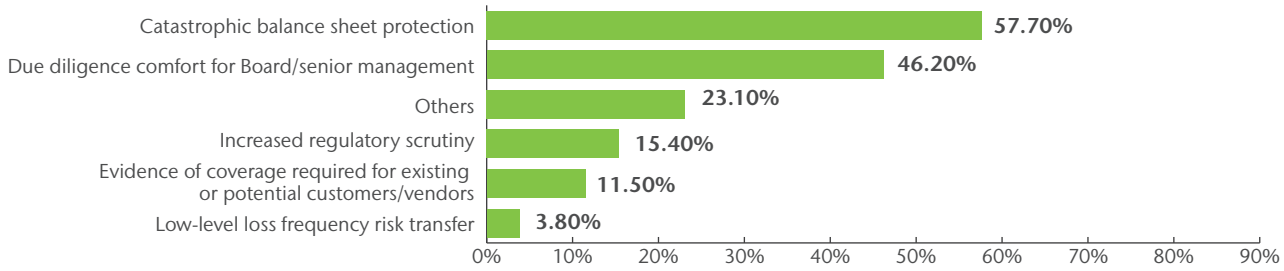


Would an independently administered cyber risk evaluation assist you in understanding and quantifying first and third party cyber exposure?



Attitudes toward cyber insurance

What are your main reasons for purchasing or considering cyber insurance (Indicate all that apply)?

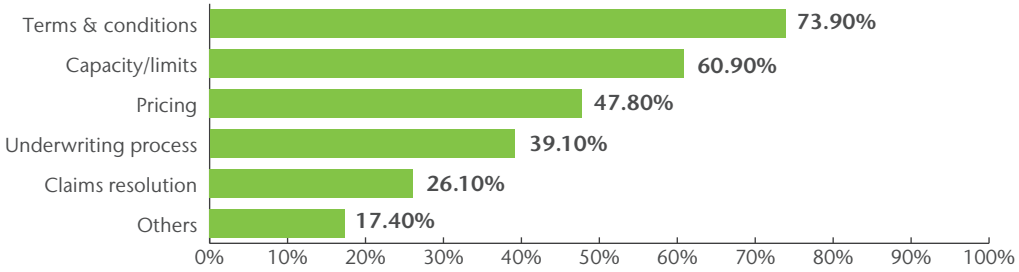


Do you currently buy cyber insurance?

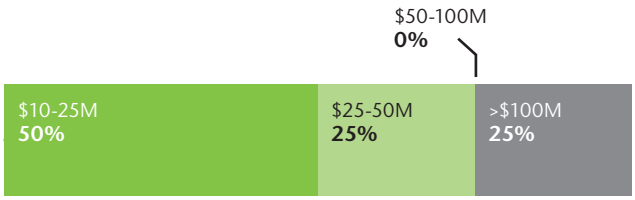
Is the expense for cyber insurance currently in budget?

Policy cover and structure

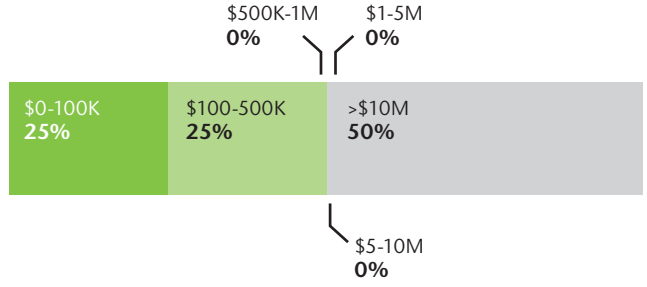
What do you perceive as the greatest issue in the cyber risk market place?



Limits

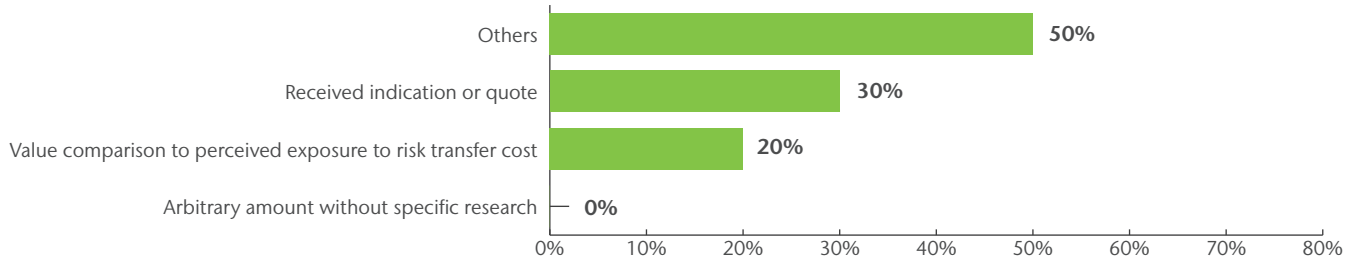


Retention levels



Estimating premium

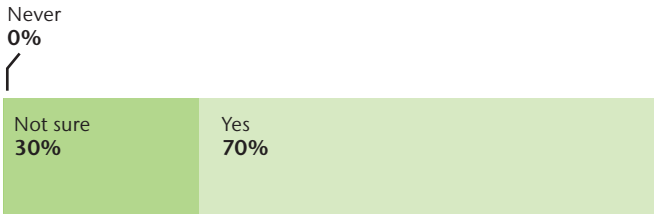
How did you arrive at the quantum for cyber risk?



