Swiss Re Institute

No 1/2017

sigma

Cyber: getting to grips with a complex risk

Executive summary

The costs of cyber security breaches are growing significantly.

Cyber threats are evolving rapidly due to the growing digital transformation of society, the widespread use of internet-enabled devices and processes, and the changing profile of hackers. Recent high-profile cyber attacks demonstrate that the extent of associated possible losses is also broadening, increasingly comprising both physical and financial damage relating to data privacy breaches and to companies' tangible and intangible assets, and also business interruption costs. As a result, the issue of cyber protection is rising up the corporate agenda, at both large and small companies.

Despite increased awareness, many firms have yet to institutionalise cyber risk management.

Despite increased awareness, corporations are generally ill-prepared to cope with cyber risks. Relatively few firms have integrated cyber security into their mainstream risk management. This situation is not sustainable. Legislation is coming on-stream in many jurisdictions that will compel firms to introduce enhanced safeguards for their customers' private information or face heavy fines should they fall short of the required standards.

Dedicated cyber insurance is developing but the scale and scope of cover relative to exposure is modest.

Companies' first line of defence against cyber threats is greater investment in security technology and robust and comprehensive risk management practices. Many are also looking for external solutions to manage their cyber exposures, including transferring risks to third parties better-placed to absorb them. A dedicated cyber insurance market is developing rapidly with an increasing number of insurers looking to write more business in this specialty line. But some significant cyber-related risks remain largely uninsured and the scale of cover is modest compared with firms' overall exposures.

Insurers and companies are building models which eventually should underpin further risk transfer solutions.

Cyber risks are complex to understand and calibrate, especially given the significant potential for correlated exposures. The very fast changing technological environment and the lack of historical claims data from which to extrapolate information about future losses is a challenge. Insurers and their clients are nevertheless wrestling with different cyber risk modelling approaches. Even if full probabilistic models are still in their infancy, the experience of other perils offers hope that better, richer cyber risk models will eventually emerge as understanding of the fundamental risk drivers develops and more data about cyber losses become available.

Product and process innovation can help make cyber risks more insurable, but cooperation between companies and insurers is also essential.

Yet progress in addressing cyber risk should not be dictated by advances in risk modelling. Product and process innovation in insurance will help make cyber risks more insurable and extend available cover to a wider set of policyholders. This includes common standards for capturing, sharing and reporting data about cyber incidents, and greater use of smart analytics to improve threat detection and risk assessment. To expand the boundaries of insurability, companies will need to work with their insurers to create a market which is sustainable. Future development of new insurance-linked securities may in due course also enable certain cyber risks to be transferred to capital market investors.

The fast-changing cyber risk landscape

Costs of cyber breaches

Cyber security breaches are a growing threat and a top global risk.

Concerns about cyber risks have been increasing over recent years against the background of several cases of high-profile data and security breaches, including state-sponsored cyber attacks. Organisations like the World Economic Forum cite cyber attacks as one of the top risks facing the world today.[1] In business, the scope of potential physical and financial losses (first- and third-party) from a cyber-related incident is very broad, emphasising the pervasive nature of the associated risks.[2]

Threats go beyond lost/corrupted data and include losses from damage to property, reputation and business interruption.

Worries about the costs of a cyber attack/security breach are no longer confined to coping with lost, stolen or corrupted data, but increasingly include potential damage to a firm's property and reputation, and also the costs associated with business interruption (BI) or severe disruption to critical infrastructure. Losses may arise from a malicious attack either from inside an organisation or externally. Equally, they can be linked to accidental machine or human error. Table 1 provides some examples of the types of loss that can occur from cyber-related perils.

Table 1:
Types of cyber-related damage

Incident type	Examples
System malfunction/ issue	Own-system malfunction or malware infection, network communication malfunction, inadvertent disruption of third-party system, disruption of external digital infrastructure.
Data confidentiality	Exposure of own data; theft of third party data.
Data integrity / availability	Deletion, encryption or corruption of own or third-party data.
Malicious activity	System misuse, malicious communication, cyber fraud/theft.

Note: Malware, is an abbreviation for "malicious software", a type of program created to infect a computer and cause harm to it.

Source: Annex from *CRO Forum Concept Proposal categorisation methodology for cyber risk*, CRO Forum, June 2016.

The broader economic costs of a cyber breach can be significant.

A study in 2016 estimated the median cost of a data breach to be around USD 200 000 per firm.[3] However, the losses resulting from some incidents can be many multiples of that, pushing up the overall average costs (see Table 2). Several other studies have sought to quantify the broader economic impact of cyber incidents including BI costs, reputational damage and loss of future customers, physical damage costs etc.[4,5] For example, Lloyds of London estimates that cyber attacks cost businesses collectively as much as USD 400 billion a year, including the damage itself and subsequent disruption to normal course of business.[6] A study by

1 *The Global Risks Report 2016*, World Economic Forum, 2016.
2 First-party losses relate to expenses as a direct result of the incident (eg, cost of forensic investigation to determine cause, notifying affected consumers, public relations campaigns). Third-party losses relate to costs of private litigation, or fines/fees brought by government agencies.
3 S. Romanosky, "Examining the costs and causes of cyber incidents", *Journal of Cybersecurity*, August 2016.
4 A 2016 study by Ponemon Institute found that information loss is the costliest consequence of a cyber attack (39% of the cost) followed by business disruption (36%), which includes diminished employee productivity and business process failures after an attack. Revenue loss and equipment damages follow at 20% and 4%, respectively. See *2016 Cost of Cyber Crime Study & the Risk of Business Innovation*, Ponemon Institute, October 2016.
5 UK telecoms company TalkTalk reportedly lost 101 000 existing customers, fell short of its near-term customer acquisition target and incurred costs of GBP 60 million after a cyber attack in October 2015. S. Farrell "TalkTalk counts costs of cyber-attack", *The Guardian*, 2 February 2016, https://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave
6 S. Gandel, "Lloyd's CEO: Cyber attacks cost companies $400 billion every year", *Fortune*, 23 January 2015, http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/

McAfee shows similar aggregate loss estimates.[7] In addition, there are opportunity costs of time and resources when dealing with cyber incidents, and also lost benefits from discouraged investment. Corporates may err on the side of caution before committing more resources to building their digital capabilities, wary of potential new cyber risks that come with doing so.

Table 2:
Estimates of the financial costs, per selected cyber incident

Event type	No. of events	Mean cost (USD mn)	Median cost (USD mn)	Maximum cost (USD mn)
Data breach(1)	602	5.87	0.17	572
Compromised systems(2)	36	9.17	0.33	100
Privacy violation(3)	234	10.14	1.34	750
Illicit access(4)	49	19.99	0.15	710
Total	**921**	**7.84**	**0.25**	**750**

Notes:
(1) Unintentional disclosure of personally identifiable information (PII) stemming from loss or theft (eg, theft of computers containing personal information of employees or customers, by a hacker or malicious employee).
(2) Compromise or disruption of corporate IT systems or intellectual property (eg, a denial-of- service attack, theft, malicious infiltration and subsequent cyber extortion).
(3) Unauthorised collection, use and/or sharing of PII. Unlike (1) and (2), which refer to incidents "suffered by" a firm, this category relates to events "caused by" a firm (eg, a firm improperly collecting or selling PII).
(4) Computer or electronic crimes directly against other individuals or firms including phishing attacks, identity theft, or skimming attacks.

All data in Table 2 refer to a 10-year period from 2005 to 2014 for a sample of incidents where cost estimates are publicly available.

Source: S. Romanosky, "Examining the costs and causes of cyber incidents", *Journal of Cybersecurity*, August 2016.

Cyber security is becoming a serious issue for corporates…

Cyber risk has moved high up the corporate agenda as the consequences of a security breach have become more apparent. A recent Swiss Re/IBM survey found that 40% of companies were affected by a cyber incident in the past three years, and that 60% of all companies expect the risk to increase in the coming years.[8] This was true across all regions and industries, and not just in those areas or sectors where cyber attacks have recently been most prominent (eg, retail and healthcare).

[7] *Net Losses: Estimating the Global Cost of Cybercrime*, McAfee and Center for Strategic and International Studies, June 2014. The McAfee study assumed the cost of cyber crime as a constant share of national income, adjusted for levels of development. It used available national estimates to extrapolate a range of estimates for cyber crime costs from USD 375 billion to USD 575 billion. This includes both direct and indirect costs, loss of intellectual property, theft of financial assets and sensitive business information, opportunity costs, additional costs for securing networks, and the cost of recovering from cyber attacks, including reputational damage.
[8] *Cyber: in search of resilience in an interconnected world*, Swiss Re/IBM, October 2016.

… and not just at the largest firms.

Companies of all sizes are increasingly aware of the potential impact of cyber attacks and security breaches on their operations.[9] According to a September 2015 report, six out of 10 UK small businesses surveyed previously experienced a breach, and over half of those occurred in the previous year (63%).[10] The terms of agreement that small and mid-sized vendors sign with larger business partners sometimes make the former responsible for unlimited losses in case of a cyber event.[11] Should a serious cyber security breach occur, small firms can find it hard to recover, and many go out of business within six months of an incident.[12]

A rapidly morphing risk

Cyber risks will inevitably evolve further as new threat factors emerge.

Cyber risks are continually evolving. Three main features underscore the dynamic nature of cyber risk: the growing speed and scope of digital transformation, the widening sources of vulnerability from hyperconnectivity, and the evolution of threat actors.

The accelerating pace of digital transformation is a challenge for firms' IT security.

Accelerating pace and scope of digital transformation

Digital technology is permeating ever further into companies' internal processes and interactions with customers, and in many cases is creating new business models. Traditional security protocols to protect legacy systems are often ill- equipped to deal with the disruptive change created by new digital applications. New services may also be driven by firms' different business units without direct involvement of their risk management teams, making it difficult for existing internal controls to keep pace.[13] There is also a growing prevalence of "bring your own device" (BYOD) culture as companies allow employees, business partners and other users to utilise personal devices to run enterprise applications and access data. Gartner predicts that 90% of organisations will support some form of BYOD through 2017, making maintaining IT security more challenging.[14]

Firms may be underestimating the complexity that digital technology creates for their business models.

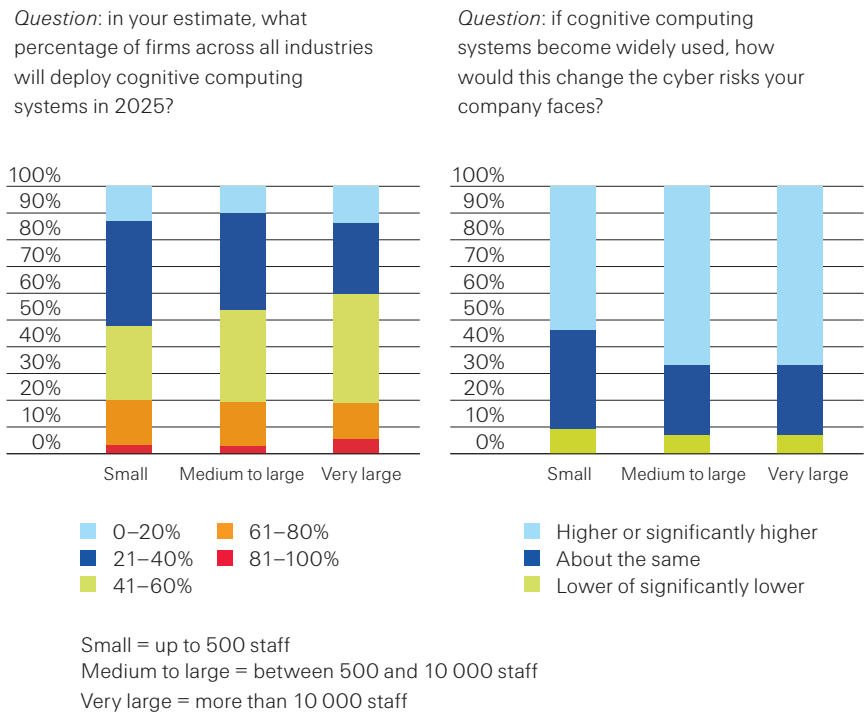
The philosophy in digital-led business is also very different from that in traditional business, creating additional security complications. In the digital world, firms move a product from design through to distribution to customers rapidly, and continuously improve the product as customer feedback arrives. CEOs often drive their organisations to move faster on digital transformation and innovation, and this can lead to underestimation of the embedded security and operational risks.[15] A recent survey indicated that 95% of companies recognise the risk landscape is changing due to digital technology. Even so, many firms classify their systems as simple when in reality they are complex.[16]

[9] Key risks for small and medium enterprises (SMEs) in 2016 - Global survey report, Zurich Financial Services, September 2016.
[10] *Small business reputation & the cyber risk*, KPMG and BeCyberstreetwise.com, September 2015.
[11] *Cyber/Privacy Insurance Market Survey — 2016*, The Betterley Report, June 2016.
[12] "Most Small Businesses Don't Recover From Cybercrime", *wsj.com*, 22 March, 2013, http://www.wsj.com/articles/SB10001424127887324557804578376291878413744
[13] *The Four Steps to Manage Risk and Security in Bimodal IT*, Gartner, 7 March 2016.
[14] *Gartner Predicts*, Gartner, January 2016.
[15] *Kick-Start Bimodal IT by Launching Mode 2*, Gartner, 29 April 2016.
[16] *The Risk of Complexity in a Digital Economy*, MIT and Infosys, June 2016.

