Cyber – The Fast Moving Target
Executive Summary

127
RESPONDENTS

5
INDUSTRY CATEGORIES

1
GLOBAL VIEW

Contact

Fergus Brooks
National Practice Leader,
Cyber Risk
t + 61 2 9253 7835
e fergus.brooks@aon.com

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 realisation that cyber risk, in some instances more pervasive than traditional exposures, is present wherever organisations 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 organisations 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.

60%

OF LARGE COMPANIES DON'T BUY CYBER INSURANCE

Attitudes toward cyber insurance

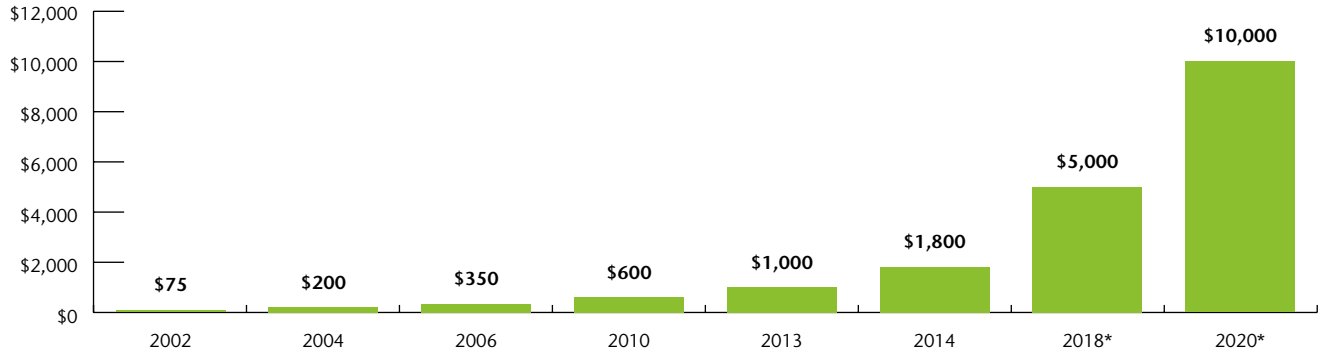
68% of companies buy cyber for balance sheet protection, closely followed by ensuring due diligence comfort for the board.

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.

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.

Cyber Insurance: Global Gross Written Premium ($millions)



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

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 modelling becomes available (like Aon's recently released Cyber Insight model) we anticipate a greater understanding of the exposure particular to any one organisation.

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 spiralling 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%