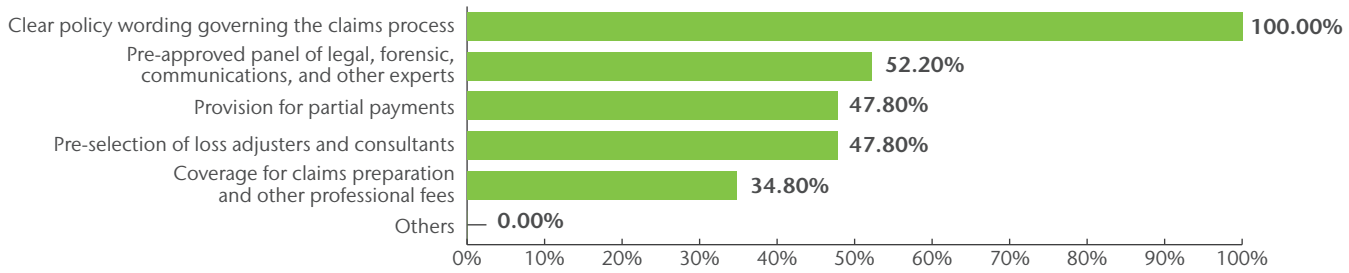
Assuming the availability of capacity through a dedicated captive facility, would you be willing to retain the self-insured layer in your captive?

Would you be willing to share risk with other companies in your industry as part of a captive facility dedicated to writing cyber risk, assuming you were comfortable with the underwriting process?

Are you concerned that claims arising from cyber coverage will be adjusted and paid fairly?



What steps should cyber underwriters take to ensure a fair claims process (indicate all that apply)?

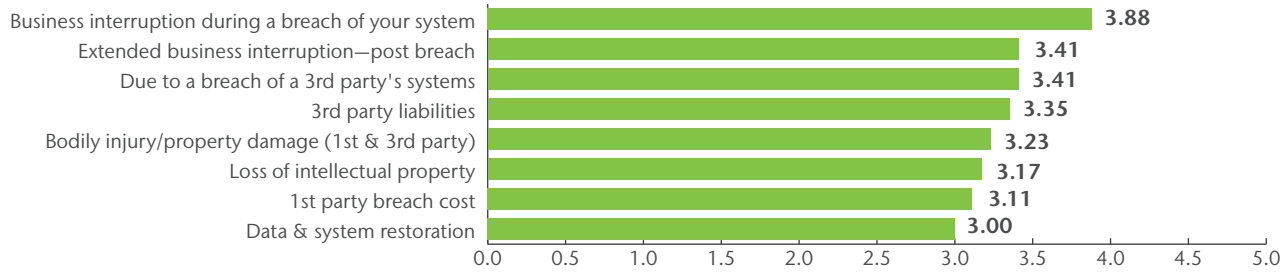


Critical Infrastructure

The critical infrastructure category covers the utility, energy, oil & gas, and petrochemical sectors. About 41% of participants represent companies with revenues less than USD 5 billion (17% under USD 1 billion).

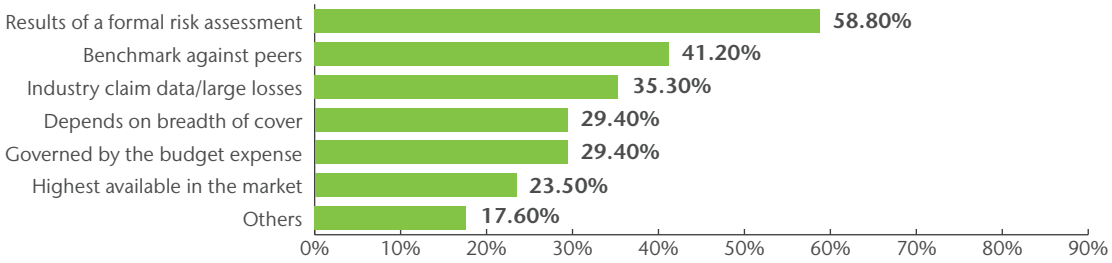
Cyber risk concerns

Which elements in cyber risk give you the greatest cause for concern?

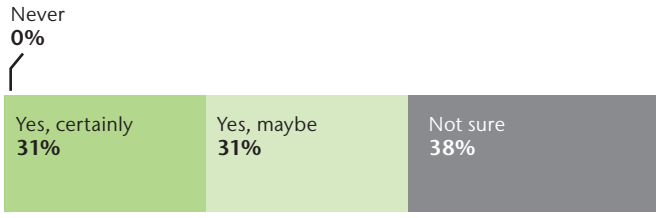


Risk assessment

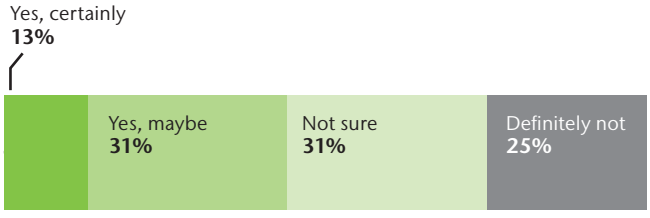
When deciding on total limits to insure, which factors influence the decision?



Based on the information currently available to you, do you know if your company complies with international best practices and standards governing information security (e.g., ISO 27001/002, NIST, or similar)?