Algorithmic-driven technologies can be used to launch new types of attacks, at scale.

Computers using sophisticated artificial intelligence (AI) algorithms can automatically search through millions of lines of software code to find weaknesses to exploit. Researchers have already demonstrated how machine-learning models can be stolen and reverse engineered to attack systems.[17] More generally, in a recent survey, 62% of respondents said that as AI becomes more prevalent, cyber and information security risk will increase,[18] echoing the findings of the recent Swiss Re/IBM survey (see Figure 1).

Figure 1:
Survey of corporations' views on adoption and risks of cognitive computing, by size of firm



Source: *Cyber: in search of resilience in an interconnected world*, Swiss Re/IBM, 2016.

Widening sources of vulnerability

The IoT increases the range of vulnerabilities...

The rapid spread of internet-enabled devices – the so-called Internet of Things (IoT) – is enabling new ways of communication, information sharing and business steering/directing (eg, remote operations). But it also increases the range of vulnerabilities. Over time IoT will create an entire world of digitally-interconnected devices, ranging from every-day household appliances items like smart toasters to unmanned aerial vehicles (UAVs) or drones and fully- autonomous vehicles.

... as connected devices may have weak security standards.

Some of these devices may have poor security, or even none at all, and can be open to malicious hackers, especially if they are exposed to vulnerabilities for which no patch or fix is available. For example, connected networks can be harnessed in distributed-denial-of-service attacks (DDoS), which enlist poorly-protected IoT devices to bring down other web-connected services.[19] Weak network security is especially concerning because a dominant application of the IoT will be in industrial processes and government infrastructure, not merely consumer devices.[20] The

[17] F. Tramèr, F. Zhang, A. Juels and T. Ristenpart, *Stealing Machine Learning Models via Prediction APIs*, USENIX Association, August 2016.
[18] *State of Cybersecurity: Implications for 2016*, an ISACA and RSA Conference Survey, 2016.
[19] H. Kuchler, "Connected devices create millions of cyber security weak spots", *Financial Times*, 23 October 2016, https://www.ft.com/content/a63b2de8-992c-11e6-8f9b-70e3cabccfae
[20] Businesses will spend a significant sum on IoT hardware in 2017 (USD 964 billion), and consumers (USD 725 billion). See *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*, Gartner, 7 February 2017, http://www.gartner.com/newsroom/id/3598917

constant interaction between remote devices and their environment provides many potential attack surfaces for the would-be hacker.

Growing cloud usage brings lower transparency and new threats.

The widespread adoption of cloud computing further complicates the problem of cyber security.[21] Lack of transparency is a challenge in a decentralised environment as firms grapple with which cloud services are in use, who is responsible and how a provider secures data from its own IT staff.[22] Cloud-hosted systems are also vulnerable to new types of malware that can seek out virtualised environments to infect.[23] And file sharing apps are susceptible to hacking even with strong security standards, because users can inadvertently introduce their own vulnerabilities like shared passwords.

Evolution of attacker profiles

The advent of low-cost hacking tools and collaboration is widening the set of attackers.

Attacker profiles are also changing (see Figure 2). Low-cost hacker toolkits drive down the cost of hacking and lower the barriers to entry for a wider class of attackers, not just those with highly specialist IT skills.[24] DDoS attacks provide a good illustration: they are relatively cheap to carry out, yet often expensive to prevent and resolve. For example, in 2016 the Mirai malware used a multitude of household internet-connected devices to launch DDoS attacks.[25] Collaboration among hackers is also becoming more prevalent, with malware being shared anonymously on web-based forums.

Figure 2:
Expansion of attacker types, resources and motivations

	Amateurs	Hacktivists	Organised crime	State sponsored
Resources	Limited technical resources	Vast networks Strong emotional commitment	Significant technical resources	Constrained only by government budget
Motivations	Fame and notoriety	Make a statement, cause embarrassment	Economic gain	Boost to innovation Leverage in negotiations
Sophistication	Not professional Uses known exploits	Sometimes low-sophistication, relentless and targeted	Professional, established syndicates	Highly sophisticated, patient, creative, persistent

Source: Swiss Re Economic Research and Consulting.

The economic gains from cyber crime are becoming much bigger.

Once driven largely by fame and attention, hackers increasingly recognise the economic gains from successful cyber attacks. Established crime syndicates with access to significant technical resources and capabilities are finding cyber crime a lucrative endeavour. State-sponsored attackers are engaging in cyber disruption and corporate espionage to access secret information, or gain unfair competitive

[21] Gartner predicts that by 2020, a corporate "no-cloud" policy will be outdated. See Gartner Says By 2020, a Corporate "No-Cloud" Policy Will Be as Rare as a "No-Internet" Policy Is Today, *Gartner*, 22 June 2016, http://www.gartner.com/newsroom/id/3354117

[22] The term "shadow IT" is sometimes used to describe the situation where business units procure new software/architecture without scrutiny of internal IT. See C. Pettey, *Don't Let Shadow IT Put Your Business at Risk*, Gartner, 3 May 2016, http://www.gartner.com/smarterwithgartner/dont-let-shadow-it-put-your-business-at-risk/

[23] D. Shackleford, "Malware analysis: How some strains 'adapt' to virtual machines", *TechTarget*, June 2015, http://searchsecurity.techtarget.com/feature/Malware-analysis-How-some-strains-adapt-to-virtual-machines

[24] Technically proficient attackers are reportedly spending an average of USD 1367 for specialised toolkits to execute attack. See *Flipping the Economics of Attacks*, Ponemon Institute, January 2016.

[25] These new types of malware are often constructed as updating software platforms to which hackers can add more functionality over time. See L. H. Newman, "The Web-Shaking Mirai Botnet Is Splintering — But Also Evolving", *Wired*, 15 November 2016, https://www.wired.com/2016/11/web-shaking-mirai-botnet-splintering-also-evolving/

advantage. For instance, bidding for international tenders, or developing "leapfrog" innovation by reducing R&D costs through intellectual property theft.

Hackers are using more sophisticated techiques to capture confidential information.

Attackers are also becoming more sophisticated, targeting a firm's employees with novel manipulative methods. Company employees are often instrumental in propagating attacks, either maliciously or by accident. In 2015, phishing and social engineering techniques ranked among the most successful attack methods to exploit enterprise networks.[26] Over time users may become aware of well-known phishing frauds and learn to recognise dubious emails, but it is hard to keep up with the new ways of tricking people into breaking normal security procedures.[27] Widely-used public platforms can also be compromised in innovative ways. For instance, in 2016 hackers demonstrated how AI can be used to create personalised tweets, and entice targets to click on malicious links.[28]

Ransomware is also a rapidly growing threat.

Cyber extortion is also becoming a popular technique used by criminals, alongside more conventional approaches such as stealing and selling private information on the black market.[29] Ransomware is a kind of malware designed to block access to a computer system or data until a sum of money is paid, often in Bitcoin. Industrial IoT ecosystems are especially vulnerable, where threats by hackers to interrupt operations could prompt a ransom payment if the loss of productivity is substantial and/or where continuous operation is critical.[30] According to the FBI, there were 2400 ransomware incidents in the US in 2015 (up from 1800 in 2014), which resulted in estimated losses of USD 24 million.[31] Elsewhere, data from AIG Europe show that ransomware and extortion account for the largest number of claims on cyber insurance policies in Europe, more than data breach incidents.[32] While individual losses from such attacks remain relatively small, the development of the "ransomware-as-a-service" business model whereby malware creators sell their code to multiple users and receive a share of any profits earned, significantly increases the potential scale and scope of any attack.[33]

[26] Phishing is the attempt to obtain sensitive information by impersonating a trustworthy entity in an electronic communication. Social engineering is psychological manipulation of people into divulging confidential information. See ISACA and RSA Conference Survey, op. cit.

[27] An example of sophisticated social engineering is a recently-publicised case of deceptive fund transfer where employees were unknowingly manipulated into transferring company funds into fraudulent accounts after receiving emails from criminals impersonating an authorised executive. See "Central banks seek global standards in wake of Bangladesh heist", *Reuters*, 15 September 2016, http://www.reuters.com/article/us-cyber-heist-basel-taskforce-idUSKCN11L269

[28] T. Simonite, "This AI Will Craft Tweets That You'll Never Know Are Spam", *MIT Technology Review*, 4 August 2016, https://www.technologyreview.com/s/602109/this-ai-will-craft-tweets-that-youll-never-know-are-spam/

[29] N. Elliott, "Ransomware Is Booming and Companies Are Paying Up", *WSJ Risk & Compliance Journal*, 27 October 2016, http://blogs.wsj.com/riskandcompliance/2016/10/27/ransomware-is-booming-and-companies-are-paying-up/

[30] B. Dickson, "What makes IoT ransomware a different and more dangerous threat?", *Tech Crunch*, 2 October, 2016, https://techcrunch.com/2016/10/02/what-makes-iot-ransomware-a-different-and-more-dangerous-threat/

[31] V.D. Anderson, "Ransomware: Latest Cyber Extortion Tool", *FBI Cleveland*, 26 April 2016, https://www.fbi.gov/contact-us/field-offices/cleveland/news/press-releases/ransomware-latest-cyber-extortion-tool

[32] P. Lucas, "Top cyber claim causes revealed by AIG", *Insurance Business*, 29 November 2016, http://www.insurancebusinessmag.com/uk/news/breaking-news/top-cyber-claim-causes-revealed-by-aig-41109.aspx

[33] See for example, "Ransomware-as-a-Service: Ransomware Operators Find Ways to Bring in Business", *Trend Micro*, 2 September 2016, http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-ransomware-operators-find-ways-to-bring-in-business

Cyber risk management in practice

Lack of action

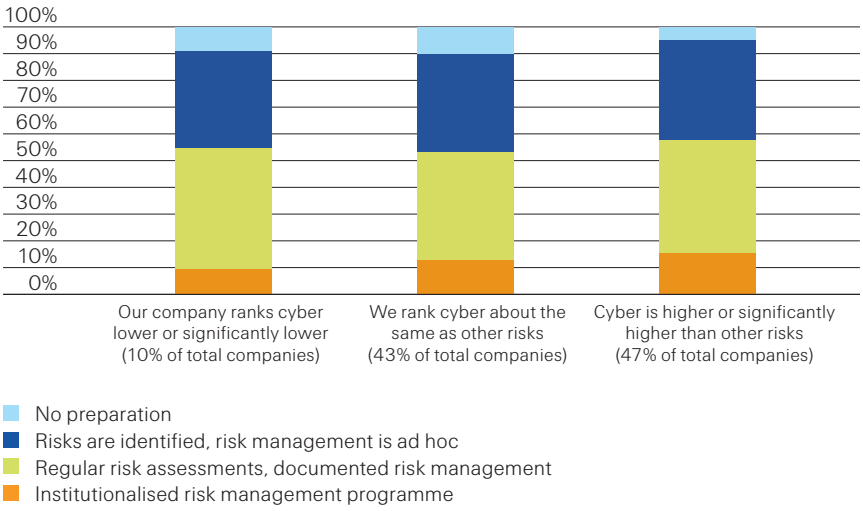
Awareness is increasing, but firms have not institutionalised cyber risk management.

Companies have developed increased appreciation of cyber risks, but it is not clear that this has translated into concrete and comprehensive action plans. Consistent with other recent studies, the 2016 Swiss Re/IBM survey found relatively few firms have institutionalised cyber risk management, even among those which see cyber as a significant threat (see Figure 3). Relatively few firms have a formal cyber risk management strategy outlining their overall risk appetite and detailed procedures to monitor vulnerabilities.[34]

Figure 3:
Survey of corporations' view on their risk preparedness

Question for horizontal axis answers: where do you currently rank your risks of digital interconnectedness as a threat relative to any other risk topics that affect your company? (lower/same as/higher)

Question for vertical axis answers: To what extent are you prepared for risks of digital interconnectedness incidents? (grouping firms in % shares according to ranking of cyber risk relative to others: lower/same as/higher).



Source: *Cyber: in search of resilience in an interconnected world*, Swiss Re/IBM, 2016.

Firms may be underestimating the possibility of being repeatedly hit by cyber attacks.

One reason for inaction could be complacency: firms may be underestimating the likelihood of being attacked multiple times. A recent survey by Lloyd's of London found that among the 92% of businesses which suffered a cyber security breach in the past five years, only 42% were concerned that another breach will happen in the future.[35] More generally, according to the security analytics firm Advisen, limited progress on risk mitigation efforts are caused by a combination of factors including limited resources, engagement and knowledge.[36] In turn this may be linked to cyber security in many organisations still being considered a technical rather than a broader strategic issue.[37] Though now often part of regular reporting to top management, cyber security monitoring is still typically driven by the IT function.

[34] For further discussion of institutionalised cyber risk management see *Enhanced Cyber Risk Management Standards* published by Department of the Treasury, Federal Reserve System and the Federal Deposit Insurance Corporation, October 2016, https://www.federalreserve.gov/newsevents/press/bcreg/bcreg20161019a1.pdf

[35] *Facing the cyber risk challenge*, Lloyd's of London, September 2016.

[36] J. Bradford, *Public-private partnership is key to combating cybercrime*, Advisen, http://www.advisen.com/tools/fpnproc/fpns/articles_new_23/P/263440646.html?rid=263440646&list_id=23

[37] Gartner reviewed more than 400 board presentations on cyber risk and found that the majority fail to resonate with the business because they focus on technical measures and operational metrics. See J. Wheatman, P.E. Proctor, R. McMillan, *The Comprehensive Guide to Presenting Risk and Information Security to Your Board of Directors*, Gartner, 3 March 2016.

