



October 2016

Cyber: in search of resilience in an interconnected world



Index

Executive summary

Introduction

**Risk
awareness**



**Risk
preparedness**



**Role of
cyber insurance**



Conclusion

Appendix

Executive summary



Risk awareness

Against the background of several high-profile data breaches and cyber-attacks over recent years, a growing number of businesses of all sizes see cyber as a high risk. Globally, insurers and corporations across most industrial sectors expect the frequency and severity of cyber-related events to increase. Firms in North America, especially in banking and professional services, typically rank cyber risk higher than counterparts in other regions. With enhanced data protection regulation due to be implemented in various countries, cyber risks are only likely to rise further up the corporate agenda. Data breaches, both via accidental and malicious attacks, are the biggest concern. There is a strong third-party component to data breaches, but corporations are currently more concerned about first-party exposures. Most nonetheless expect that the risk from third-party exposures will increase over the next 10 years.



Risk preparedness

Unsurprisingly, senior management at firms which rank cyber as a high risk are engaged and knowledgeable about the evolving threats. This is especially true in the hospitality, consumer products and auto sectors. Even so, some firms are ill-equipped to respond, in part because key messages on cyber security are rarely linked to business objectives and strategy, and are often positioned as a purely technical issue. The picture from a talent and skills perspective is mixed; 60% of firms which rank cyber as a high risk do not feel confident that their workforce currently has adequate skills to cope with the threat. Smaller firms are especially vulnerable. About 40-45% of all firms do regular risk assessments, and also document risk practices. However, the remainder mostly still manage cyber risk in an ad hoc manner. Few companies have as yet institutionalised cyber risk management, even among those which say they see a cyber-attack or data breach as a significant threat.



The role of cyber insurance

Many companies want to protect themselves against the losses associated with a cyber event through insurance. Firms that rank cyber as a high risk are almost twice as likely to have cover than those that do not. However, anecdotal evidence suggests that dedicated cyber insurance penetration is lower than our survey suggests, at least outside of the US. This could be a sign that corporations are living under an illusion of protection amidst lack of clarity about what cyber risks are covered in existing property and liability policies, and which are not. Firms without specific cyber insurance say they have not explored coverage (main reason), although some feel that they do not have much exposure to cyber risks, or prefer to self-insure. Demand for cyber insurance is expected to rise, especially among firms who see themselves as high-risk and those with existing cover. The majority of insurers currently selling cyber insurance do so as separate coverage (63% of insurers). Corporate clients would like to buy insurance against a range of risks but cite a lack of corresponding available cover in some areas. Half of insurers who do not provide cyber insurance plan to write cyber protection in the next couple of years, although nervousness about overstepping the boundaries of insurability can act as a drag on product innovation. Both insureds and insurers are open to flexible tech-enabled solutions. Of the insurers who write cyber cover, 70% either provide or plan to offer services beyond insurance, mainly in partnership with third-party providers. Companies and insurers agree that data sharing will increase but currently there is limited legislation to encourage information sharing. The role of government in legislating on data sharing and potentially mandating cyber insurance is complex, and could make the cyber risk environment more complicated still.

Introduction

Technological progress is prompting seismic changes in how societies are organised, firms are run and individuals live their lives. In particular, the proliferation of digitally connected devices, the explosion of ecommerce and the Internet of Things (IoT) are disrupting a whole host of economic activities, from product design and manufacturing, right through to spending and distribution. At the same time, however, these trends raise significant challenges which could make it difficult to realise all of the potential benefits from digitalisation. Most obviously, in the absence of clear and agreed-upon architectures for connected systems, technical IT vulnerabilities will persist and even grow. Cyber security and how to manage the associated risk is thus becoming an increasingly important topic for firms.

To examine the issues raised by increased digital interconnectedness, at the beginning of 2016 Swiss Re, in collaboration with IBM's Institute for Business Value (IBV) undertook a global survey of companies, including insurers (see Appendix for details about the survey design and sample).¹ The broad aim was to find out more about how corporates perceive the impact of the evolving cyber landscape on their businesses, and the measures they are adopting to monitor and manage the associated risks.

Results from the survey are supplemented with qualitative insights from interviews with subject matter experts. In particular, Swiss Re and IBM conducted in-depth interviews with risk management professionals at large and medium-sized corporations, and also consulting firms across the main regions.²

This report reviews some of the main survey findings alongside other evidence, organised around three core themes:

Risk awareness:

how alert are companies to the emerging cyber threats?

Risk preparedness:

how has this awareness translated into risk management action?

Role of cyber insurance:

how do companies perceive insurance policies to protect against cyber-related perils?

¹ An earlier paper reported some of the initial findings from the survey. See *Cyber and beyond: Insurance and risk in a digitally interconnected world*, IBM Institute for Business Value in association with Swiss Re, June 2016.

² For a broader review of emerging risks, see SONAR: New emerging risk insights, Swiss Re, May 2016.

Risk awareness



Figure 1: Current view of cyber threats

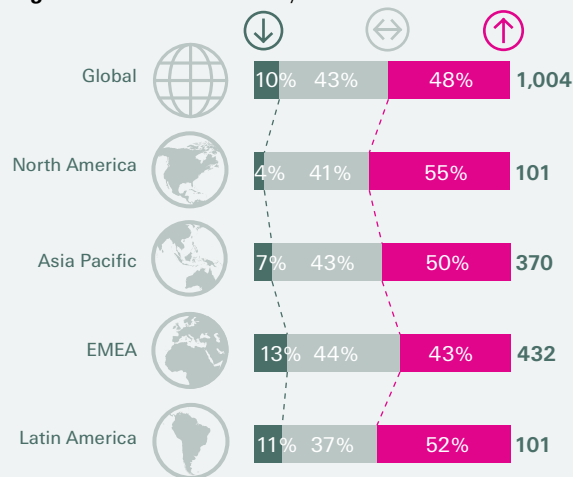
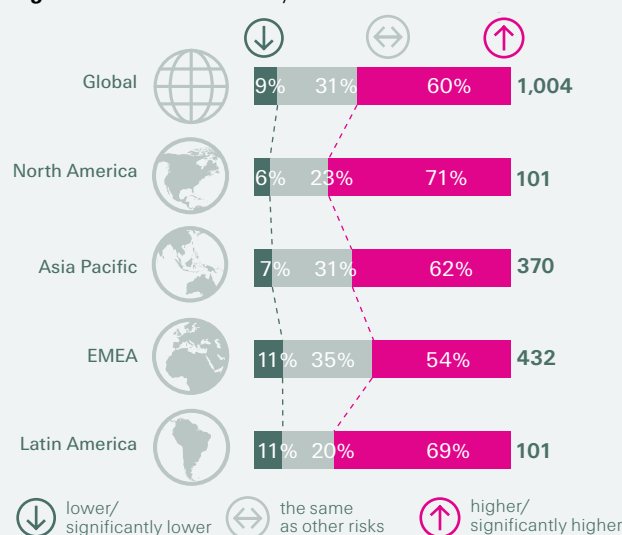