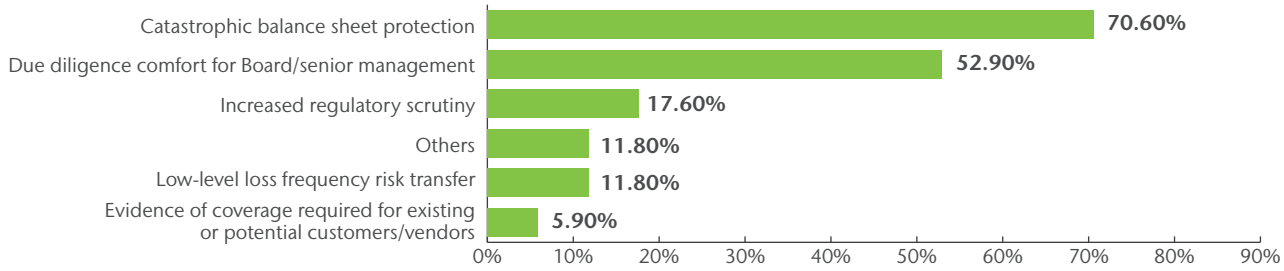


Would an independently administered cyber risk evaluation assist you in understanding and quantifying first and third party cyber exposure?



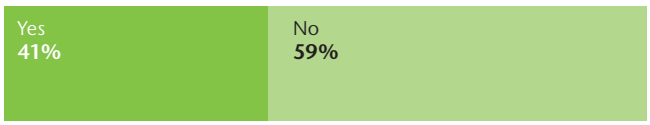
Attitudes toward cyber insurance

What are your main reasons for purchasing or considering cyber insurance?



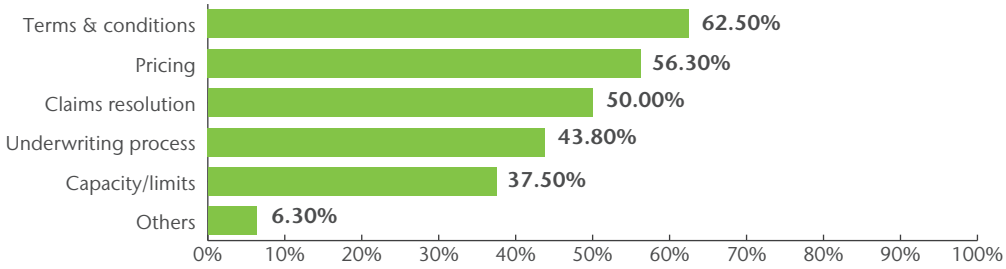
Do you currently buy cyber insurance?

Is the expense for cyber insurance currently in the budget?



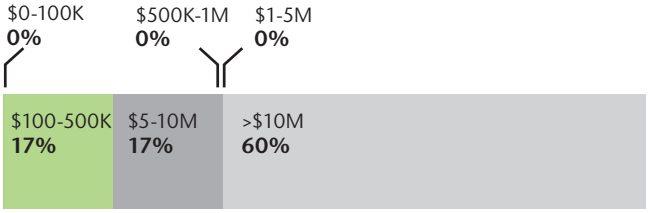
Policy cover and structure

What do you perceive as the greatest issues in the cyber risk market place?



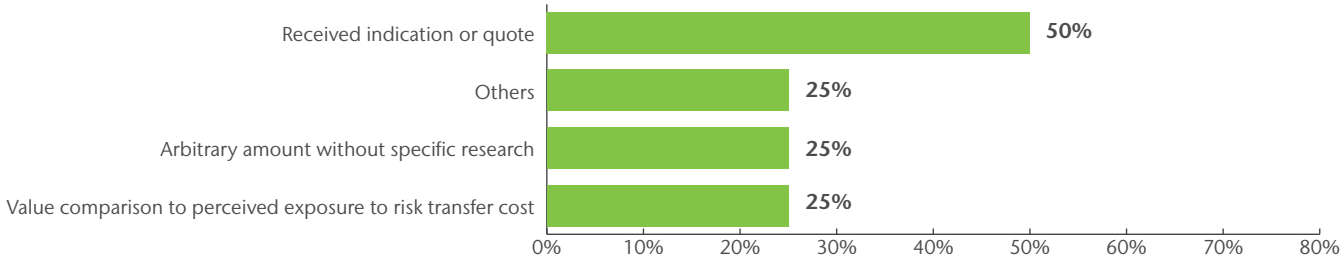
Limits

Retention levels

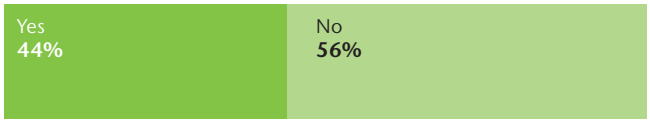


Estimating premium

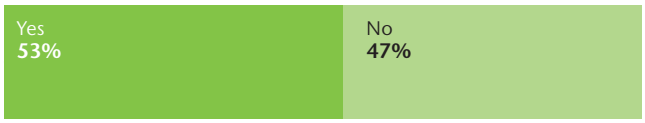
How did you arrive at the quantum for cyber risk?



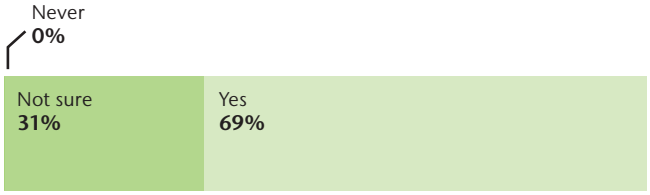
Assuming the availability of capacity through a dedicated captive facility, would you be willing to retain the self-insured layer in your captive?