Companies in some emerging markets may be especially ill-prepared.

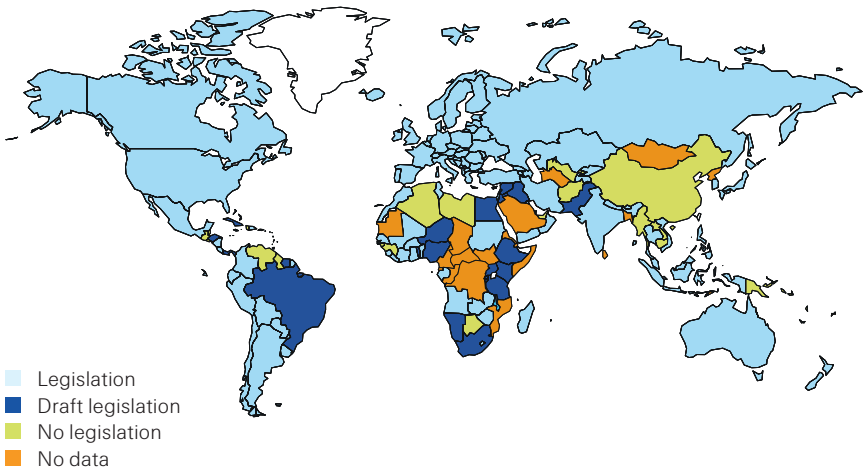
There are regional disparities with emerging markets seemingly least prepared. A report on the Asia Pacific region found that firms were not able to detect attackers in their environments for a median of 520 days, which is much higher than the global median of 146 days.[38] A further issue is that companies in these markets use custom software which may not always receive the kind of scrutiny that big software companies apply to their products. At the same time, it is difficult to assess the true extent of under-preparedness in many emerging markets as often companies and governments are not required to disclose attacks.[39]

Heightened regulatory scrutiny of cyber issues

Regulators globally are demanding that companies and institutions do more to protect consumer data.

Regulators and legislators are pushing for change to ensure that cyber security breaches are neither a source of systemic instability nor unduly harm consumers that rely on organisations to safeguard their private information. Around the world, 107 countries (of which 66 are developing economies) have enacted legislation that calls for the protection of data and privacy (see Figure 4). Less than 40% of countries in Asia and Africa have a law in place, although draft legislation is typically in the pipeline in these regions.

Figure 4:
Data protection and privacy laws worldwide



Source: UNCTAD Global Cyberlaw Tracker; data extracted on 1 December 2016.

[38] B. Boland, "M-Trends Asia Pacific", *www.fireeye.com*, 24 August 2016, https://www.fireeye.com/blog/threat-research/2016/08/m-trends_asia_pacifi.html

[39] L. Lewis, D. Weinland, M. Peel, "Asia hacking: Cashing in on cyber crime", *Financial Times*, 19 September 2016, https://www.ft.com/content/38e49534-57bb-11e6-9f70-badea1b336d4

New data protection regulations impose stringent requirements with far reaching but uncertain consequences.

Under the new European Union (EU) General Data Protection Regulation (GDPR) which takes effect in 2018, European companies will face significant fines if they fail to protect data.[40] Firms must also be able to purge an individual's details from their systems if that information is no longer relevant or necessary, which can be difficult if data are fragmented across organisations and/or there is limited visibility on information held externally. However, companies do not yet appear to have absorbed the serious financial and legal consequences of non-compliance. A recent survey by Lloyds of London found that the understanding of the implications of EU GDPR is low: 57% said they know "little" or "nothing" about the new regulations.[41] Another survey found that of respondents from Europe, the Middle East and Africa (EMEA), a fifth have not started preparing for GDPR, and only a quarter are completely prepared for its introduction. Likewise, in Australia barely a third of surveyed IT decision makers feel completely prepared to handle mandatory breach notifications as part of amendments to the Australia Privacy Act set to come into force in 2017.[42]

Evolving legal interpretations also complicate firms' efforts to estimate costs from cyber breaches.

Changes in cyber case law could also drive litigation and increase settlement costs, although the fragmented and still emerging legal precedents make it difficult to calibrate the future impact. For example, US courts allow law suits to proceed in some instances where the mere possibility of identity theft following a data breach counts as an injury that might merit compensation. Previously, courts could dismiss data breach suits if plaintiffs could not show that damage was suffered.[43] While these cases have often been settled out of court, in future it may only be necessary to show that data were released for firms to face legal sanction.

And compliance requirements have implications for all parties in a supply chain.

Regulatory pressures will impact how all parties in a company's supply chain think about cyber risk, as compliance requirements and liability for damages from a breach are increasing for all. For example, the US Pentagon must be notified if any of their contractors or sub-contractors suffer a cyber attack. But more broadly, not all companies or institutions are fully aware of the risks embedded in their supply chain. For example in Europe, 80% of companies do not assess the cyber risk profile of their suppliers.[44]

Growing cyber insurance market

Demand for cyber insurance is increasing, underpinning a rapid increase in aggregate premiums.

In the context of growing cyber hazards, widening sources of vulnerability and heightened regulatory pressure, demand for insurance protection against cyber risks is increasing. According to Zurich/Advisen, the proportion of firms reporting that they buy cyber liability insurance has almost doubled since 2011.[45] And a Swiss Re/IBM survey found that firms are increasingly considering purchasing specific cover to guard against cyber-related losses. The market for standalone cyber insurance is growing rapidly: estimates from different insurance institutions vary (see Figure 5), but suggest annualised cyber insurance premium growth of at least 15% over the next 5 to 10 years

[40] Fines will depend on the incident and type of violations. But in general, infringements of key GDPR provisions are subject to administrative fines up to EUR 20 million or up to 4% of global turnover, whichever is higher. Lesser infringements are subject to administrative fines up to EUR 10 million or up to 2% of global turnover, whichever is higher.

[41] Lloyd's of London, op. cit.

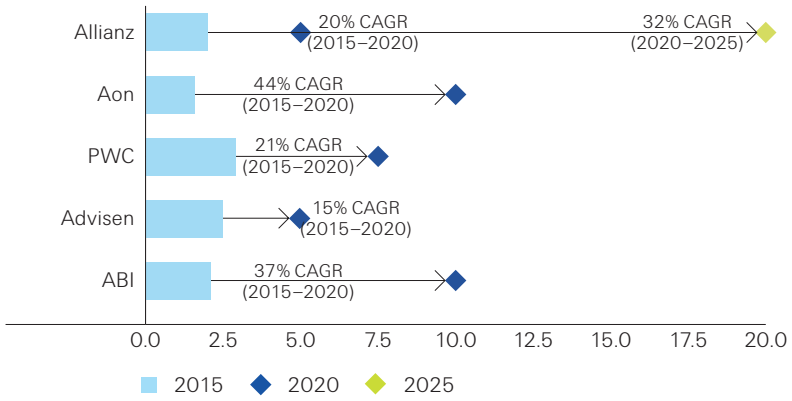
[42] *Global Advanced Threat Landscape Survey 2016*, CyberArk, 2016.

[43] N. Hong, "For Consumers, Injury is Hard to Prove in Data-Breach Cases", *WSJ*, 26 June 2016, http://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988

[44] *Continental European Cyber Risk Survey: 2016 Report*, Marsh, October 2016.

[45] *Information security and cyber risk management*, Advisen/Zurich, October 2016.

Figure 5:
Estimates of worldwide cyber insurance premiums (2015-2025), USD billion, by selected market participants



Source: Allianz, Aon, PwC, Advisen, ABI, Swiss Re Economic Research and Consulting.

Cyber policy limits typically range from USD 5 million to USD 100 million.

Dedicated cyber insurance typically provides core protection against data and network security breaches and associated losses, with capacity limits ranging from around USD 5 million to USD 100 million. Most policies are written on a "claims-made and reported" basis meaning that claims must be notified to the insurer during the policy period, or at most within 30 to 60 days of policy expiration.

The cyber insurance market is fairly concentrated although more insurers are looking to enter.

The cyber insurance market is still relatively concentrated. Three insurers (AIG, Chubb and XL Group) reportedly have around 45% of the market in the US.[46] That seems likely to change, however, with many insurers looking to expand their cyber protection capabilities. Half of the insurers questioned in the Swiss Re/IBM survey who currently do not offer cyber insurance plan to do so in the next few years.

[46] "AIG, Chubb, XL Group Lead in US Cyber Coverage Market Share: Fitch Ratings", *Insurance Journal*, 6 September 2016, http://www.insurancejournal.com/magazines/features/2016/09/06/424904.htm

Cyber insurance is a relatively new business line. The US is the largest market.

Evolution of cyber insurance

Insurance for cyber risks is a relatively new business and one that is evolving rapidly. The first dedicated policies appeared in the US in the late 1990s and targeted privacy/security liability issues arising with the growing use of the internet (see Figure 6). The US remains the largest market for cyber insurance, accounting for most of the USD 2 billion-USD 3 billion in worldwide premiums in 2015, although much of US cover is written by international insurers (eg, via the London Market).

Figure 6:
Major milestones over recent decades in the development of standalone cyber insurance policies

1990s

- Standalone products emerged in the US in the mid/late 1990s. Evolved from professional liability policies (eg, E&O, D&O).
- First policies written to address exposure to online content or software.
- These "internet insurance" policies:
  - were limited to computer security failures;
  - did not provide coverage for first-party costs from a data breach; and
  - did not extend to non-electronic records or accidental disclosure.

2000s

- Online media policies began to include losses from "unauthorised access", "network security", and "viruses". But there were significant exclusions (eg, actions of rogue employees and regulatory fines) and no first-party cover.
- Mid 2000s, cover introduced for some first-party losses (eg, cyber business interruption, cyber extortion) and damage from accidental data breaches.
- US data privacy regulations catalysed product innovation, including protection against costs incurred for IT forensics, PR and customer notification.

2010s

- Growth in number of carriers with standalone products, not just in US.
- Increased reliance on IT and high-profile hacking scandals boosted demand for cyber insurance globally (both dedicated cover and endorsements to traditional property/casualty policies).
- EU authorities reach agreement on data protection reform; legislation to be implemented in 2018.
- Data protection legislation in other jurisdictions coming on-stream, raising awareness of cyber threats and need for protection.
- Insurers partner with external IT experts to deepen knowledge of cyber risks.

Source: Swiss Re Economic Research & Consulting.

Standalone cyber policies differ but most blend loss protection for various data and network security breaches.

Different insurers use different terminology, but nowadays standalone cyber coverage typically blends some combination of the following components:

- *Network, IT security failure:* BI insurance, covering an insured's loss of income, operating expenses and often data restoration costs when business operations are interrupted or suspended due to a failure of IT security as a result of malicious attack, including DDoS events.
- *Network, IT system failure:* BI insurance, with similar coverage to security failure (above) but when business operations are interrupted or suspended due to failure of IT systems (non-malicious cyber events) and sometimes human error/mishap.
- *Contingent business interruption (CBI):* covers the insured's loss of income and operating expenses in case of a disruption at a digital supplier (eg, a cloud provider) and in some cases also at a conventional utility service (eg, electricity) provider.
- *Privacy breaches:* covers claims relating to expenses incurred in the response to a data breach, including crisis management costs (eg, IT forensic costs, notification costs and in some cases regulatory fines).
- *Network liability:* covers damages at a third-party provider as a result of a disruptive event coming from or passing through the insured's system.
- *Errors and omissions:* covers claims arising from errors in the performance of services provided, including software and consulting.
- *Media liability:* covers claims such as infringement of intellectual property, copyright/trademark infringement and libel and slander.
- *Cyber extortion:* covers claims relating to the extra costs incurred in dealing with an infection coming from ransomware and – where legally allowed – the ransom if deemed necessary to pay it.

Originally aimed at privacy/security liability costs, cyber insurance has broadened to include other types of loss.

Cyber policies were originally designed to cover non-physical perils and damage to intangible assets. These include the cost of notifying individuals, credit monitoring, IT forensics, public relations and crisis management and communication. But over time the cover has broadened. Now some cyber products are combined with other insurance policy types, such as technology errors and omissions liability insurance.

Some important cyber-related risks nonetheless remain uninsured ...

Over time, cyber insurance has evolved to include more risks, but many firms still highlight a lack of availability of cover for some cyber-related risks (see Figure 7). According to a 2016 survey of corporate insurance buyers, two highlighted reasons for not purchasing cyber-cover are inadequate coverage and the scarcity of relevant insurance solutions.[47] For example, many insurers offer BI cover in their cyber policies, but some companies say the limits are too low to cover the potentially very large losses that a cyber event could trigger, although the situation is improving as limits have progressively increased.

... including both physical and non-physical damage.