Figure 2: Future view of cyber threats



Q. Corporations – Where do you currently rank threats from digital interconnectedness relative to other risks? And in 10 years how will that rank change?

Perceptions of threats from digital interconnectedness

- Against the background of several high-profile breaches over recent years, close to half of corporations in the survey (48% in Figure 1³) currently consider the risks associated with digital interconnectedness (ie, cyber) to be greater than other risks. As attackers grow more sophisticated and enhanced regulatory scrutiny leads to large fines for privacy breaches, firms anticipate that the frequency and severity of incidents will increase.⁴ As a result, 60% of companies expect cyber will become a bigger risk in 10 years' time (see Figure 2).
- **Analysis by firm size:** Size does not play a huge role; 40% of small firms currently rank cyber as a higher threat than other risks. Smaller businesses are starting to realise the potential risk of cyber-attacks and security breaches, which echoes studies showing that cyber-criminals using ransomware have begun to attack smaller companies more frequently.⁵

- **Analysis by industry:** There is broad agreement on the increasing risk across sectors, but more firms in transportation, pharma and hospitality rank the threat of digital interconnectedness higher, and with good reason. The management and operation of transport networks is becoming increasingly digital and computer reliant; pharma and biotech firms worry about fraud and crime, especially linked to online sale of fake medicines and products; and hospitality firms now deal with large digital databases of customer records and ever increasing transaction volumes.^{6,7}
- **Analysis by region:** Executives at North American companies appear more concerned about cyber threats than their counterparts in Europe, the Middle East & Africa (EMEA), perhaps reflecting the tougher data protection laws there. But with enhanced regulations in the EU coming on-stream, mitigating data breaches is sure to be a discussion point in more European board rooms in the coming years. The survey indicates that firms in Latin America also perceive the threat from cyber as more significant than in other regions. Hackers there are reportedly very active and inventive. For example, in recent years there has been a rise in hackers in Latin America linking up with more experienced cyber-criminals in Russia and Eastern Europe, which has probably heightened risk awareness.⁸

³ Note: reported percentages in the figures in this document may not sum to 100% due to rounding.

⁴ Under new EU General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88) which shall apply from 25 May 2018, companies will face fines of up to EUR 20 million, or 4% of their global annual turnover, if they fail to protect data properly.

⁵ The UK Government Security Breaches Survey found that nearly three quarters (74%) of small organisations reported a security breach in 2015, an increase on the 2013 and 2014 surveys. SMEs are now being pinpointed by digital attackers. See Information Security Breaches Survey - 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf.

⁶ "Online sale of fake medicines and products targeted in INTERPOL operation", www.interpol.int, 9 June 2016, <http://www.interpol.int/News-and-media/News/2016/N2016-076>

⁷ "Cyber Risk in the transportation industry", Marsh Insights, 2015.

⁸ Latin America: The New Frontier for Cyber Attacks, Joint study by the Center for Strategic Studies and McAfee, 29 April 2016.

Risk awareness



Ranking different types of digital interconnectedness risks

Table 1: Relative ranking of digital interconnectedness risks (by industry)

Which cyber risks is your company currently exposed to?	Source	All sectors	Pharma & biotech	Transportation	Consumer prod.	Hotel	Auto mfg.	Banking	Chemicals/petrol	Telecom infra.	Indust. product	Professional serv.	Electronics	Media	Utilities infra. power	Retail	Health-care
Data corrupted	Malicious																
Data stolen and misused	Malicious																
Data exposed	Accidental																
Data deleted or corrupted	Accidental																
Data deleted	Malicious																
Fraud/crime	Malicious																
Physical damage	Malicious																
BI from activity in network	Accidental																
Loss of IP	Malicious																
BI from DoS/malware	Malicious																
Contingent BI (cloud failure)	Cloud																
Tech errors & omissions	Accidental																
Extortion	Malicious																
Reputational damage	Both																
Contingent BI (utility failure)	Contingent																
Physical damage	Accidental																

Q. Corporations – Which of the following risks is your company currently exposed to? Lowest exposure  Highest exposure

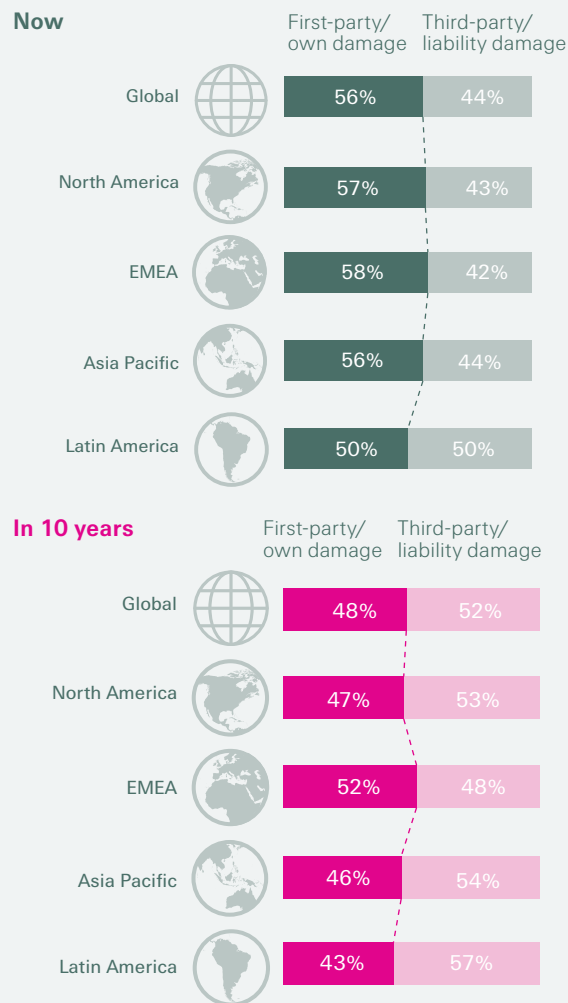
Data breaches are a key concern. *Malicious* data corruption, theft and misuse are the top two risks for 13 of the 15 industries surveyed (see Table 1), which reflects that a growing number of criminals are beginning to target attacks on firms' intangible information assets. The risk of accidentally exposing or corrupting data comes a close second. Again, the concern is shared across industries. Often employees act as unwitting accomplices, and malicious attackers frequently leverage these mistakes. Most breaches in the recent past used legitimate user credentials, like passwords which were weak, default or stolen.⁹