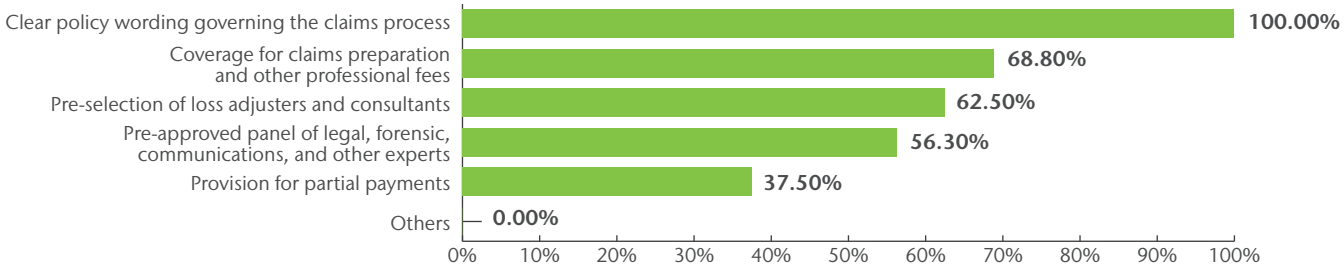
Would you be willing to share risk with other companies in your industry as part of a captive facility dedicated to writing cyber risk, assuming you were comfortable with the underwriting process?



Are you concerned that claims arising from cyber coverage will be adjusted and paid fairly?



What steps should cyber underwriters take to ensure a fair claims process (indicate all that apply)?

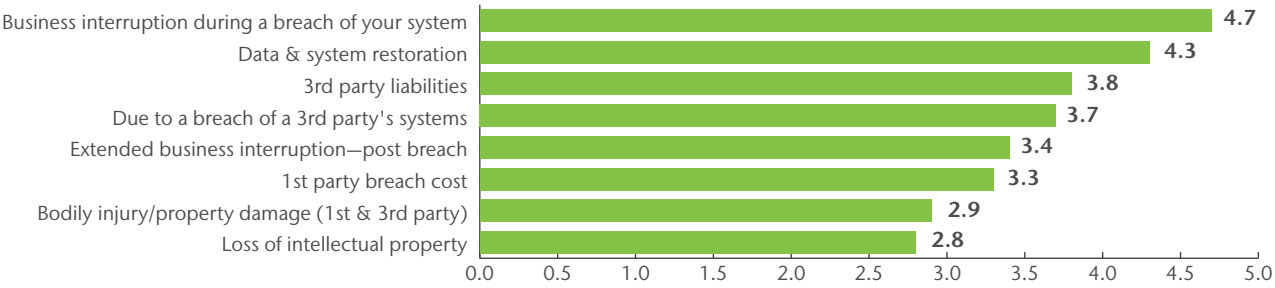


Transport

The transport category covers the aerospace & defense, aviation, and transportation sectors. About 55% of respondents represent companies with revenues under USD 5 billion and a quarter of participants represent companies with revenues of USD 25 billion and above.

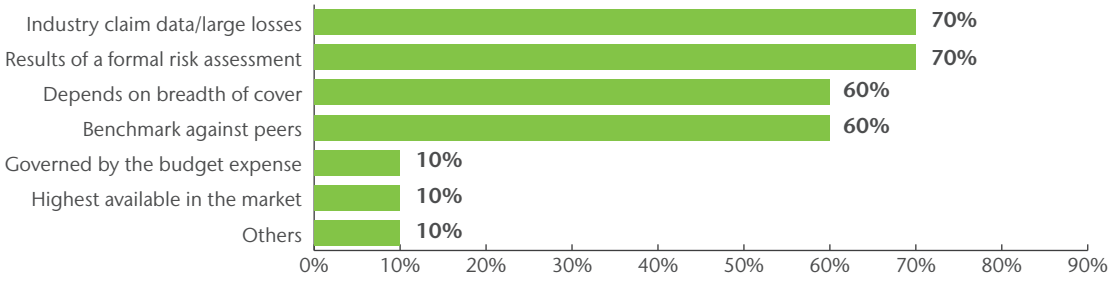
Cyber risk concerns

Which elements in cyber risk give you the greatest cause for concern?

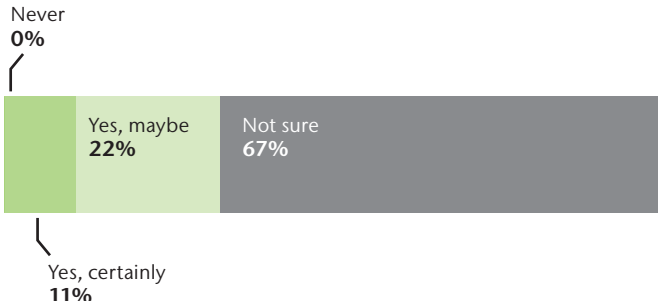


Risk assessment

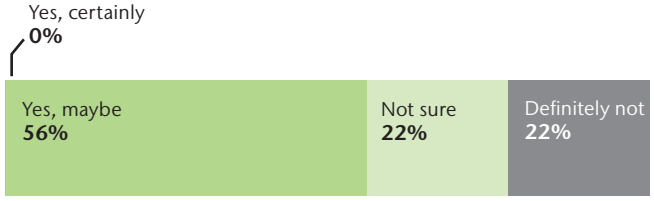
When deciding on total limits to insure, which factors influence the decision?



Based on the information currently available to you, do you know if your company complies with international best practices and standards governing information security (e.g., ISO 27001/002, NIST, or similar)?