Aside from BI, another area of shortfall in cover is for physical damage. Few insurers include bodily injury and property protection in their standalone cyber insurance, though some related losses might be covered under traditional property and liability insurance.[48] Cyber policies usually have war exclusions and even those that cover cyber terror will typically exclude damages not covered in traditional cyber policies (like loss of property and damage to physical assets).[49] For example, a major source of contention between insurers and their insureds reflects lack of clarity on what may be deemed a cyber attack and an act of cyberterrorism.[50] Similarly, reputational risk is seldom covered by cyber insurance.[51] Insurers also tend to offer minimal cover for intellectual property (IP) theft and damage from industrial espionage. And where it is offered, some businesses consider the limits for IP insurance to be too low.[52]

[47] More generally, over half of respondents to the 2016 annual survey of members of the Association of Insurance and Risk Managers in Industry and Commerce (Airmic) cite a lack of cyber insurance. See *The top priority risks are also among the most difficult to insure*, Airmic, 7 June 2016, https://www.airmic.com/news/press/top-priority-risks-are-also-among-most-difficult-insure

[48] AIG's CyberEdge PC product introduced coverage that provides bodily injury and property damage protection that may result from a cyber attack. The coverage is provided on an excess-and-difference-in-conditions basis (meaning the insured's other liability policies will pay first, with CyberEdge PC stepping in where those policies do not cover, subject to its own coverage terms). See *AIG Launches Primary Cyber Coverage for Property and Liability Exposures*, businesswire.com, 19 July 2016, http://www.businesswire.com/news/home/20160719005867/en/AIG-Launches-Primary-Cyber-Coverage-Property-Liability

[49] M. Aguirre, A. Bansal, E. Douglas, et.al. *Can Cyber-Insurance Coverage Keep Apace With Cyber-Exposure?* Towers Watson, September 2015, https://www.towerswatson.com/en/Insights/Newsletters/Global/emphasis/2015/emphasis-2015-3-can-cyber-insurance-coverage-keep-apace-with-cyber-exposure

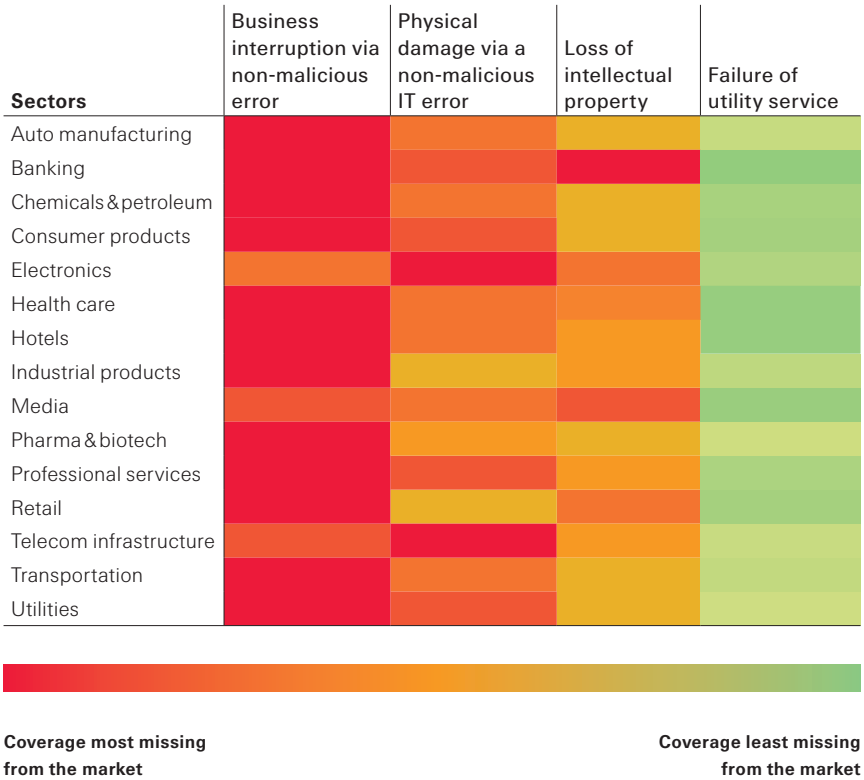
[50] Ibid.

[51] In the past, buyers of cyber insurance have complained that the policies on offer are too limited as they do not cover the damage that an attack can cause to a company's reputation or brand. See "Lloyd's chief urges UK to share cyber attack data", *Financial Times*, 28 November 2016. https://www.ft.com/content/acac3a5e-b255-11e6-a37c-f4a01f1b0fa1

[52] *Intellectual Property and Media Liability Insurance Market Survey - 2016*, The Betterley Report, April 2016.

Figure 7:
Survey of cyber risks for which companies feel insurance cover is not readily available, by sector

Question: which risks of digital interconnectedness would you like to insure your company against where there are currently no insurance solutions available?



Source: *Cyber: in search of resilience in an interconnected world*, Swiss Re/IBM, 2016.

The cost and lack of standard cover may deter some buyers.

The cost of cyber insurance can be another reason not to buy cyber cover. Low cyber insurance penetration and the associated limited amount of loss data means that many insurers adopt a flat pricing structure, whereby firms are charged broadly similar rates regardless of their underlying risk.[53] Furthermore, when asked if pricing of cyber insurance has become more consistent over time, around a third of brokers in a 2016 survey answered that cyber pricing was still very disjointed across insurers, only slightly lower than in the previous years' survey.[54] In part that could reflect insurers' different rating tools and limited historical loss data. The lack of standardised language in cyber policies makes it difficult for companies to purchase their desired insurance cover through multiple insurers, although industry initiatives are underway to introduce common standards.[55]

[53] *UK cyber security: the role of insurance in managing and mitigating the risk*, HM Government/Marsh, March 2015.
[54] *2016 Survey of Cyber Insurance Market Trends*, PartnerRe/Advisen, October 2016.
[55] In analysis of 427 cyber risk insurance policies, including forms and endorsements, riskgenius.com found that there were 78 unique clauses amongst the 140 definitions of Malicious Code. Out of the 67 insurance carriers represented in the data set, 20 of them utilised more than one definition of Malicious Code. See "Evaluating Insurance Policies with Machine Learning", *riskgenius.com*, http://blog.riskgenius.com/insurtechebookform-0

Even within traditional policies, there is considerable uncertainty about the extent of cyber cover provided.

Moreover, ambiguity persists about the scope of existing insurance cover for cyber-related losses. The UK Prudential Regulatory Authority found that insurers' "silent" exposure to cyber risk – implicit within 'all risks' and other liability insurance policies – is material and likely to grow, especially in casualty and specialty lines.[56] With insurance regulators pressing insurers to recognise and address silent cyber exposure, this may encourage further cyber-related exclusions in traditional property and liability insurance.

Despite the rapid growth of cyber risks, the size of the cyber insurance market is still small.

In summary, the cyber insurance market is growing strongly, but premiums and policy limits remain small relative to the value of the tangible and intangible assets that could be impaired by a cyber risk event. According to a Aon/Ponemon study, only around 12% of information assets are covered by insurance, compared with 51% of property, plant and equipment.[57] To broaden and deepen the market, close cooperation between insured and insurers will likely be necessary. On the business side, demand is high and growing for cyber risk transfer, but for insurers improved understanding and better quantification of the potential for significant cyber losses remains a challenge.

[56] "Silent risk" refers to insurers' potential exposure to cyber risks within broader cover they provide that are not explicitly accounted for in cyber insurance policies. See *PRA concerned about 'silent' cyber risk underwriting*, out-law.com, 17 November 2016, http://www.out-law.com/en/articles/2016/november/pra-concerned-about-silent-cyber-risk-underwriting/

[57] *2015 Global Cyber Impact Report*, Aon/Ponemon Institute, April 2015.

The challenge of quantifying cyber risk

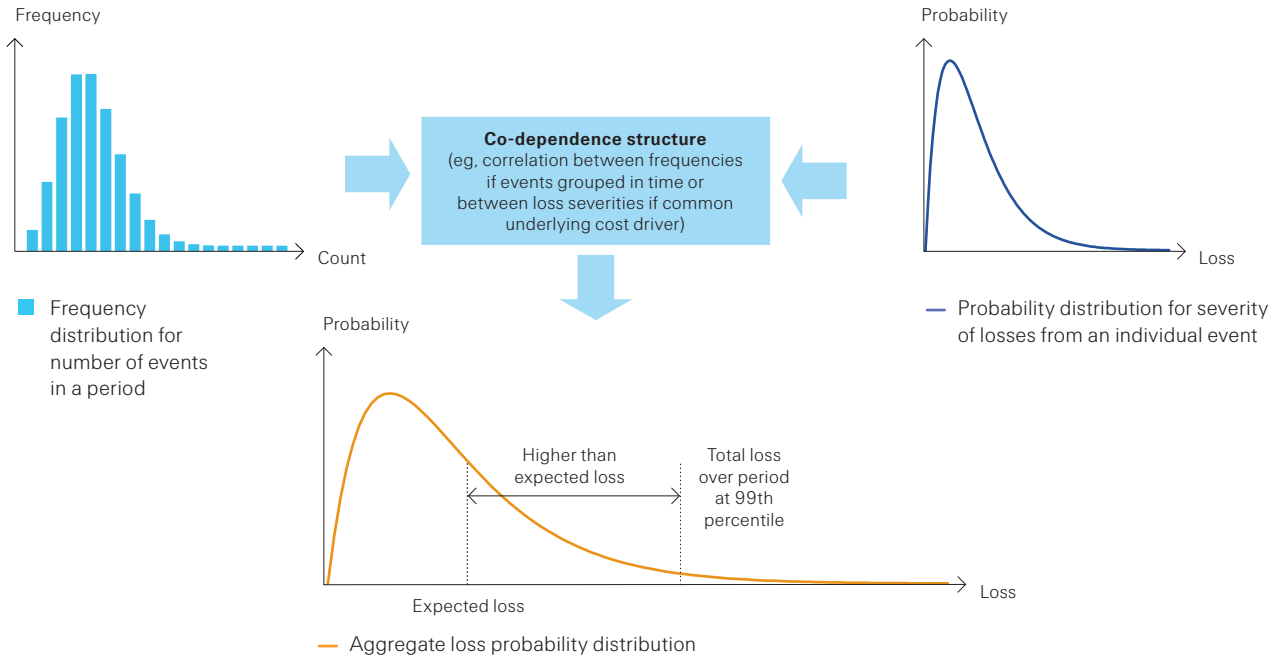
Any risk analysis will consider the likelihood of an event and its potential impact.

At its core, any formal quantification of risk should seek to capture the frequency of a particular event together with the severity of any associated future losses. That is, in the case of an adverse event, how often bad things are likely to happen and how bad they might be when they do. Both frequency and severity should be considered because loss events can occur infrequently but with high severity (eg, catastrophic damage to physical assets), and there are also plenty of high-frequency, low-severity events (eg, minor accidents).

Past evidence on the frequency and severity of losses is typically used to inform about the probability distribution of future losses.

The traditional actuarial approach to measuring risk is to use information on both the number and magnitude of past losses to infer probability distributions for the frequency and severity of future losses over a particular horizon. Combining these two distributions gives an aggregate loss distribution to provide a forward-looking view of the full range of possible losses that might arise in relation to a particular peril and the associated likelihood of that peril occurring (see Figure 8).[58] A firm can assess probabilistically how much damage from the peril it faces and compare that with its willingness and ability to bear the risk that losses might turn out much larger than expected.

Figure 8:
Stylised respresentation of the traditional actuarial approach to risk quantification



Source: Swiss Re Economic Research & Consulting.

[58] Deriving an aggregate (compound) loss distribution from empirical frequency and severity distributions can be generally achieved in two ways. A closed form analytical solution may be used to calculate the compound distribution. Alternatively, Monte Carlo techniques can be used to simulate the many possible different combinations of loss frequencies and magnitudes. See for example, P. Shevchenko, "Calculation of aggregate loss distributions", *The Journal of Operational Risk* 5(2), 2010.

Hurdles facing cyber risk modelling

But modelling cyber risk is challenging.

However, while such an inductive approach to modelling risk is straightforward for many perils, the nature of cyber risks present a new set of challenges. The frequency and severity of cyber events as well as their co-dependence are not easy to establish, making it difficult to assess potential aggregate losses.

There are limited empirical data on cyber-related losses ...

Limited information about actual and prospective losses

There is a lack of historical data on cyber incidents from which to extrapolate information about future losses (both frequency – including unsuccessful attacks – and severity). Companies may not even know when they have been attacked, at least contemporaneously, let alone systematically collect data about the damage caused. This situation is exacerbated by the absence of a commonly-accepted framework to capture information about cyber incidents.[59] Cyber threats are not as easily identifiable as physical threats and cyber crime capabilities can be more easily hidden. Corporates might be reluctant to publicise breaches because of the shame of admitting security failures, the potential reputational impact on future sales, and also a desire not to attract further attacks.

... especially about extreme catastrophe events.

Furthermore, while firms are increasingly starting to track information about their cyber exposure and implement routine cyber hygiene protocols to prevent data privacy/IT security breaches, extreme losses from cyber events have to date been rare. From a statistical perspective, actual history is just one realisation of what might have happened. For routinely occurring events such as data breaches, the actual history of losses is often large enough to encompass most realistic possibilities. But for rare and severe risks, relying on historical information may be misleading because it may encourage perception biases about these sorts of tail events.[60]

Cyber threats are constantly evolving and morphing.

Ambiguity about the underlying risk drivers

Even with detailed information about cyber-related losses and the underlying factors that gave rise to them, past events may not necessarily be a good guide to the future. The risk is constantly evolving with new actors, attack methods and technologies coming into play, making it extremely difficult for firms to understand and monitor their exposure. The potential for "unknown-unknown" cyber threats creates significant ambiguity around the underlying sources of exposure, especially since these may be different for regular data/IT security breaches compared with catastrophic cyber events.

A small shift in the balance between hackers' capabilities and firms' cyber defences can prompt a significant shift in the frequency and severity of attacks.