Physical damage is becoming a worry. This is especially true for industries where an attack on a firm's industrial control systems could lead to first-party damage to physical property. Healthcare firms, however, ranked highly the risk of errors and omissions (eg. medical billing, and financial costs associated with privacy breaches). Respondents are in general less worried about contingent business interruption from cloud failure. Major cloud providers now have the financial wherewithal to hire top security talent from agencies such as the NSA, CIA or FBI. As a result, better security could well become a driver of cloud adoption as platform vendors allocate more resources and scale to secure their infrastructure.

⁹ 63% of data breaches used weak, default, or stolen passwords, according to the Verizon Data Breach Investigations Report, 2016, <http://news.verizonenterprise.com/2016/04/2016-data-breach-report-info/>

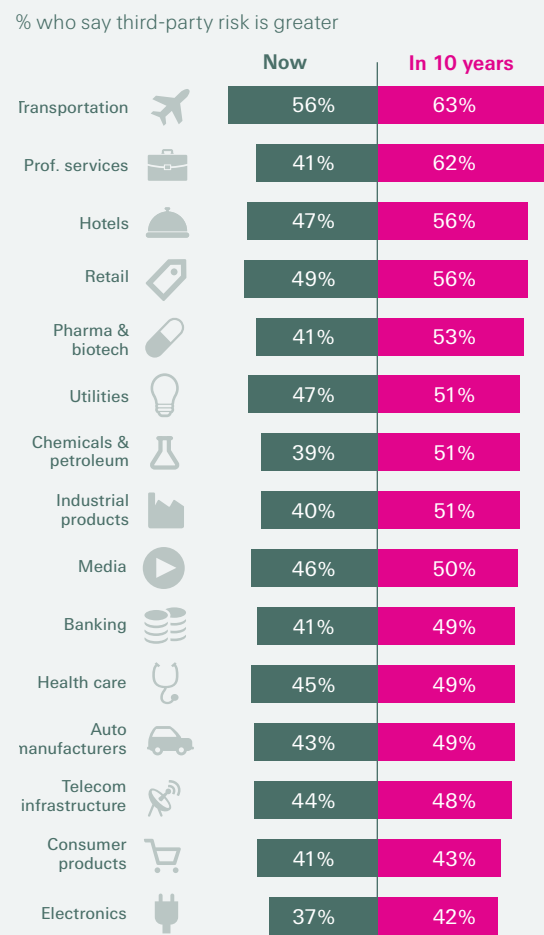
Risk awareness

Figure 3: Corporations' views on first-party threat versus third-party threat



Q. Corporations – Which threat from risks of digital interconnectedness do you currently see as greater? Now/in 10 years?

Figure 4: Current and future views of third-party digital threat (by industry)



First-party versus third-party loss

First party

- While firms worry about both first- and third-party losses, more corporations (56% in Figure 3) currently see first-party loss as a higher risk. However, this proportion dips slightly over a 10-year horizon (to 48% in Figure 3). This view is shared across regions, except in Latin America.
- Surprisingly, given the well-established US data privacy legislation, North American companies currently seem more concerned about first- rather than third-party risks. This could be because third-party events often also create large first-party losses, such as forensic and crisis management expenditures.
- Concerns about first-party losses are broadly similar across industries, although firms operating in chemicals & petroleum, industrial products, and electronics seem most worried.

Third party

- Corporations think third-party risks will become more important over the coming decade (from 44% to 52%). This is true internationally and across sectors. Those that see new uses for interconnected technologies both within and beyond their customer bases are most concerned about third-party exposure.
- Corporations that worry most about third-party risks are typically those that use and process a large amount of customer data. The latter are often targeted in cyber-attacks. A weak system that enables a hacker to access confidential information – a booking system at a hotel or a sales database at a retailer, for example – could put at risk important personal customer data.
- In the transportation sector (see Figure 4), where firms increasingly store or process third-party confidential information on networks, 56% see third-party loss as a higher risk (rising to 63% in 10 years). Firms in professional services, hospitality, and retail also see this as more relevant in 10 years, possibly for similar reasons.

Risk preparedness



Figure 5: C-Suite engagement with cyber risk topics

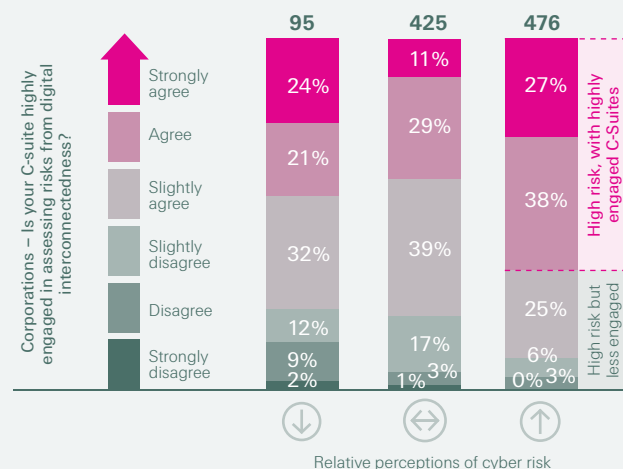
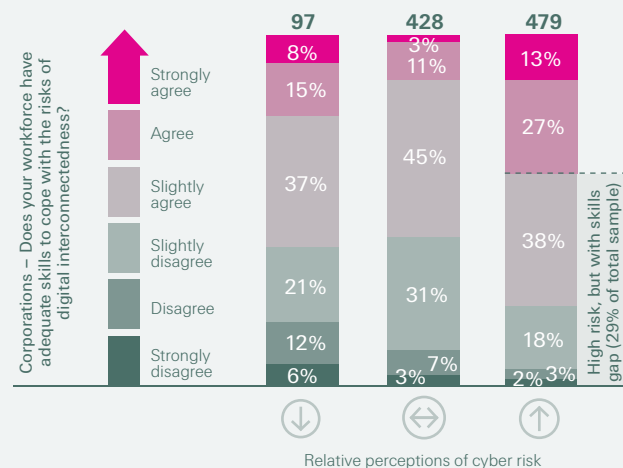