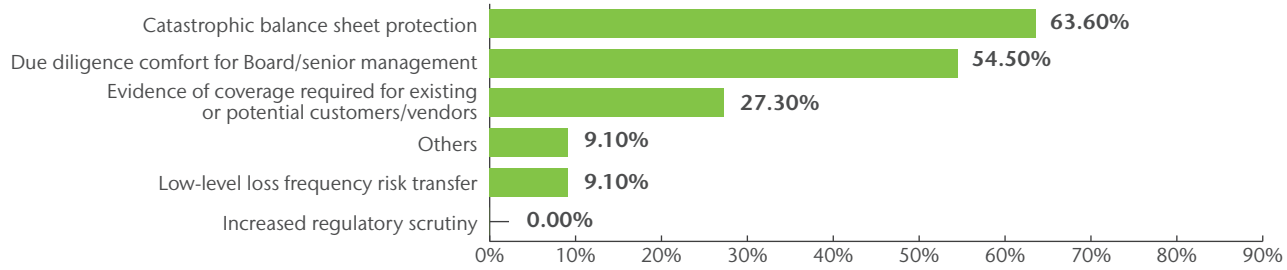


Would an independently administered cyber risk evaluation assist you in understanding and quantifying first and third party cyber exposure?

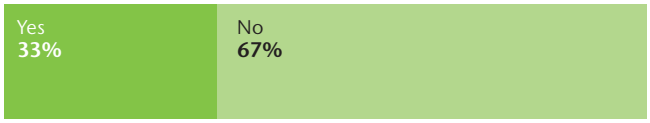


Attitudes toward cyber insurance

What are your main reasons for purchasing or considering cyber insurance?



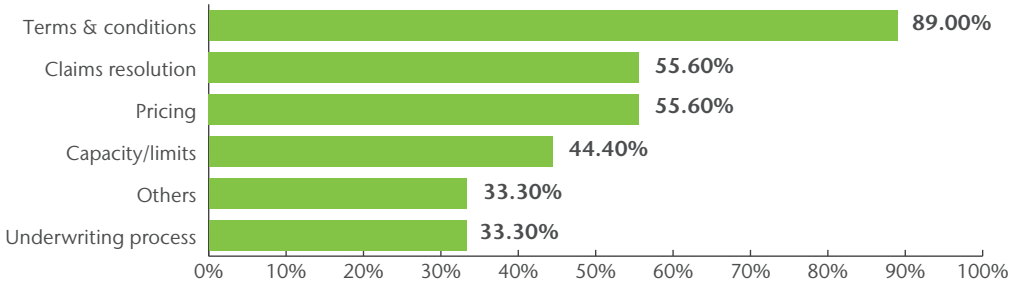
Do you currently buy cyber insurance?



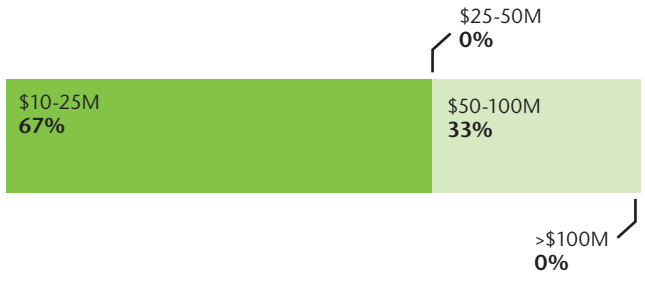
Is the expense for cyber insurance currently in the budget?

Policy cover and structure

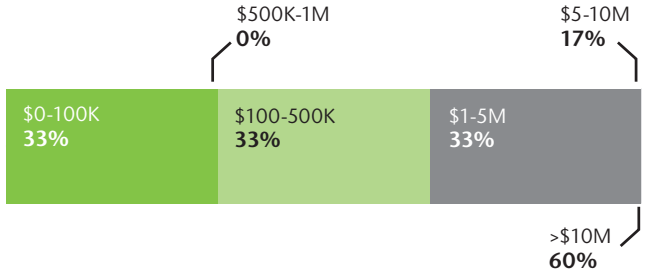
Which elements in cyber risk give you the greatest cause for concern in general and in regards to business interruption and extra expense coverage?



Limits

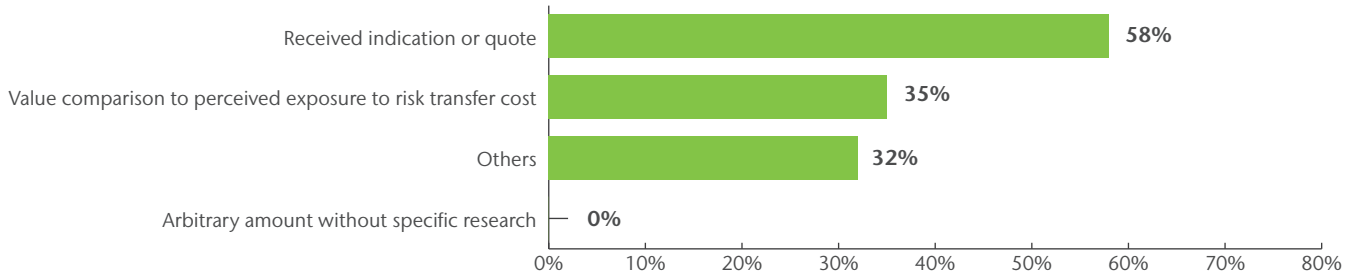


Retention levels



Estimating premium

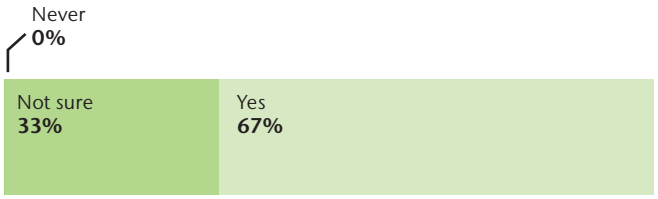
How did you arrive at the quantum for cyber risk?