The human factor adds a huge element of complexity to the modeling of cyber risks, not least the potential for accidental and malicious disruption both from insider and external attacks. Hackers' motivations and their effectiveness will respond to the latest security measures. By the same token, the actions taken by firms to detect and counter threats aim to reduce their vulnerabilities, making information about past attacks less relevant in predicting future ones. Low-level attacks are often not isolated events but continuous. Even a small shift in the balance between the capabilities of hackers and cyber defences could lead to a significant shift in the frequency and severity of cyber attacks.[61]

[59] For example, an attack on Yahoo in 2014 only came to light about two years later when the company was investigating reports of a separate breach. See D. Volz, "Yahoo says hackers stole data from 500 million accounts in 2014", *reuters.com*, 23 September 2016, http://www.reuters.com/article/us-yahoo-cyber-idUSKCN11S16P

[60] See G. Woo, "Counterfactual Disaster Risk Analysis", *variancejournal.org*, 29 February 2016, http://www.variancejournal.org/issues/articlesinpress/Counterfactual-Woo.pdf.

[61] T. Harvey, "Prudential Regulation Authority on the Challenges Facing Cyber Insurers", *rms.com*, 22 November 2016, http://www.rms.com/blog/tag/cyber-risk/

Potential for significant accumulated losses

Cyber risks are often highly interdependent ...

Cyber risks are often highly interdependent: one compromised system may increase the vulnerability of other systems in a single company. For large multi-national companies, cyber security incidents can open up all software, IT systems and infrastructure to attack. Furthermore, there is typically a IT monoculture: many organisations tend to use similar software, security programs and other computer infrastructure. As a result, a successful attack on one company implies others are vulnerable to the same attack.[62] The migration of companies' IT services to the cloud increases the potential for correlated problems across firms should disruptions occur to key "software as a service" products or network providers.

... both within firms and across firms ...

The degree of dependence will vary according to the type of cyber threat (see Figure 9). In particular, the failure of an individual computer due to a hardware problem would probably cause limited damage in the same firm or more generally elsewhere. An insider who abuses his access privileges could affect almost all computers within the internal network, causing significant disruption within a company, but the potential for compromising other firms' systems is limited. In contrast, attacks involving user interaction such as phishing or spyware/malware, can lead to correlated vulnerabilities across firms if a few employees in many different firms are targeted. Typically, other types of malware such as worms, viruses and Trojans lead to correlated damage both within and across firms because they are seldom limited to a single network.[63]

Figure 9:
Examples of different kinds of cyber risk correlation

		Across-firm correlation	
		Low	High
Within-a-firm correlation	Low	*Hardware failure*	*Spyware/phishing*
	High	*Insider attack*	*Worms, viruses and Trojans*

Source: Based on R. Böhme and G. Kataria, *Models and Measures for Correlation in Cyber Insurance - Working paper*, University of Cambridge, June 2006.

... which can lead to significant loss accumulation.

Such interdependence means that losses from individual cyber incidents can often aggregate significantly, especially if the correlating cause takes time to reveal itself. This potential for loss accumulation is particularly problematic for insurers which assume cyber-related risks from their customers, either as part of regular insurance policies or through standalone cyber cover (see Box: *Accumulation risk*).

[62] *Promoting UK Cyber Prosperity: Public-Private Cyber-Catastrophe Reinsurance*, Z/Yen Group and Long Finance, July 2015.

[63] A virus is a type of malware that propagates by inserting a copy of itself into another program and spreads from one computer to another, leaving infections as it travels. In contrast, worms are standalone software and do not require a host program or human help to propagate. Trojans do not reproduce by infecting other files, and nor do they self-replicate, unlike viruses and worms, but are spread through user interaction such as opening an e-mail attachment or downloading and running a file from the internet. For more information see http://www.cisco.com/c/en/us/about/security-center/virus-differences.html

Accumulation risk

Insurers who take on cyber risks from their clients hope to be able to diversify their exposure.

Insurers by definition accept risks from insureds in return for premiums. They do so in the hope that by pooling together a sufficiently large number of independent risks, the chances of simultaneously paying out to many policyholders is limited and that aggregate losses for the portfolio become predictable. Such diversification is one of the principles on which the business model of every re/insurance company is founded.

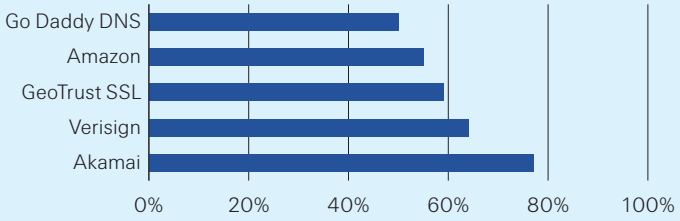
But they could face significant accumulated losses from the same underlying incident …

The nature of cyber risk means that one cyber event might trigger multiple claims under different policies (for example reputational risk, property damage, professional indemnity, and Directors and Officers). The same event could also prompt multiple claims from multiple clients under different policies spread across different geographies, The interconnectivity of IT systems means that cyber incidents could trigger several insurance products and independent policies in a chain mechanism, similar to CBI cover.[64]

… or from resulting correlated exposures to different events.

In addition, the overall loss burden from cyber risk may stem from a number of unrelated loss events affecting numerous insureds during any given policy period or a combination of scenarios.[65] Insurers' clients may also tend to depend on the same group of IT service providers (see Figure 10), which could lead to concentrated losses if there is an outage or breach at key network infrastructures.

Figure 10:
Use of selected internet service providers by policyholders within a sample insurance portfolio



Source: *Risk Degrees of Separation: The Impact of Fourth Party Networks on Organizations*, BitSight, 2016.

The correlating cause of claims may also be hard to identify making processing claims difficult.

Moreover, in the case of a cyber attack it can be difficult to identify all the claims that have been caused by the same piece of malware, or result from the same underlying attack method or perpetrator. It may take time to identify the correlating cause, which may also be never fully understood. In such circumstances, insurers may find it difficult to differentiate which of the many claims they face are attributable to the same fundamental cause, or to other background or baseline incidents.[66]

The potential for accumulated losses acts as a key deterrent for re/insurers writing cyber protection.

To date, there has not been a truly systemic cyber catastrophe event that has triggered large numbers of claims. Nevertheless, according to a recent survey, almost two thirds of respondent insurers believe aggregation issues related to cyber exposures are significant.[67] The potential for substantial accumulated losses is a key constraint on insurers' appetite for taking on cyber risks, and is a particular concern for reinsurers which stand ready to absorb extreme losses from multiple cedants. Without effective accumulation risk controls, a re/insurer could find itself burdened with catastrophic losses that exhaust its capital, impairing its ability to make good on promises to policyholders.[68]

[64] *Cyber resilience: The cyber risk challenge and the role of insurance*, CRO Forum, December 2014.
[65] *Questionnaire on cyber risk insurance to the private sector*, OECD, 2016, http://www.gfiainsurance.org/en/upload/positionpapers/GFIA-16-11%20Response%20to%20OECD%20Cyber%20Insurance%20Questionaire.pdf
[66] *Managing Cyber Insurance Accumulation Risk*, Risk Management Solutions, Inc and Centre for Risk Studies, University of Cambridge, February 2016.
[67] *Cyber Risk Survey Report*, Weightmans LLP&Insurance Day, November 2015.
[68] For further insights on cyber accumulation risks see the discussion in *Casualty Accumulation Risk*, CRO Forum, October 2015.

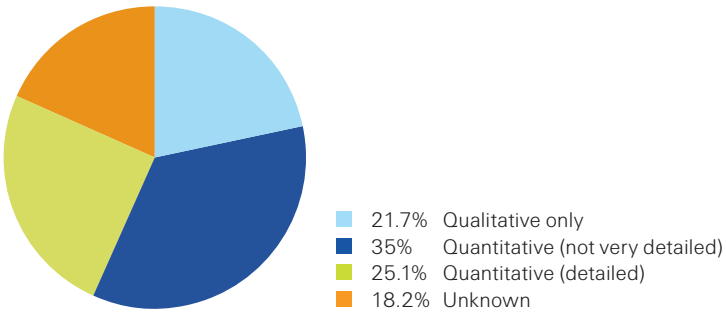
Deterministic scenario analyses

Most corporations do not use detailed quantitative cyber risk models.

Because of the complexities involved in quantifying the full range of cyber risks, companies and insurers have tended to take a relatively rudimentary approach to modelling. A recent US survey of security professionals indicated that only around a quarter of companies employ detailed quantitative cyber risk models, with the majority relying on simple metrics or qualitative approaches (see Figure 11). Likewise, recent polls found that only around a third of UK firms estimate the potential financial impact of cyber attacks, and 60% of companies in continental Europe have never estimated the financial impact of a cyber-loss scenario.[69]

Figure 11:
Survey of cyber risk management approaches used by corporates

Question: does your company develop a quantitative model for assessing and managing cyber risk?



Source: *Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey*, SANS Institute, 2016.

[69] *UK Cyber Risk Survey Report: 2016*, Marsh, September 2016 and *Continental European Cyber Risk Survey: 2016 Report*, Marsh, October 2016.

To the extent that the risk is quantified, it is usually through deterministic scenario analyses.

Most quantitative approaches currently tend to focus on companies' potential exposure under a limited number of specific, yet hypothetical, scenarios. Models typically take a deterministic view to derive point estimates of the size of possible losses if the scenario were to happen. In other words, they seek to provide "what-if" type guesstimates of the impact should downside risks crystallise. By careful selection, construction and analyses of different scenarios, a broad picture of the firm's risk position can be created.[70]

These often aim to provide estimates of probable maximum losses from a cyber-related incident.

A key aspect of such scenario analysis is to incorporate the potential for large-scale individual or aggregate losses. A number of insurance brokers and vendors of risk-management analytics have developed scenario tools to help their clients and insurers assess and manage their probable maximum losses (PML) from cyber-related perils.[71] For instance, the risk modeling firms AIR Worldwide and RMS have developed cyber exposure databases for a large number of companies that can be used to build a detailed picture of possible losses under various deterministic scenarios.[72] Similarly, as part of its regular Realistic Disaster Scenario (RDS) framework, in 2015 Lloyd's of London asked its syndicates to design and stress their exposures against three extreme cyber attack scenarios, and estimate their potential aggregate exposure to each of them.[73]

A drawback of deterministic approaches is calibrating how plausible are the assumed loss scenarios.

However, a major drawback with pure deterministic scenario analysis is the difficulty of establishing the plausibility of losses under adverse scenarios. It is always possible to design a scenario that generates extreme catastrophic losses, but without a mechanism for calibrating the likelihood of those events, let alone how that compares with the probability of alternative outcomes, it is difficult to know how much weight to place on the resulting estimated losses.

Towards probabilistic models of cyber risk

Some researchers are building probabilistic models to quantify cyber risks.

Responding to this weakness, a number of researchers are developing probabilistic models to assess potential cyber losses, although their development is at an early stage. Compared with deterministic tools, these models look to quantify the full probability distribution of future losses instead of a single best estimate. In this sense they are closer to traditional actuarial approaches to modelling risk. Sometimes referred to as cyber value-at-risk (VaR), proponents suggest these models provide a foundation for quantifying risk and instil discipline and rigour into the risk assessment process.[74]

[70] T. Hull, "A Deterministic Scenario Approach to Risk Management", *2010 Enterprise Risk Management Symposium*, Society of Actuaries, 12-15 April 2010.

[71] For example, in May 2016 Guy Carpenter announced a strategic alliance with Symantec Corporation to create a cyber aggregation model (see http://www.gccapitalideas.com/2016/05/17/guy-carpenter-forms-strategic-alliance-to-develop-cyber-aggregation-model/). At the beginning of 2016, catastrophe modelling firm RMS launched Cyber Accumulation Management System, a tool for insurers to identify their accumulations and correlated risk, and stress test their portfolios against a range of cyber losses (see http://www.rms.com/cyber). Similarly in April 2016, AIR Worldwide released the industry's first open-source deterministic cyber risk scenarios in a bid to begin to increase insurers' understanding of their aggregated risk from large-scale cyber attacks that could lead to catastrophic accumulated losses.

[72] S. Stransky, E. Ritt, *Cyber Scenario Modelling and Decision Making*, Air Worldwide, 2016.

[73] *Cyber-attack: managing catastrophe-risk and exposures*, Lloyds of London, 9 November 2015, https://www.lloyds.com/~/media/files/the%20market/communications/market%20bulletins/2015/11/y4938.pdf

[74] See N. Sanna, "What is a Cyber Value-at-Risk Model?", *fairinstitute.org*, 28 January 2016, http://www.fairinstitute.org/blog/what-is-a-cyber-value-at-risk-model

These typically combine experts' views with assumptions about the frequency-severity distribution of future losses.

The rarity of extreme catastrophe cyber losses and the sparseness of historical loss data even for some relatively minor events, means that modellers have to rely on auxiliary information to generate estimates of aggregate loss distributions. One approach is to combine experts' views of various cyber threats with assumptions about the underlying statistical properties of the frequency-severity distribution of cyber losses under different scenarios. The latter can be chosen to allow explicitly for potentially severe downside risks from a cyber incident.[75]

Figure 12:
Stylised representation of probabilistic cyber risk modelling approaches

Source: Swiss Re Economic Research & Consulting, based on insights from http://www.fairinstitute.org/

Combined with methods to account for correlated exposures these might eventually be used to quantify potential loss accumulations.