Figure 6: Workforce skills to cope with cyber risks



↓ lower/ significantly lower ↔ the same as other risks ↑ higher/ significantly higher

Engagement and knowledge about cyber risks

C-Suite engagement

- The majority of respondents from companies that rank cyber as a high risk say they have adequate buy-in from senior management, and that their top executives have sufficient knowledge on the issue (see Figure 5). This is especially true among larger firms in North America. From a sectoral view, firms in the hospitality, consumer products and auto sectors rank cyber as a high risk and also have highly engaged C-suites.
- But some firms raised red flags. About a third of high-risk corporations felt their C-Suite executives could be more engaged. Part of the reason for management disinterest could be that key messages on cyber security are rarely linked to business objectives in a clear manner. It is difficult to quantify evidence of threats given their multi-faceted nature and potential for highly interdependent hazards. Since risk managers primarily report technical and operational metrics, senior leaders continue to view security as a technical discipline.¹⁰

Workforce expertise

- The picture from a talent and skills perspective is rather mixed: the majority of firms have work to do here. 60% of respondents who rank cyber as a high risk do not feel confident that the workforce currently has adequate skills to cope with the threat (Figure 6). Smaller firms are especially vulnerable, probably reflecting budget constraints on hiring specialist staff. At the regional level, Latin American firms felt this most acutely, followed by European firms. From a sectoral view, firms in media, consumer products, hospitality and banking are the least prepared.
- In general, corporations will increasingly run into a significant talent gap, with the International Information System Security Certification Consortium predicting a 1.5m hiring shortfall in cyber specialists over five years.¹¹ Corporations will have to compete with technology companies and cloud providers to attract the experienced talent required to advise and protect against cyber-attacks. Recognising this issue, firms are reportedly developing internship programs, partnering with universities, and offering cybersecurity training to general IT professionals.

“Cyber risk management is not solely an IT department issue. It requires a broader approach to ensuring protection of all information assets.”

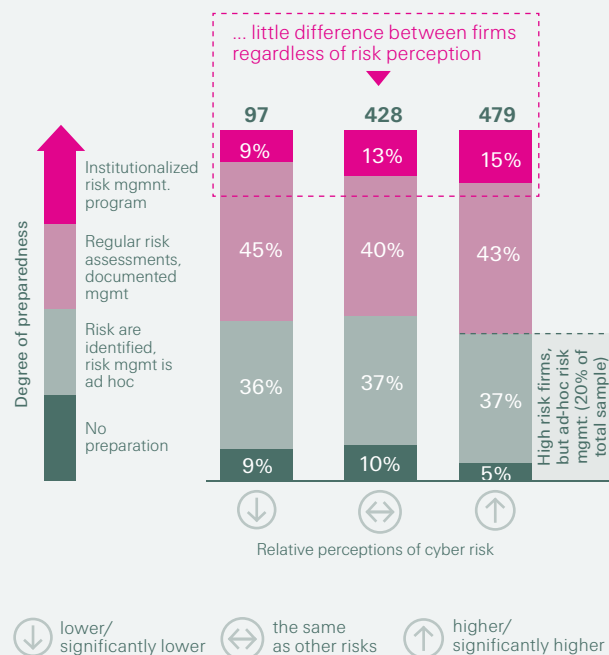
Senior risk manager, Brazilian industrial

¹⁰ How Boards of Directors Really Feel About Cyber Security, Osterman Research, June 2016. 54% of board members feel that the data presented is too technical; <http://baydynamics.com/content/uploads/2016/06/how-board-of-directors-feel-about-cyber-security-reports.pdf>

¹¹ The 2015 (ISC)2 Global Information Security Workforce Study, A Frost & Sullivan White Paper, www.isc2cares.org.

Risk preparedness

Figure 7: Corporations' view on their risk preparedness



Q. Corporations – To what extent are you prepared for risks of digital interconnectedness incidents?

Linking risk awareness to risk preparedness

- Few companies have yet institutionalised cyber risk management, even among those which see cyber as a significant threat. Around 40-45% of firms do regular risk assessments and document risk practices (see Figure 7) but of the remainder, most still manage cyber risks in an ad hoc manner (even larger firms). As a result, there may be gaps in knowledge and data that impair a firm's ability to make informed risk retention/transfer choices. Security breaches may go undetected for extended periods of time, increasing the potential for harm.¹²
- Analysis by industry:** Firms in healthcare, media and consumer products seem worst prepared, with over 50% of respondents saying that while cyber risks have been identified, risk management is ad hoc. Healthcare firms face a key challenge (particularly in North America and EMEA). They now use a wide range of health tracking technologies and computer systems at the heart of which lies sensitive patient data, thus making them increasingly attractive targets for hackers.

- Analysis by region:** While around 40% of firms across all regions struggle to turn risk awareness into management action, a higher proportion (more than half) of all firms in EMEA do not have a clear and well-documented understanding of their cyber risk profile. This is especially true of small and medium-sized firms in the region, many of which are making greater use of the internet and are becoming more exposed to potential cyber threats.¹³ Other regions fare little better. While resource constraints at smaller firms may explain why they are less likely to carry out regular risk assessments, over 40% of larger firms globally also fall short of best practice in this area.