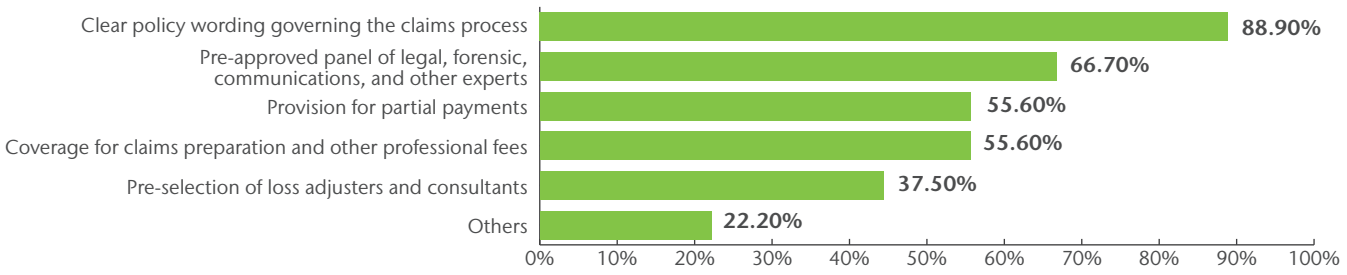
Assuming the availability of capacity through a dedicated captive facility, would you be willing to retain the self-insured layer in your captive?

Would you be willing to share risk with other companies in your industry as part of a captive facility dedicated to writing cyber risk, assuming you were comfortable with the underwriting process?

Are you concerned that claims arising from cyber coverage will be adjusted and paid fairly?



What steps should cyber underwriters take to ensure a fair claims process (indicate all that apply)?

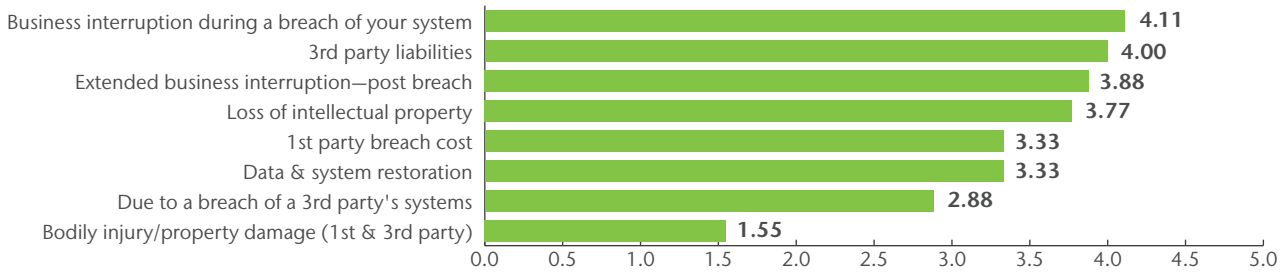


Heavy Industry

The heavy industry category is comprised of participants from the construction, engineering, manufacturing, and forest products sectors. About 59% of participants represent companies with revenues of USD 5 billion and above.

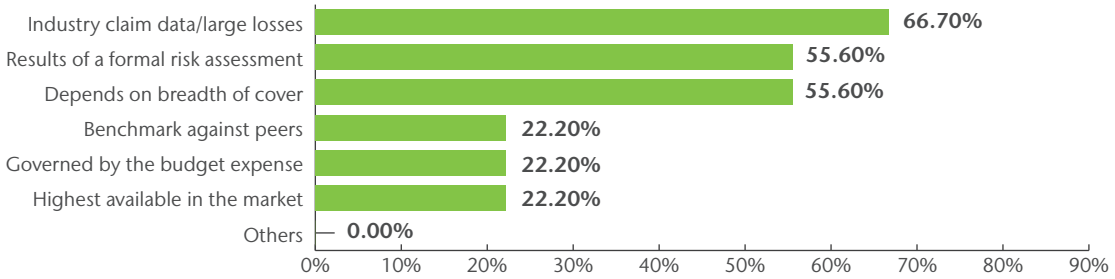
Cyber risk concerns

Which elements in cyber risk give you the greatest cause for concern?

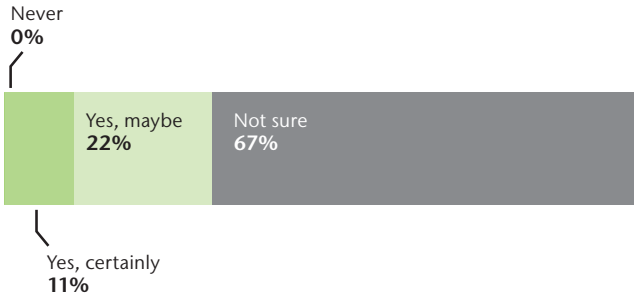


Risk assessment

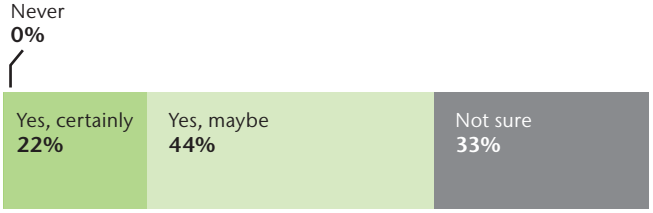
When deciding on total limits to insure, which factors influence the decision?