Together with assumptions about the potential co-dependence of firms' exposure to the same threats, this approach can be used to gain a risk-based perspective on accumulated losses, which is crucial for insurers assuming risks from multiple policyholders (see Figure 12).[76] Whatever dependency structure is assumed, however, (whether for example, copula-based, using correlation matrices or a common risk driver approach), it should be capable of being stressed to reflect the potential for the future to be more unusual than the past.[77]

[75] Some researchers advocate using scenario analysis to inform expert guesstimates of the maximum, minimum and most likely amount of damage that might accompany a cyber incident. These statistics are then used in combination with Monte Carlo simulation and an assumed underlying distribution such as a beta-PERT to generate probabilities against a range of cyber-related losses.

[76] For re/insurers, overcoming the challenges in modelling accumulation are arguably much more crucial than getting a handle on marginal frequency and severity probability distributions.

[77] *A Clearer View of Emerging Risks*, Guy Carpenter, September 2015.

A challenge is to benchmark the risk calibrations without comprehensive loss experience information.

Studies based on selected information about known data and privacy breaches tend to indicate that the distribution of costs is highly skewed. Most incidents tend to result in small amounts of damage, but a few can lead to large-scale losses (see Table 2 on page 3).[78] Yet, without comprehensive details of the full suite of cyber-related events and associated losses (including property damage, reputational harm, business interruption and personal injury or loss of life), it is virtually impossible to benchmark/back-test risk calibrations. In other words, implied overall loss distributions can only be illustrative given that they are based on simplifying assumptions which are not grounded in actual loss experience. This limitation is clear once the potential for unknown-unknown loss events or risk factors is acknowledged.

In response, some modellers stress the importance of detailed probabilistic assessments of all risk factors and their interaction.

To partially address this issue, some modellers suggest a highly granular approach to scenario building. This involves examining the same scenario multiple times and from different angles, to derive a comprehensive assessment of the underlying causal factors and their permutations that affect the frequency-severity of cyber losses. This probabilistic perspective is applied to every risk factor that is analysed – the assets that could be impaired, the likely threat actors, the types and magnitudes of the threat, the particular vulnerabilities and mitigation mechanisms in place etc.[79]

Others also advocate counterfactual analysis to inform about possible extreme outcomes.

As a guard against potential cognitive biases – for example, the tendency to underestimate risks if large losses have yet to materialise – some researchers suggest that counterfactual analysis can be useful. By examining past events and exploring what might have happened for different constellations of risk factors, it is possible to build a fuller picture of the range of possible extreme losses that might have arisen, could still happen, and should be mitigated in the future. Datasets might be further augmented by scenarios inspired and constructed from detailed stochastic modeling of past historical events. Such retrospective probabilistic assessments can provide useful insights into previously unanticipated future catastrophes, and so reduce catastrophe surprises.[80]

The limits of models

Models are an aid to understanding, but will almost inevitably be wrong.

Ultimately all models are necessarily an abstraction from reality. They are simply tools to aid understanding. Even in the sphere of natural catastrophes (nat cat) where significant modelling advances have been achieved, the last few years have demonstrated that the real world is often quite different from the model view.[81] Also, threats and vulnerabilities can often be considered as independent of one another in the physical world, but with cyber risk there is potential for a much more correlated, non-linear impacts. The discovery of a vulnerability in an IT system often triggers an avalanche of attacks which specifically target exactly that element.[82]

[78] See for example, M. Kuypers, T. Maillart, E. Paté-Cornell, *An Empirical Analysis of Cyber Security Incidents at a Large Organization*, Freeman Spogli Institute for International Studies, Stanford University, 2016.

[79] For example, the Factor Analysis of Information Risk (FAIR) approach sets out a framework for decomposing the set of complex factors that contribute to information and operational risk, and how they affect each other. In doing so it seeks to set out a standard taxonomy and ontology for risk. For further discussion, see http://www.fairinstitute.org/

[80] G. Woo, op cit.

[81] "The new approach to cat modelling", *Specialty underwriters at a crossroads*, Reactions, in association with Russell, Autumn 2013.

[82] I. Robertson and A. Warr, "Why we need a new approach to cyber-security and risk assessment", *www2.warwick.ac.uk*, 27 April 2016, http://www2.warwick.ac.uk/research/priorities/cyber/blogs/?newsItem=094d434554536416015458 0bc4622c40

The recent financial crisis showed the weakness of VaR models in underestimating the probability of rare events.

The 2008-09 financial crisis revealed very clearly the weaknesses of probabilistic models such as VaR. In pursuit of mathematical tractability, simplifying assumptions were employed which significantly underestimated the potential for large losses on financial investments (ie, fat tails in the overall loss distribution). Extreme loss events can happen more often than people think. Moreover, traditional risk measurement approaches like VaR tend to focus on the issue solely from the solvency perspective (size of loss relative to a firm's own capital resources), when other factors such as a firm's liquidity position (its ability to meet liabilities as they fall due) could be as important in containing any resulting damage.

Some critics argue that formal risk models should be replaced with heuristics that simply look to improve firms' resilience.

For some analysts, such shortcomings mean that developing models to quantify what is ultimately unmeasurable is likely to be futile: trying to pinpoint numbers from the tails of loss distributions that are highly uncertain and volatile is unhelpful and potentially dangerous. For them it is better to build robust IT systems that enable companies to withstand difficult-to-predict, catastrophic events. Rather than rely on spuriously precise models, it is as much about defining, tracking and evaluating factors that affect the propensity for a catastrophic cyber event or that might lead to serial aggregation of losses. Firms should also build architectures that are "anti-fragile", where shocks and disruptions make firms stronger, more resilient and better able to adapt to new cyber threats.[83]

Yet models, by blending formal statistical analysis and expert judgment ...

Such a critique of formal risk modelling is arguably too fatalistic. Models cannot and should not be the final or absolute arbiters in firms' risk management decisions.[84] Cyber losses may also be prone to irreducible uncertainty that cannot be remedied by collecting more data, by using more sophisticated statistical methods or more powerful computers, or by thinking harder and smarter.[85]

... will help improve cyber risk assessment.

Nevertheless, by blending partial data and statistical modelling know-how with experienced-based judgement, firms and insurers can over time increase their understanding of cyber risk. This process will likely be accelerated and enhanced if lessons from the Oasis open-source framework to collaborate and share insights about nat cat models can be applied in the cyber field.[86] Work by the CRO Forum to develop a common cyber risk categorisation goes in this direction.[87] Allied with loss information sharing platforms such as ORX and ORIC International, such initiatives should enable companies and insurers to build up a clearer picture of the scale and source of cyber risks.[88]

[83] See for example, N. Taleb, *Anti-fragile: Things That Gain from Disorder*, Random House, November 2012.
[84] D. Rowe, *Value at Risk: A Valuable Tool That Was Greatly Oversold, Notes from the Vault*, Federal Reserve Bank of Atlanta, June 2013.
[85] For more discussion about the limits of formal modelling see A. Lo and M. Mueller, *WARNING: Physics Envy May Be Hazardous To Your Wealth!* , MIT, 12 March 2010, http://web.mit.edu/alo/www/Papers/physics8.pdf
[86] Oasis, a not-for-profit company, is owned by over 40 of the world's leading insurers, reinsurers and brokers and forms, together with an Associate Member community of over 100 companies and academic institutions, a broad community of organisations dedicated to improving catastrophe loss modelling.
[87] *Concept Proposal categorisation methodology for cyber risk*, CFO Forum, June 2016, http://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web.pdf
[88] ORX Association and ORIC International are operational risk loss data exchanges helping advance the measurement and management of operational risk through sharing operational risk intelligence. See https://www.orx.org/Pages/HomePage.aspx and https://www.oricinternational.com/

Lessons from other perils

The experience of nat cat modelling offers hope that richer cyber models will eventually develop.

Risk modelling tends to evolve as data and knowledge about the underlying perils and hazards deepen. This is certainly the case with nat cat risk models. Since the introduction of the first commercially available nat cat models in the late 1980s, updates have occurred regularly and convergence among various vendors' models suggests uncertainties have been progressively reduced.[89] These improvements have typically reflected advances in computing techniques and capabilities, improved scientific understanding of natural perils and their impact, and expanded coverage of the phenomena captured by the models.[90] This offers hope that richer cyber models will emerge as understanding of the fundamental risk drivers develops and more data about the underlying stochastic processes that generate cyber losses becomes available.

Modelling cyber liability and property-type risks may require fundamentally different approaches.

At the same time, a cookie-cutter approach where the same generic set-up is applied to different risks is unlikely to be optimal. Liability and property-type cyber risks may require fundamentally different approaches, depending on the extent of knowledge, claims experience and sources of loss accumulation. In particular, deterministic scenario analyses for multiple, fixed events may be entirely appropriate to gain a credible and meaningful assessment of worst-case scenarios while the associated probabilities of occurrence remain so difficult to define.[91]

Various modelling approaches are being explored which might ultimately be extended for cyber risk measurement.

In this vein, some re/insurers are developing highly-granular, multiple scenario models for liability risks to quantify ranges of expected losses and their sensitivity to changing technological, economic, legal and societal conditions.[92] Meanwhile, others are looking at applying insights from network analysis or models of infectious disease pandemics to understand potential casualty risk accumulations.[93] Over time such models may be extended to include cyber risks, which increasingly combine features of both property and liability risk exposures, including (contingent) business interruption. Agent-based models are also emerging which seek to incorporate the adaptive preferences and behaviours of attackers and defenders in analysing cyber threats and vulnerabilities, much like some models of terrorism risk.

[89] *Managing Catastrophe Model Uncertainty: issues and challenges*, Guy Carpenter, December 2011.
[90] Ibid.
[91] For further discussion of the relative strengths of deterministic scenario models, see K. Clark, "Measuring up the metrics", *globalreinsurance.com*, September 2010, http://www.karenclarkandco.com/news/pdf/20-21_GRSept10.pdf.
[92] *Bringing a forward-looking perspective into liability modelling: Liability Risk Drivers*, Swiss Re, April 2016.
[93] Reactions, in association with Russell, op. cit.

Initiatives to boost cyber resilience

Self-protection and risk prevention

Cyber risks cannot be eliminated entirely. Firms need to play their part to make the economy more resilient.

Even with better quantification, it will be impossible to eliminate cyber risks completely, especially given that the threats will continually evolve with ever greater dependence of business and society on digital technologies. To make economies more resilient, companies need to improve their cyber risk management. Their first line of defence against cyber threats is greater investment in security technology and increased employee awareness of the latest hacking techniques and other cyber risks. Many recent data breaches have their genesis in elementary system flaws such as weak hash password functions or lack of encryption. Likewise, Verizon's Data Breach Investigations Reports consistently reveal that most cyber breaches capitalise on preventable lapses in basic cyber hygiene, including failures to patch known software defects or to implement appropriate password or other authentication regimes, susceptibility to phishing attacks, and insufficient least-access regimes.[94]

Companies are investing heavily in preventive and detection-response capabilities.

There are signs that firms are gearing up to address these vulnerabilities. Global spending on information security products and services reportedly reached USD 81.6 billion in 2016, an increase of 7.9% over 2015, according to recent estimates.[95] The upward trend is expected to continue with increased investment in enhanced detection-and-response approaches alongside more traditional preventive security.

But cyber risk protection is not just about building stronger firewalls or hiring specialist IT staff; it is a broader strategic issue.

However, standalone and/or bolt-on security measures that focus on one aspect of firms' operations such as IT firewalls or antivirus products will not be enough. According to one report, 46% of compromised IT systems in 2013 had no malware on them.[96] By the same token, simply considering cyber threats through the lens of regulatory compliance will not adequately capture the full range of risks, although it may help to catalyse action to recognise and address obvious system weaknesses. Put simply, cyber risk is not just an IT or regulatory issue. It is a strategic business risk. Cyber attackers are continuously discovering new ways to exploit vulnerabilities and companies can no longer assume that it is merely sufficient to hire competent IT professionals and have the latest security protocols in place.[97] The threat from disgruntled existing or former employees demonstrates the importance of an organisation's culture in mitigating cyber risks.[98]

It is as much about integrating cyber resilience into firms' overall risk management procedures.

Risk mitigation is most effective when embedded within a holistic and routine assessment of the evolving cyber landscape and associated risks. Firms should look to leverage their internal IT department's expertise to scope out their vulnerabilities and identify the sorts of cyber events that could cause significant damage. This might include regular stress-test exercises that consider firms' robustness against various events that could be highly disruptive. New technology, even though it can add to risks, can also play a role in helping firms identify emerging threats. Cognitive computing, for instance, may ultimately help anticipate changing cyber risks, flagging up abnormal deviations when a system is compromised and taking action to counter new threats as they arise.[99]

[94] According to a recent survey, while 55%% of respondents state their organisation has changed or evolved processes for managing privileged accounts, 40% still store privileged and admin passwords in a Word document or spreadsheet. See *Global Advanced Threat Landscape Survey 2016*, CyberArk, 2016.

[95] *Gartner Says Worldwide Information Security Spending Will Grow 7.9 Percent to Reach $81.6 Billion in 2016*, Gartner, 9 August 2016, http://www.gartner.com/newsroom/id/3404817

[96] *M-Trends Report*, Mandiant, 2014.

[97] *How to make the case for buying cyber risk insurance to the board*, Aon 2014.