¹² For example, an attack on Yahoo in 2014 only came to light about two years later in August 2016 after reports of a separate breach were being investigated. See <http://www.reuters.com/article/us-yahoo-cyber-idUSKCN11S16P>

¹³ See for example, Potential business impact of 'cybercrime' for small and medium enterprises (SMEs) in 2015, Zurich, <https://www.zurich.com/en/media/news-releases/2015/2015-1203-01>

Role of cyber insurance



Figure 8: Corporations' cyber insurance buying behaviour (by risk perception)

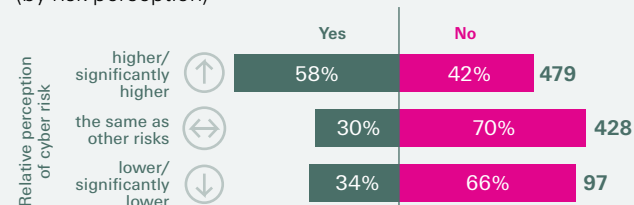


Figure 9: By firm size

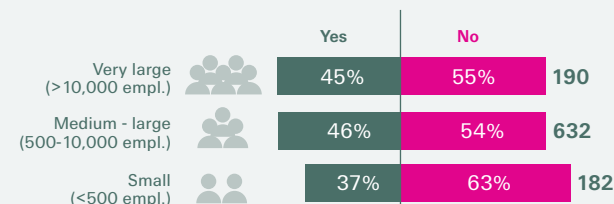
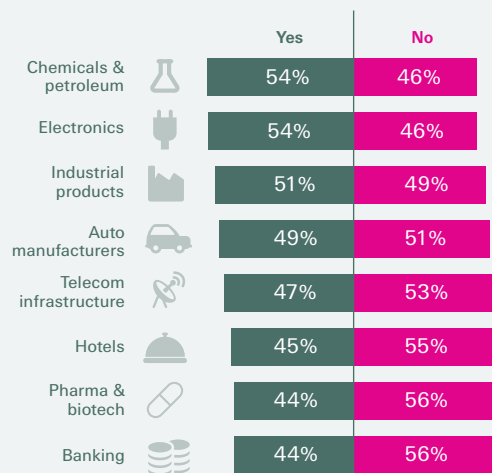


Figure 10: By industry (top eight purchasers)



Q. Corporations - Do you currently have a specific cyber insurance policy?

Insurance purchase patterns

- As expected, firms that rank cyber as a high risk are more likely to buy cyber insurance than firms that do not (see Figure 8). Studies show that the benefits of insurance in terms of added rigour in risk management may be as important as the actual loss indemnification.¹⁴
- **Analysis by region:** Just under 50% of firms report buying cyber cover, with little variation across regions. However, anecdotal evidence and other surveys show that cyber insurance penetration outside of the US is currently much lower than our survey results suggest.¹⁵ This highlights an important issue: corporations may be living under an illusion of protection amidst continued ambiguity about what cyber risks are covered as add-ons to existing property/liability policies, and which are not. Insurers and firms need to address this perception gap.

- **Analysis by industry and firm size:** Companies in the electronics, chemicals & petroleum, and industrial products sectors are most likely to purchase cyber insurance (see Figure 10). Small companies do not yet seem to have considered buying cyber cover despite their potentially greater vulnerability (see Figure 9). Recent studies show that smaller firms typically have fewer defences against breaches and are becoming more regular targets and need to be prepared.¹⁶

"Greater use of standalone-types of cover would help to bring greater transparency to the market place and avoid the piecemeal process of various exclusions across different types of policies."

Risk Director, US car manufacturer

¹⁴ The US Department of Homeland Security is hoping cyber insurance can act as an incentive for having a better security posture, which can be done by offering more coverage and lower premiums to organisations that follow best practices and maintain strong cybersecurity. <https://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf>

¹⁵ According to Marsh's European 2015 Cyber Risk Survey Report, only 12% of European organisations had bought cyber insurance

¹⁶ Beazley Breach Insights, July 2016, discovered that there was a sharp rise in data breaches in H1 2016, with most of the attacks targeting small banks and credit unions. <https://www.beazley.com/Documents/2016/201607-Beazley-Breach-Insights.pdf>

Role of cyber insurance



Table 2: Barriers to purchasing cyber insurance (by industry)

Reasons for not buying cyber insurance	We have not explored coverage (144 firms)	We are self-insured (136)	Do not feel we have sufficient exposure (135)	Feel coverage is illusory (121)	Feel coverage is too expensive (116)	Inadequate available coverage (terms, limits) (105)	Don't understand products on the market (78)	Believe we are covered by traditional insurance (55)
Auto manufacturers 								
Banking 								
Chemicals & petroleum 								
Consumer Products 								
Electronics 								
Health care 								
Hotels 								
Industrial products 								
Media 								
Pharma & biotech 								
Professional services 								
Retail 								
Telecom infrastructure 								
Transportation 								
Utilities 								

- **Barriers to purchase:** The main reason for not buying insurance is that firms have not explored it. But some prefer to self-insure. As part of enhanced risk management practices, some corporates are considering setting up captives to manage their cyber exposures. Others feel they do not have sufficient exposure to cyber risk, and a number of corporations, especially those in Asia Pacific, feel cover is illusory. There is also a segment of corporations who balk at the cost of insurance; especially companies with fewer than 1000 employees
- **Analysis by industry:** There are wide variations across industries (see Table 2). Firms in consumer and industrial products, and in media feel it is too expensive, while there are firms in electronics, healthcare, and telecom that have not yet explored coverage. Some banks, hotels, pharma and utility companies have a strong preference to self-insure. Auto manufacturers, chemical and petroleum, and transportation firms are most likely to believe that coverage is illusory.

“What large firms are looking for is a way to transfer the tail risks associated with cyber exposures to insurers who ought to be better placed to absorb the risk.”

Risk Director, US car manufacturer

Q. Corporations – Do you currently have a specific cyber policy to insure yourself against risks of digital interconnectedness? Why not?

Lowest ranked reason  Highest ranked reason

Role of cyber insurance



Table 3: Barriers to purchasing cyber insurance (by region)

Reasons for not buying cyber insurance		We have not explored coverage (144 firms)	We are self-insured (136)	Do not feel we have sufficient exposure (135)	Feel coverage is illusory (121)	Feel coverage is too expensive (116)	Inadequate available coverage (terms, limits) (105)	Don't understand products on the market (78)	Believe we are covered by traditional insurance (55)
Global 									
North America 									
Asia Pacific 									
EMEA 									
South America 									

Lowest ranked reason  Highest ranked reason

Q. Corporations – Do you currently have a specific cyber policy to insure yourself against risks of digital interconnectedness? Why not?