Based on the information currently available to you, do you know if your company complies with international best practices and standards governing information security (e.g., ISO 27001/002, NIST, or similar)?

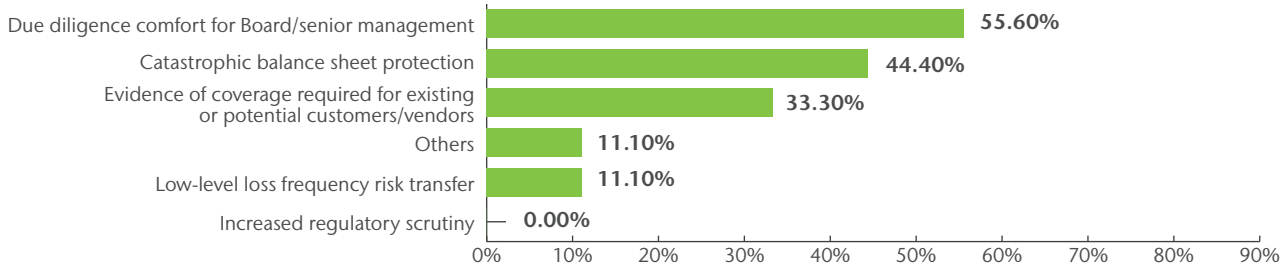


Would an independently administered cyber risk evaluation assist you in understanding and quantifying first and third party cyber exposure?



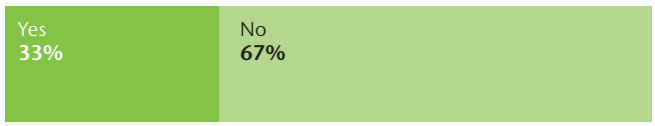
Attitudes toward cyber insurance

What are your main reasons for purchasing or considering cyber insurance?



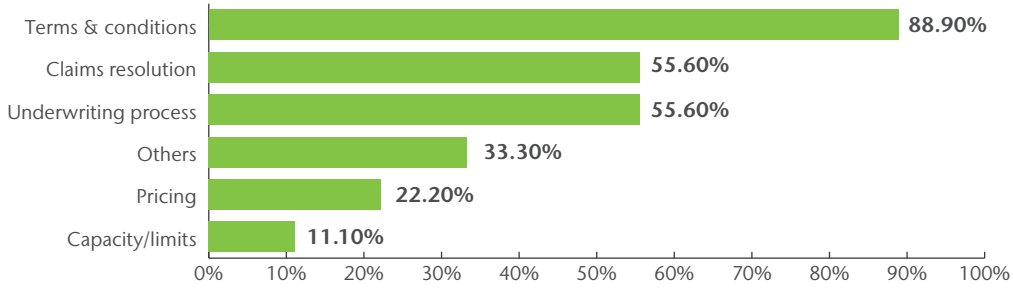
Do you currently buy cyber insurance?

Is the expense for cyber insurance currently in the budget?



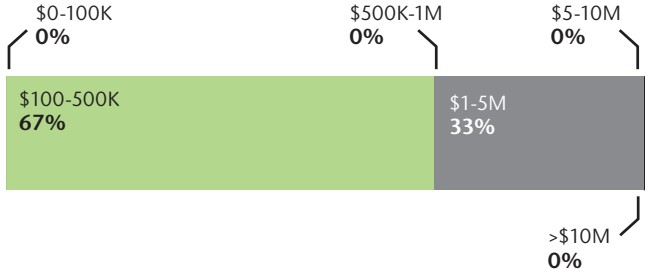
Policy cover and structure

Which elements in cyber risk give you the greatest cause for concern in general and in regards to business interruption and extra expense coverage?



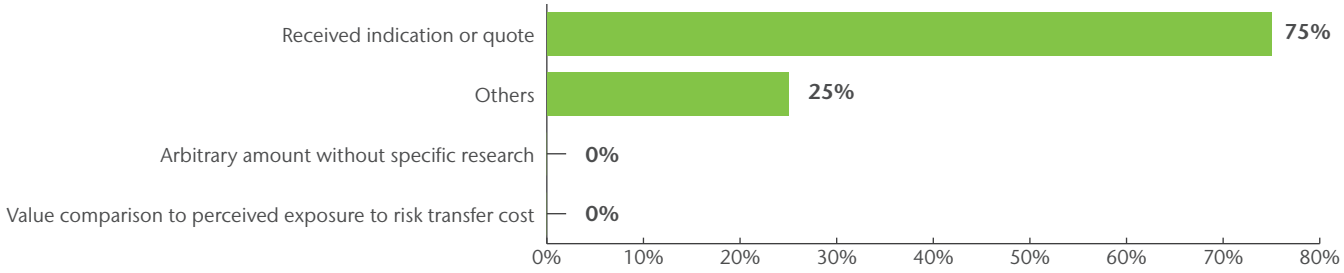
Limits

Retention levels



Estimating premium

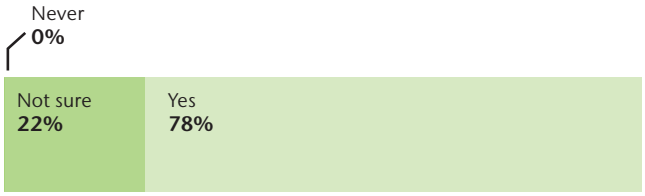
How did you arrive at the quantum for cyber risk?