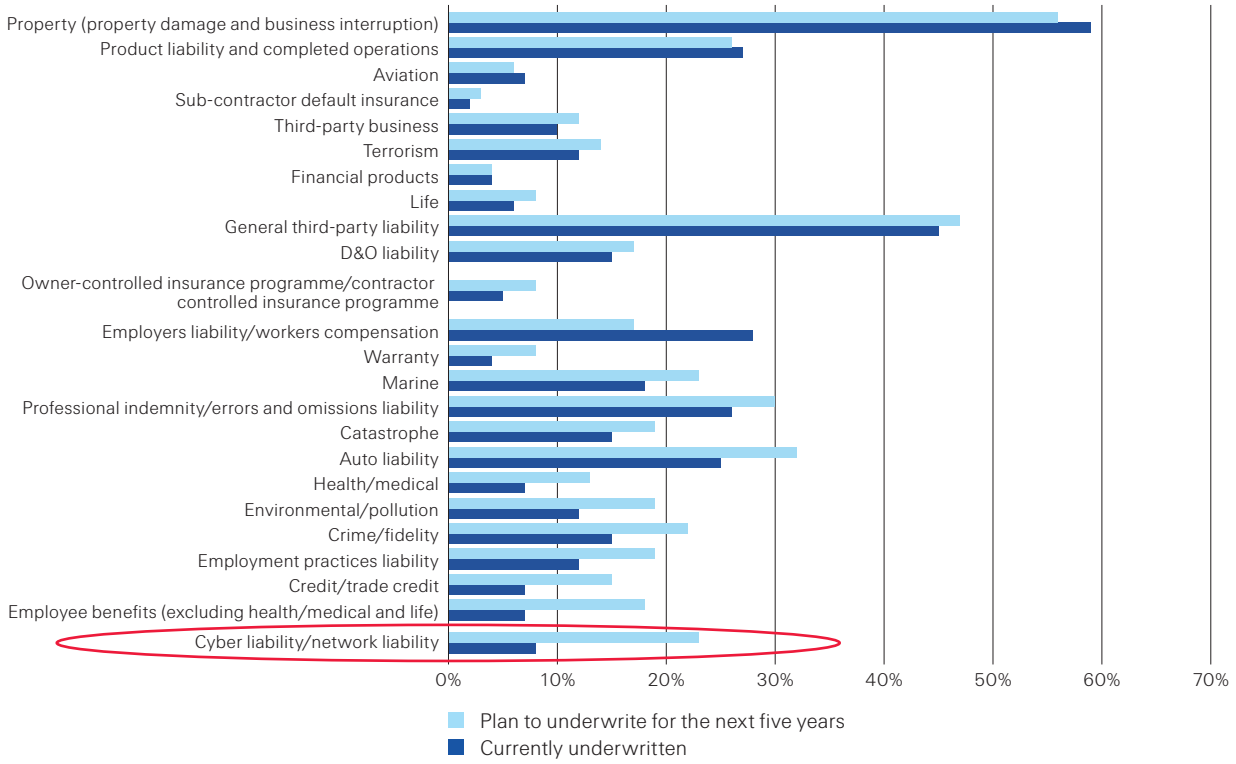
[98] A recent global analysis of staff engagement surveys indicated that employees at organisations experiencing data breaches report less favourable training and performance-related remuneration, at least compared with employees at leading companies in their industries. See *The inside threat: Why employee behavior and opinions impact cyber risk*, Willis Towers Watson, May 2016.

[99] E. Hunter, "Cognitive Computing Takes On Cyber-Security", *theinnovationenterprise.com*, 20 January 2016, https://channels.theinnovationenterprise.com/articles/cognitive-computing-takes-on-cyber-security

Some firms are exploring the use of captives to manage their cyber exposures.

As part of enhanced risk management practices, some companies are considering setting up captive insurers to organise their cyber exposures.[100] Traditionally captives have been used to underwrite property damage, workers' compensation, medical malpractice and third-party liability risks. A 2015 survey found that 8% of firms underwrote cyber risk through a captive, and that 23% planned to do so within five years.[101] This represented the sharpest increase in the potential use of captives across the various risks surveyed (see Figure 13).

Figure 13:
Risks underwritten by a captive, currently and in five years



Source: Aon.

Using a captive can promote an increased appreciation of the cyber risks facing a firm.

Funds are accumulated in the captive as a means to self-insure against risks. Consolidating exposures within a separate corporate structure may promote a greater understanding, for example, of cyber risks, including regular reviews of data protection and network security practices and collection of crucial information and intelligence. This may be especially valuable for large, international corporations which run significant and sometimes disparate businesses in different locations. Business information gleaned through operating a captive insurer might also allow a company to obtain more favourable pricing on cyber re/insurance.

[100] A captive is a special type of insurance company set up by a firm, trade association or group of companies to insure the risks of its owner or owners.
[101] *Global Risk Management Survey*, Aon, 2015

Innovation in cyber re/insurance

Richer data about cyber incidents and their impact will support further development of cyber insurance.

Cyber insurance can also play a bigger role in boosting resilience. An important factor influencing the pace of market development will be the capture and analysis of relevant data and information needed to underwrite cyber risks accurately. Knowledge of the range of cyber risks, their impacts, and the reliability of the data are crucial to actuarial efforts to estimate risk occurrences and their severity. Insurance companies usually know less than the insureds about the risks as well as the actions taken to mitigate the associated losses. They typically do not hear about near misses, nor do they have early warning signs of an attack. Even when information is shared by a policyholder it may be incomplete, ambiguous, or erroneous. This asymmetry of information has important implications for insurers' potential exposures and their willingness to provide cover.

Corporates appear willing to share information.

At face value many firms appear willing to share information about their cyber breaches with external parties, including insurers, if it leads to better insurance solutions. This is true globally and across most sectors (see Figure 14). There may be some residual reluctance to reveal forensic information about cyber attacks, especially if there are outstanding legal and regulatory issues related to an event, but firms do not have to adopt an all-or-nothing approach. They can choose how much and how often they share data regarding their efforts to combat malware, although it is important to recognise the partial nature of shared information when drawing inferences. For example, some organisations might elect to distribute data via a third-party solution provider, which in turn aggregates the data and shares it on an anonymous basis.[102]

Figure 14:
Survey of firms' willingness to share information

Industry	*Question*: do you believe that acceptance of data sharing will increase overall? (% yes)	*Question*: would you be prepared to collaborate more strongly (eg, information sharing with the industry and insurers)? (% yes)
Electronics	57%	51%
Media	58%	42%
Health care	64%	42%
Transportation	64%	49%
Banking	64%	53%
Telecom infrastructure	67%	56%
Pharma & biotech	68%	53%
Chemicals & petrol	68%	59%
All sectors	68%	54%
Consumer products	68%	60%
Industrial products	71%	63%
Auto manufacturing	72%	56%
Professional services	73%	53%
Retail	75%	52%
Utilities	78%	51%
Hotels	78%	67%

Source: *Cyber: in search of resilience in an interconnected world*, Swiss Re/IBM, 2016.

[102] *5 Key Ways To Detect Anomalous Behavior On Your network. Threat Intelligence for Your Data Security and Management Framework*, Information Security Media Group, 2016.

Methods to capture standardised data on cyber risk exposure are being developed.

A number of external vendors such as AIR and RMS have built data schema that provide firms with a standardised approach to identify, quantify and report cyber exposures to insurers.[103] Similarly, the CRO Forum is promoting a common language and framework to capture salient information about cyber incidents and vulnerabilities.[104] Such information sources will benefit insurers' by providing ways to monitor and evaluate their clients' evolving cyber exposure in a systematic and uniform manner, and thereby also assess their own accumulation risk.

Greater understanding of cyber risks will enable flexible and tailored insurance solutions.

For their part, insurers are looking to develop flexible insurance products that are less complex, better meet the needs of companies and adapt to the changing cyber threats they face. This includes tailoring cover for small and medium-sized businesses that hitherto have been underserved by insurance and are often less well placed to cope with cyber risks than larger firms. Insurance can also be configured for quick payment, for example, through the up-front settlement of BI claims. This can be particularly important given the strains on liquidity that might arise following a cyber incident. Ancillary services provided by insurers can also help post-incident recovery.

Partnering with cyber security experts …

Some re/insurers are seeking partnerships with cyber security firms and data analytics vendors to fill gaps in their knowledge and scale up/provide additional services to their clients. For example, in May 2015 ACE Group announced a tie-up with FireEye to combine real-time cyber threat detection with loss mitigation advice and services.[105] Similarly, as a complement to its cyber risk mitigation and insurance products, AIG acquired a minority stake in K2 Intelligence, an investigative consulting firm.[106] Also, Swiss Re has added to its underwriting toolbox a cyber risk assessment platform provided by Cyence, a cyber risk modelling and analytics firm. These specialist cyber risk assessment companies typically use sophisticated intelligence to capture and analyse information present in the public and the non-public part of the internet.

[103] See for example *RMS Launches New Data Standard for Managing Cyber Insurance*, RMS, 19 January 2016 https://www.rms.com/newsroom/press-releases/press-detail/2016-01-19/rms-launches-new-data-standard-for-managing-cyber-insurance and Verisk Cyber Exposure Data Standard and Preparer's Guide, air-worldwide.com, 2016, https://www.air-worldwide.com/Documentation/Cyber-Exposure-Data-Standard/air_cyber_exposure_data_schema_and_preparers__guide.htm

[104] CRO Forum, June 2016, op. cit.

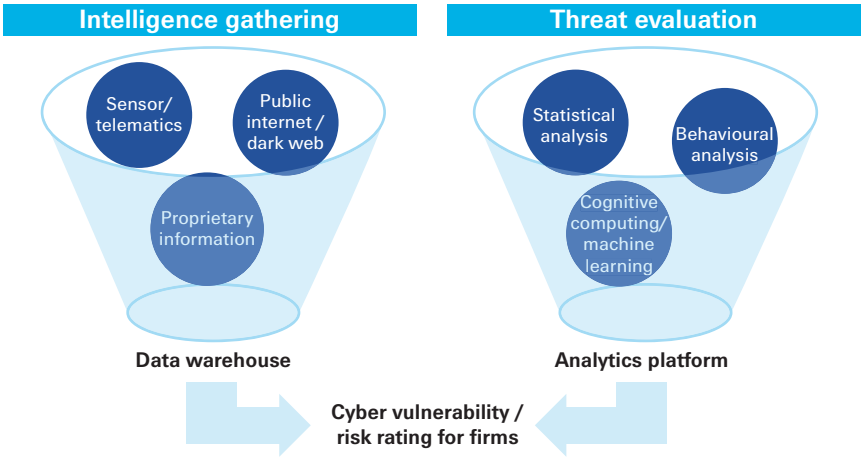
[105] *FireEye and ACE Group Announce Strategic Alliance to Mitigate Cyber Risk*, FireEye, 18 May 2015, http://investors.fireeye.com/releasedetail.cfm?ReleaseID=913633

[106] "AIG Invests in K2 Intelligence to Deepen Cyber, Other Risk Mitigation Capabilities", *businesswire.com*, 15 April 2015, http://www.businesswire.com/news/home/20150415006706/en/AIG-Invests-K2-Intelligence-Deepen-Cyber-Risk

… and leveraging smart analytics …

More generally, Big Data and smart analytics may augment traditional actuarial analysis to enable re/insurers to create a multi-dimensional risk profile of selected companies and/or industry segments, and respond quickly to fast-changing underlying risk factors. For example, are an insured's employees accessing the internet using an outdated web browser that is vulnerable to new spyware, malware and viruses? Or does a company's intellectual property, proprietary data or security information, including stolen passwords, appear in dark web forums? Combining such intelligence with statistical and behavioural analytics – particularly those that understand not only network connections but the business relevance and context of those interactions – may help isolate those movements and patterns that indicate susceptibility to malicious activity (see Figure 15).[107]

Figure 15:
Smart analytics as a complementary underwriting tool



Source: Swiss Re Economic Research & Consulting.

… will also help insurers evaluate cyber risks.

Such analysis will not replace underwriting expertise and risk-based judgement.[108] However, alongside information from detailed cyber vulnerability analysis and penetration testing, it can form a complementary risk assessment tool.[109] Over time product and process innovation can help make cyber risk more insurable. Combined with greater legal certainty about policy wordings and the limits of liability, this will help lower premiums, adjust limits (sums insured, retention, reinstatements etc) to better match customers' needs, and make cyber cover more affordable to a wider set of insureds. Greater differentiation in risk assessment, if reflected in insurance premiums, will also incentivise good risk management behaviour.

[107] *Analytics steps up to meet evolving cybersecurity threats*, SAS, http://www.sas.com/en_us/insights/articles/risk-fraud/analytics-steps-up-to-meet-evolving-cybersecurity-threats.html

[108] According to a recent survey of US insurance brokers, the majority (60%) of respondents believe that partnerships between insurance carriers and cyber security firms will be most beneficial for post-event response and consulting rather than pre-event risk quantification. See *Cyber Insurance Market Watch Survey*, The Council of Insurance Agents and Brokers (CIAB), October 2016.