- **Analysis by region:** Across the main regions, corporations offer different reasons for not buying insurance (see Table 3). Awareness has not yet translated into action, especially in Latin America and EMEA where firms have typically not explored coverage, even though many (56% in Latin America, 24% in EMEA) rank cyber as a high risk. Corporations in emerging markets in Latin America and Asia are more likely to retain cyber-related risks than firms in other regions.
- **Risk profile of non-buyers** (not graphically represented): It is understandable that those firms that do not see cyber risk as significant will choose not to buy dedicated insurance. Yet even among firms that rank cyber as a high risk, more than a third chose not to buy cover (35% of non-buyers rate cyber as a higher risk now; 55% rate it higher in 10 years). These firms seem not to view cyber insurance, at least in its current guise, as an optimal mechanism for risk transfer.

Role of cyber insurance

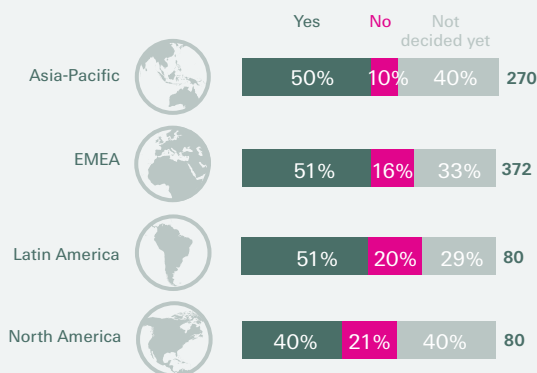


Figure 11: Insurers' views on the structure of cyber insurance



Q. Insurers – Risks of digital interconnectedness insurance is currently offered as separate, or existing coverage?

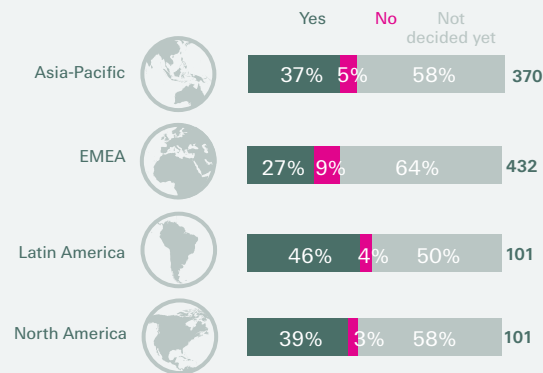
Figure 12: Insurers' intentions (by region)



Q. Insurers – Do you plan to write cyber insurance?

Q. Insurers – Do you plan to write cyberinsurance in the future?

Figure 13: Corporations' intentions (by region)



Q. Corporations – Do you plan to buy (more) cyber insurance?

Insurers' appetite for cyber offerings

- **Cyber insurance capacity:** Insurers that currently offer cyber insurance (46% of the sample) view the world differently from their peers who do not. They see a greater increase in the frequency and severity of incidents that could potentially affect their clients, and are presumably better prepared to assume and manage the risks. These insurers are ready to invest in the necessary technology to monitor and evaluate cyber threats (55% vs. 38%), and are more open to the idea that this will promote highly flexible insurance solutions. They are also slightly more hopeful than insurance companies which do not offer cyber policies that acceptance of data and information sharing among firms will increase, enabling greater risk transfer.
- **Type of policies:** The majority of insurers (63% in Figure 11) that sell cyber insurance do so as separate coverage. The offering mix is very similar across regions. Larger insurers (> USD 5bn premium) are slightly more likely to offer separate cover (70%). Studies show that standalone policies are evolving to reflect the emerging risks, and on current trends remain the most likely way to secure protection.¹⁷
- **Outlook:** There is significant interest from insurers to step up their cyber protection capabilities. Half of those who currently do not offer cyber insurance plan to do so in the next few years (see Figure 11 – right-hand panel). Insurers across most regions have similar aspirations (Figure 12). While about a third of insurers have not decided yet, there is a much larger proportion (around 60% in Figure 13) of corporations that are undecided about whether they will buy cyber insurance. Insurers therefore have their work cut out to tap into this segment of undecided potential customers. Very few corporations, and only 15% of insurers who do not offer cyber insurance, unequivocally rule out future involvement.

¹⁷ According to a recent report by the International Underwriting Association, cyber extensions, drop-down cover and standalone policies have evolved to reflect the emerging risks, and are the only way to obtain comprehensive protection. See http://www.iaa.co.uk/IUA_Member/Press/Press_Releases_2016/IUA_research_reveals_complex_cyber_risk_picture.aspx

Role of cyber insurance



Table 4: Perceived gaps in available coverage (by sector)

Which risks would you like to insure against where there are currently no insurance solutions available?	Business interruption via non-malicious (ie, "error")	Physical damage via a non-malicious IT error	Loss of intellectual property	Failure of utility service
Auto manufacturers 				
Banking 				
Chemicals & petroleum 				
Consumer products 				
Electronics 				
Health care 				
Hotels 				
Industrial products 				
Media 				
Pharma & biotech 				
Professional services 				
Retail 				
Telecom infrastructure 				
Transportation 				
Utilities 				
All sectors (coverages that are missing from the market) % of responses	38%	29%	23%	10%
% of insurers that write, or plan to write these risks	15%	14%	14%	17%

Coverage with the lowest gap  Coverage with the greatest gap

Q. Corporations – Which risks of digital interconnectedness would you like to insure against where there are currently no insurance solutions available?

Product innovation in cyber insurance

- **Scope of cover:** There are quite a few types of cover that companies would like to buy, but where they also see a lack of available insurance solutions (see Table 4). It could be that the nature of cyber risks that insurers are happy to take on (eg, small, routine cyber risks) are not really aligned with the risks that companies most want to shed (ie, catastrophic loss events). Less than 20% of insurers currently write or plan to offer cyber protection in areas where corporations have highlighted coverage gaps. The demand-supply mismatch is most pronounced in business interruption and physical damage due to non-malicious acts, although some new risks are being introduced into selected insurance policies.¹⁸
- **Additional services:** 70% of insurers either provide or plan to offer ancillary cyber-related services, mainly in partnership with third-party providers. A significant proportion (33%) of corporations already see value in add-on services. While many insurers offer post-breach services, moving into risk mitigation services gives them an opportunity to reduce risks during the term of the policy, and also potentially moderate claims and losses.