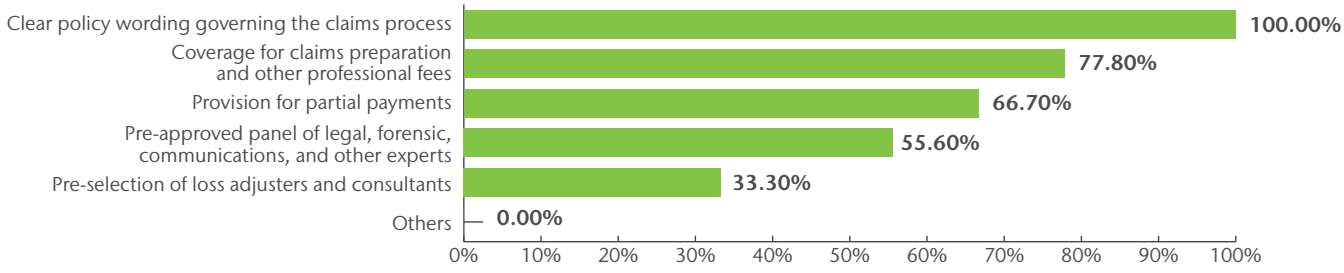
Assuming the availability of capacity through a dedicated captive facility, would you be willing to retain the self-insured layer in your captive?

Would you be willing to share risk with other companies in your industry as part of a captive facility dedicated to writing cyber risk, assuming you were comfortable with the underwriting process?

Are you concerned that claims arising from cyber coverage will be adjusted and paid fairly?



What steps should cyber underwriters take to ensure a fair claims process (indicate all that apply)?



Methodology

This web-based survey was issued to risk managers and directors of captive insurance companies. This is Aon's first cyber survey, which targeted 128 of Aon's captive clients who currently have an established captive managed by Aon Captive and Insurance Management.

All responses for individual organizations are held confidential; only consolidated data was incorporated into this report. Percentages for some of the responses may not add up to 100% due to rounding or respondents being able to select more than one answer. All revenue amounts are shown in US Dollars.

Aon Captive & Insurance Management

Aon's Captive & Insurance Management team manages approximately 1,100 insurance entities worldwide, including captives, protected and incorporated cell facilities, special purpose vehicles, and specialist insurance and reinsurance companies.

As a business unit within Aon's Global Risk Consulting group, we leverage the diverse risk consulting expertise required for a successful risk management program. Our consulting and management teams work closely together to create and implement innovative solutions.

Sources

A cyber attack on U.S. power grids means more than just being without power for a few days. In Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath, author Ted Koppel suggests that the effects of a cyber attack in the U.S. and its aftermath are widely underestimated.

The risks associated with a cyber attack could potentially impact all Aon clients. In Koppel's book, Aon is the sole and exclusive insurance broker expert featured, with Kevin Kalinich, Global Practice Leader for Cyber Insurance, revealing ways organizations and insurance companies are working together to unravel the risks associated with "the Internet of Things." Kevin's comments in the book relate to the evolution of assessing and evaluating risks stemming from cyber-related events.

Contacts

For report inquires

Peter Mullen
Chief Executive Officer
Aon Captive and Insurance Management
Aon Risk Solutions
peter.mullen@aon.com
+1.441.278.1769

Adam Peckman
Global Practice Leader—
Cyber Risk Consulting
Aon Global Risk Consulting
Aon Risk Solutions
adam.peckman@aon.co.uk
+44 20 7086 3544

John D. Dempsey, CPA, CFE
Managing Director and Global Practice Leader—
Claims Preparation,
Advocacy and Valuation
Aon Global Risk Consulting
Aon Risk Solutions
john.dempsey@aon.com
+1.203.423.8211

Jay Gotelaere, FCAS, MAAA, CERA, ASA
Group Managing Director,
Risk Consulting Americas
Aon Global Risk Consulting
Aon Risk Solutions
jay.gotelaere@aon.com
+1.312.381.2772

Kevin P. Kalinich, Esq.
Global Practice Leader—Cyber Insurance
Aon Risk Solutions
kevin.kalinich@aon.com
+1.312.381.4203

Stephanie Snyder Tomlinson
U.S. National Sales Leader—Cyber Insurance
Aon Risk Solutions
stephanie.tomlinson@aon.com
+1.312.381.5078

Mark Buningh
Cyber Risk Practice Leader—Netherlands
Aon Risk Solutions
Aon Global Risk Consulting
mark.buningh@aon.nl
+31 6 5134 6614

Stephen Trickey
Chief Commercial Officer & FSG National
Leader—Australia
Financial Specialities
Aon Risk Solutions
stephen.trickey@aon.com
t: +61 292537577

Andrea Garcia Beltran
European Cyber Sales Leader—EMEA
Global Broking Centre | Financial and
Professional Services
Aon Risk Solutions
andrea.garciabeltran@aon.co.uk
+44 (0)20 7086 0428

Christian Hoffman
National Practice Leader—
Aon Professional Risk Solutions—US
Aon Risk Solutions
christian.hoffman@aon.com
+1.212.441.2263

For media and press inquires

Cybil Rose
Account Director
KemperLesknik
cybil.rose@kemperlesnik.com
+1.312.755.3537

About Aon

Aon plc (NYSE:AON) is a leading global provider of risk management, insurance brokerage and reinsurance brokerage, and human resources solutions and outsourcing services. Through its more than 72,000 colleagues worldwide, Aon unites to empower results for clients in over 120 countries via innovative risk and people solutions. For further information on our capabilities and to learn how we empower results for clients, please visit: http://aon.mediaroom.com.

#18397 03/16

Risk. Reinsurance. Human Resources.

Empower Results®