“Firms are looking to partner up with insurers; they want a tailored suit not one off the peg. They may not yet be sure what the shape of the body will be and are prepared to get the trousers first and the jacket later.”

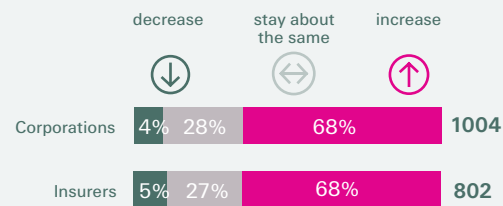
Senior risk manager, Asian-based conglomerate

¹⁸ Previously limited to liability and breach response, cyber insurance is reportedly expanding to include property and business interruption product options, although cover for reputational damage or loss of intellectual property remains rare. See, for example, Cyber/privacy insurance market survey – 2016, The Betterley Report, June 2016.

Role of cyber insurance

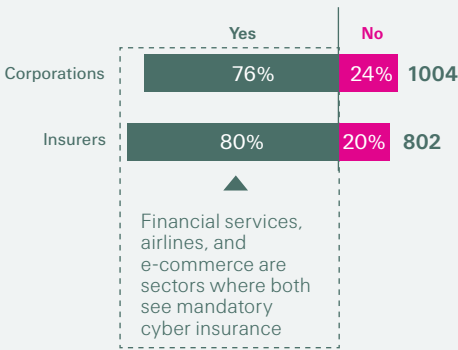


Figure 14: Insurers’ and corporates’ views on data sharing



Q. Will the acceptance of data and information sharing increase?

Figure 15: Insurers’ and corporates’ views on mandatory cyber insurance



Q. Should cyber insurance be mandatory for some industries?

Views on data sharing and mandatory insurance

Acceptance of data and information sharing

- There are few formal mechanisms to mandate or encourage sharing information about cyber-attacks or security breaches, yet the time seems ripe for data sharing arrangements and standards. Both insurers and firms agree that data sharing will only increase (see Figure 14), and two thirds (68%) are ready to consider this. This coincidence of views holds true across most regions, with the exception of Latin America where corporations (76%) are more open to data sharing than are insurers (60%).
- While it seems firms are warming to the idea of sharing what might be commercially sensitive information, insurers also need to demonstrate that the shared data will meaningfully improve their range of services. Corporations continue to view data sharing as a double-edged sword, fearing that information sharing within and across industries could even increase cyber risks significantly in the future.

Mandatory insurance for some industries

- The majority of both insurers (80%) and firms (76%) feel that cyber insurance should be mandatory in some industries (see Figure 15). Insurers in most regions seem keener on this idea than corporations, except in Latin America where 85% of corporations felt it would be beneficial (compared with 75% of Latin American insurers). Support for mandatory cover is strongest among the financial services (including insurance), airlines and e-commerce sectors, where both insurers and corporations agree that mandatory insurance would be beneficial.
- However, the role of government in this field will be complex. Government intervention is often seen as muddying the waters rather than helping. Consistent with that, 65% of firms and 48% of insurers see governments as accentuating cyber risks not reducing them, perhaps reflecting worries about increased potential for sensitive information to be leaked.

“A simple data dump to insurers is unlikely to be helpful – will insurers understand the information they receive?”

Senior risk manager, US multinational conglomerate

Conclusion

The spectre of cyber risk is evolving rapidly. Cyber threats are becoming more pervasive and potential sources of vulnerability are growing as digitalisation permeates ever deeper into economic life. But while risk awareness among corporates is already high and is increasing, in part reflecting heightened publicity of recent cyber-attacks and closer scrutiny from regulators and legislators, this does not yet seem to have translated into widespread improvement in mainstream risk management practices and strengthening of cyber defences.

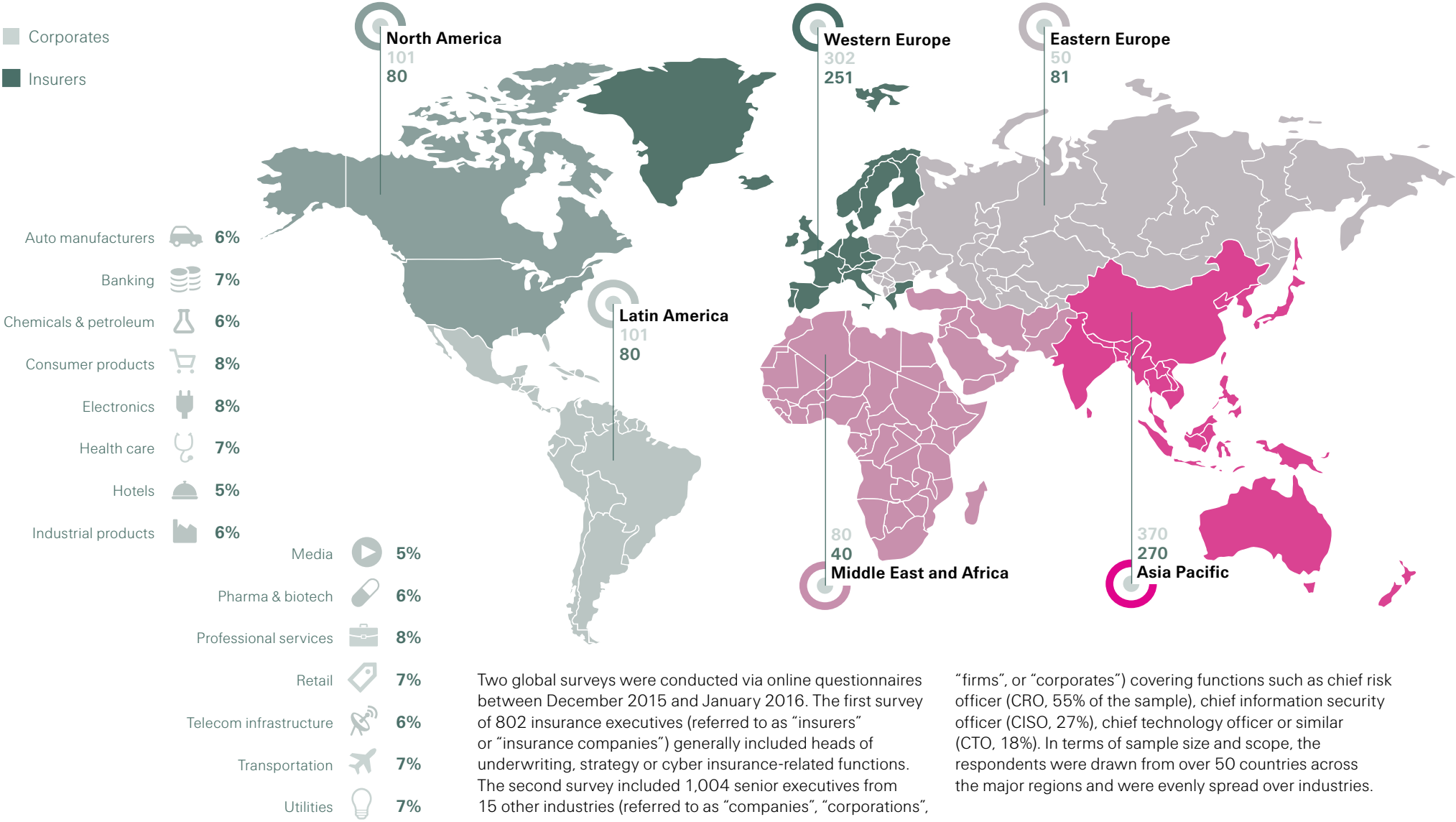
Cyber insurance can and should be part of a firm's armoury. Companies can transfer cyber-related risks to insurers more able to absorb the prospective losses and retain those they feel more comfortable managing themselves. More firms are considering purchasing specific cyber risk cover to guard against associated losses. This is especially important given some ambiguity about how far existing property and casualty policies cover cyber risks. But cyber risk insurance is a two-way street. If firms are serious in their demand for cyber protection, company risk profiles also have to improve, with greater investment needed in cyber security architecture and skilled staff in order to develop robust pre-and post-loss risk management procedures and capabilities. Firms also have to become comfortable with sharing potentially sensitive information, so that insurers can do a better job in assessing and underwriting the risks. Such a change in mindset is unlikely to happen as long as cyber security is positioned as a purely technical issue rather than a broader strategic business concern.

For their part, insurers have to develop a better understanding of the challenges that cyber threats present, and be more innovative in developing new and transparent products that genuinely meet their corporate clients' needs. A key issue will be to enhance their insurance offerings to address emerging gaps in cover while not overstepping the boundaries of insurability. Cyber risks are complex to understand and quantify, especially given the significant potential for losses from a single event to accumulate, and this has made insurers justifiably cautious. Completely new ways of thinking will be needed to calibrate cyber risks, determine what data are most needed to inform actuarial analyses, and how such data can be collected and made available in a manner that provides sufficient trust in their reliability. Insurers will need to develop new measurement frameworks and metrics that are sufficiently flexible to take into account rapid changes in the technological and business environment.

In short, insurance can play a central role in helping to boost cyber resilience in the global economy. To do so, the insurance industry must enhance its consultation and collaboration with corporations seeking or needing cover; IT-security companies developing new protection systems; and the authorities responsible for defining data exchanges, potential mandatory coverages and the possible role of the state as a re/insurer-of-last resort. If insurers do not respond to the latent corporate demand for dedicated cyber risk insurance and develop the technological expertise in the area of cyber security, new entrants with more technology expertise could fill the void. Some insurance companies seem to be ready to step up and are willing to invest in order to be able to underwrite this highly specialised risk, although insurers need to remain alert to the limits of their risk-absorbing capacity.

Appendix – Survey details

Geographical and industrial spread of respondents



Published by:

Swiss Re Ltd
Economic Research & Consulting
P.O. Box
8022 Zurich
Switzerland

Telephone: +41 43 285 2551
Fax: +41 43 282 0075
E-Mail: sigma@swissre.com

Armonk Office:
175 King Street
Armonk, NY 10504
Telephone: +1 914 828 8000

Hong Kong Office:
18 Harbour Road, Wanchai
Central Plaza, 61st Floor
Hong Kong, SAR
Telephone: + 852 25 82 5644

Authors and contributors:

Swiss Re
Darren Lee Pain
Jonathan Anchen
Dr. Maya Bundt
Dr. Eric Durand
Michael Schmitt

IBM Institute for Business Value
Christian Bieck

Editor:

Paul Ronke

The editorial deadline for this study was 19 September 2016.

The internet version may contain slightly updated information.

Graphic design and production:
Corporate Real Estate & Logistics / Media Production, Zurich

© 2016 Swiss Re All rights reserved.

The content of this report is based on a collaborative research project between Swiss Re and the IBM Institute for Business Value. The entire content of this study is subject to copyright with all rights reserved. The information may be used for private or internal purposes, provided that any copyright or other proprietary notices are not removed. Electronic reuse of the data published in this publication is prohibited.

Reproduction in whole or in part or use for any public purpose is permitted only with the prior written approval of Swiss Re Economic Research & Consulting and if the source reference is indicated. Courtesy copies are appreciated.

Although all the information used in this study was taken from reliable sources, Swiss Re does not accept any responsibility for the accuracy or comprehensiveness of the information given or forward looking statements made. The information provided and forward-looking statements made are for informational purposes only and in no way constitute or should be taken to reflect Swiss Re's position, in particular in relation to any ongoing or future dispute. In no event shall Swiss Re be liable for any loss or damage arising in connection with the use of this information and readers are cautioned not to place undue reliance on forward-looking statements. Swiss Re undertakes no obligation to publicly revise or update any forward-looking statements, whether as a result of new information, future events or otherwise.

Swiss Reinsurance Company Ltd
Mythenquai 50/60
P.O. Box
8022 Zurich
Switzerland

Telephone +41 43 285 2121
Fax +41 43 285 2999
www.swissre.com