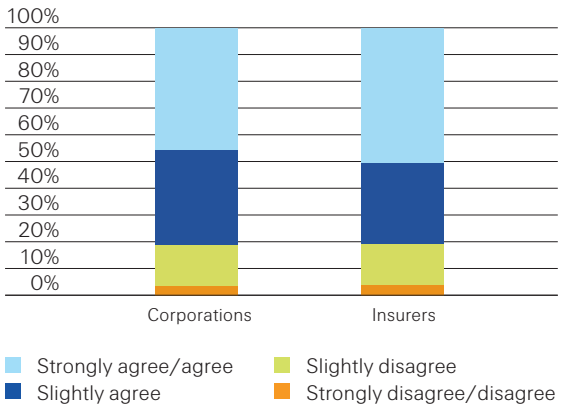
[109] Although sometimes the terms are used interchangeably, vulnerability analysis usually refers to identifying and measuring security vulnerabilities, while penetration testing seeks to replicate the actions of a cyber attacker intent on breaching information security protocols and/or disrupting the normal functioning of the organisation.

Both firms and insurers foresee potential for digital technology to facilitate flexible insurance solutions.

Both insurers and corporates appear to agree about the scope for new digital technology to promote flexible insurance solutions. In the recent Swiss Re/IBM survey, close to half of insurers (51%) and corporates (46%) were open to the idea that digital technologies will allow flexible insurance solutions (see Figure 16). These might include usage-based cyber insurance products where, for example, coverage levels track changing technologies, new forms of cyber attack, and new approaches to cyber defence. More speculatively, parametric solutions whereby insurance is linked to an independently-derived quantitative assessment of the current cyber threat level might also eventually be possible if standard industry threat indices can be developed.

Figure 16:
Survey of companies'/insurers' views about the potential to buy/offer flexible, tech-led insurance solutions

Question: If flexible insurance solutions based on digital interconnection technologies are offered, it is highly likely that my company will buy /offer them



Source: *Cyber: in search of resilience in an interconnected world*, Swiss Re/IBM, 2016.

However, the potential for large single or accumulated losses means there are limits to the cyber cover that re/insurers can provide.

Even with richer data, advances in risk quantification and greater collaboration with policyholders, however, cyber insurers must be careful not to overstep the boundaries of insurability. Cyber exposures pose significant tail and aggregation risks. Thus far losses from potential catastrophic cyber events have been manageable – for example, the Stuxnet attack on an Iranian power station in 2012, and an attack on a Ukrainian power plant in 2015, both resulted in physical damage to infrastructure without triggering widespread disruption. But insurers must be alert to the potential for unexpectedly large losses both through dedicated cyber policies and silent cover. Businesses themselves should also be concerned about risk aggregation given that single attacks can lead to losses across a large number of firms, which can create counter-party risk (including in relation to their insurer).

Sharing risks among insurers within a dedicated cyber pool may be one way to increase risk-absorbing capacity

In a bid to increase the insurability of catastrophe cyber losses, some commentators have suggested the creation of a dedicated pool mechanism through which individual insurers could share risks.[110] This would allow smaller insurance companies looking to expand their business to participate without the customary start-up costs, while limiting their liabilities to match their own appetite for risk. In addition to promoting stability of capital in the market, a pool might facilitate rapid sharing of information when cyber events occur. This can result in a quicker reaction and response, and hopefully limit the spread of a problem.

Risk transfer to capital markets

The transfer of peak cyber risks to capital markets is another.

Another way to increase overall loss-absorbing capacity for cyber risk is by developing investment vehicles that enable capital market investors to take some of the exposures. Natural catastrophe bonds (cat bonds) were developed in the 1990s to cover peak property risks, partly in response to growing perceptions that catastrophes could result in a scale of damage that even reinsurers might not be able to cover. While property-related risks continue to dominate the cat bond and other insurance linked securities (ILS) markets, there has been a broadening of risks transferred to capital markets to include life, accident and health, and casualty risks. Recently too, the bank Credit Suisse securitised some of its exposure to extreme operational risks, including cyber-related catastrophe losses.[111]

The ILS market for cyber risks remains nascent but it will likely expand in the future.

Some commentators believe that further innovations in ILS will ultimately pave the way for more cyber risks to be transferred to capital markets. As well as cyber catastrophe bonds, sidecar structures that pool risks for corporates, funded captive-type vehicles or some form of contingent capital instruments could all yet emerge, allowing capital markets to take on peak cyber exposures. The development of proportional agreements that allow investors to share cyber risks with expert insurance underwriters (rather than more typical excess-of-loss structures) could also encourage ILS market expansion.[112]

Investors may still need to be convinced of the portfolio diversification benefits of cyber risks.

On top of the data and risk modelling challenges, additional hurdles must be overcome if alternative risk transfer markets for cyber are to develop. First, investors will likely require more evidence that returns on securities linked to cyber risks are genuinely uncorrelated with other asset classes. One of the attractions of existing cat bonds is that the underlying perils to which they are linked tend not to occur at the same time as other events that affect credit and equity markets, offering investors diversification benefits. In contrast, the effects of a widespread cyber attack could, among others, also hit the value of stock and bond market investments.

[110] See for example, T. Ryan and W Carbone, *Cyber liability insurance: As the market heats up, is it time to cool off in a pool?*, Milliman, 23 May 2016 http://us.milliman.com/insight/2016/Cyber-liability-insurance-As-the-market-heats-up--is-it-time-to-cool-off-in-a-pool/

[111] In May 2016, the first-ever ILS related to operational risk was issued by Credit Suisse. Similar to a traditional catastrophe bond, the securitisation enables the Swiss bank to transfer to capital market investors the risk of extreme losses resulting from failed or inadequate business processes. The securities provide wide-ranging cover, including for some cyber risk exposures such as an IT system failure that causes BI, as well as more conventional operational failings linked to, for example, unauthorised activity, accounting errors, documentation errors and regulatory compliance. See "Credit Suisse Sells Operational Risk Bonds, Insuring Rogue Trading, Cyber Crime", *insurancejournal.com*, 27 May 2016, http://www.insurancejournal.com/news/international/2016/05/27/410088.htm

[112] R. Amaral, "Cyber Risks and ILS", *riskandinsurance.com*, 15 October 2016, http://www.riskandinsurance.com/cyber-risks-ils/

Willingness to absorb basis risk could also hamper the development of cyber-related ILS.

A second factor that may hold back ILS for cyber risks is potential basis risk – the difference between the sponsor's actual losses and the security's payout for a covered event. Sponsors of ILS typically want as broad coverage as possible so that they can recover the full range of losses they might incur. However, investors often want securities where the payoff is triggered by well-defined and observable metrics, because this reduces the potential for adverse selection and moral hazard (eg, less motivation to limit losses), and also lowers their costs in evaluating company-specific underwriting and financial results. Such differences in preferences often hinder the formation of a deep and liquid risk transfer market, especially when understanding of the underlying risks remains nascent.

However, the experience of nat cat bonds suggests that product innovation can foster the transfer of cyber risks to capital markets.

Nevertheless, the experience of the cat bond market suggests that over time, innovation can help align supply and demand for cyber protection through capital market vehicles. There are now a wide variety of cat bonds with indemnity-based triggers where payouts are linked to the actual losses incurred. Greater standardisation of cyber threats may help define event-driven risks with binary outcomes over a defined time period, and that could encourage investor interest. For example, some proponents of ILS suggest a trigger based on inbound data volume and how long an outage persists might be a simple way to approximate the impact of a DDoS attack, even though care would be needed to ensure the trigger mechanism could not be manipulated.[113] Worries about basis risk might also be reduced if greater information sharing leads to corresponding clarity in the coverage terms, limits and exclusions. At the same time, sponsors might become more comfortable with less-than-full loss indemnification if that leads to more timely payouts or gives them greater control over the dissemination of information about their cyber vulnerabilities.

Supporting role for governments

Government can help promote cyber resilience.

To the extent that companies collectively invest in socially sub-optimal cyber security and/or there are inherent frictions that impede cyber insurance and other risk transfer mechanisms, governments have an important role to play in promoting cyber resilience.[114] By reshaping incentives and increasing awareness of cyber threats, governments could nudge the private sector into improved market-led solutions. Two areas in particular stand out: information capture and dissemination about cyber threats and losses; and setting the legal framework.

[113] "Could the capital markets solve the $1B cyber insurance policy gap?", *artemis.bm*, 23 March 2015, http://www.artemis.bm/blog/2015/03/23/could-the-capital-markets-solve-the-1b-cyber-insurance-policy-gap/

[114] The interconnectedness of cyberspace means that if one company adopts cyber security measures, the entire community benefits as infections emerging from this company are minimised. Equally, failure to undertake security measures can potentially have large negative effects on other users.

A number of governments have set up forums to exchange information about evolving cyber threats and their impact.

Information co-ordination and dissemination

A number of governments have initiated or are setting up forums that enable companies to share databases, methods, analytical tools and models to promote best practices. These complement private-sector led initiatives to share intelligence about emerging threats (eg, through the Financial Services Information Sharing and Analysis Center, a key vehicle for the global financial industry to share cyber and physical threat intelligence).[115] Such industry-wide common data sharing platforms help increase cyber risk awareness and preparation. They are also a first step to enhanced cyber resilience (see Table 3). In anonymised form and subject to agreed use, the information will increase risk modelling possibilities and help underwriters understand individual and aggregate exposure better, leading to more risk-adequate insurance, (ie, cheaper pricing for the more resilient firms and a rise in the amount of available capacity for cyber cover).[116]

Table 3:
Selected private and government-led cyber information collaboration schemes

Country	Initiative	Aim
UK	Cyber Security Information Sharing Partnership (CiSP).	Collaborative initiative between industry and government to share cyber threat and vulnerability information. The forum is designed to capture emerging threats and trends while protecting individual insurer and insured data confidentiality.
Switzerland	The Reporting and Analysis Centre for Information Assurance (MELANI)	Public-private partnership to gather and share information about security threats to computer systems, the internet and critical national infrastructures. The MELANI website is open to private users of home computers and the internet as well as small and medium-sized enterprises (SMEs) in Switzerland
US	Cyber security Information Sharing Act (CISA); Cyber Threat Intelligence Integration Center (CTIIC); Information Sharing and Analysis Centers (ISACs).	CISA provides incentives, including liability protection, for companies to share information about cyber security breaches among one another and with the government. It also allows the federal government to share unclassified data with other agencies, businesses, and the public. CTIIC coordinates and analyses intelligence related to cyber threats and incidents. ISACs are trusted entities established by critical infrastructure owners and operators to foster information sharing and best practices about physical and cyber threats and mitigation.
Finland	Finnish Communications Regulatory Activity Authority (FICORA).	One of FICORA's core functions is to disseminate information about cyber security.
Netherlands	Nationaal Cyber Security Centrum (NCSC)	NCSC is the facilitator of several Information Sharing and Analysis Centres (ISAC), which are set up per sector (eg, water, telecom, nuclear etc.). Each ISAC is composed of sector-related members and has a chair. NCSC encourages meetings between ISACs' chairs for cross-sector information sharing.
Germany	Kooperation zwischen Betreibern Kritischer Infrastrukturen (UP KRITIS)	A joint initiative of the Federal Office of Civil Protection and Disaster Assistance (BBK) and the Federal Office for Information Security (BSI). Its objective is to facilitate co-operation across industries to maintain the supply of critical infrastructure services in Germany.
Belgium	Cyber Threat Intelligence Research Project (CTISRP)	Launched by Deloitte Belgium in 2013 for public and private organisations from Europe to discuss sharing of cyber threat information. Members come from 13 different sectors and meet several times a year.

Source: Swiss Re Economic Research & Consulting, various public sources.

[115] For the Financial Services Information Sharing and Analysis Center website, go to www.fsisac.com/

[116] In developing the privacy breach product for the US market, insurers benefited from the availability of a database that collated all personal data breaches known due to the near-universal and mandatory breach notification law in the country.

Governments are well placed to co-ordinate intelligence gathering given their access to classified information.

Governments are ideally placed to co-ordinate information sharing, not least because they have access to classified information, including intelligence gleaned through supranational agencies and networks. For example , the UK government has set up the Cyber Security Information Sharing Partnership (CiSP) and is seeking to collaborate with the private sector to make these sort of data more accessible and usable for insurers. However, some firms remain nervous about government-led cyber intelligence co-ordination given that it might create additional security vulnerabilities. Almost two thirds of corporate respondents in the Swiss Re/IBM survey indicated that government actions can increase cyber risks, which could reflect worries that information can be leaked or misused.

They can also support the development of cyber security standards which can facilitate risk assessment.

Alongside intelligence sharing, governments can be instrumental in developing detailed standards to promote highly secure IT systems. Compliance with best practice arrangements can in turn help insurers evaluate the strength of firms' internal controls and better assess their relative resilience against cyber threats. The National Institute of Standards and Technology (NIST) Framework in the US and the International Organisation for Standardisation (ISO) 27001 standard provide companies with tools to assess and increase their own cyber security. Such a principles-based approach is likely to be more flexible than a strict rules-based regime in adapting to the dynamic cyber risk landscape. Gaining security certification, for example for ISO 27001, can also increase insurers' comfort levels in offering cyber insurance.

Legal framework

Some argue that cyber insurance should be made mandatory.

In setting laws and regulations, governments have an important influence on how cyberspace is used and protected. Some commentators go as far as to suggest that the purchase of cyber insurance should become mandatory, at least for third-party liability and for some key industries that are at high risk of attacks.[117] This view is echoed in survey evidence with more than three quarters of insurer and non-insurer respondents suggesting that cyber insurance should be mandatory for some industries, especially financial services and airlines.[118]

Although others worry compulsory cover may be administratively costly and encourage moral hazard.

Advocates of mandatory cover argue that it would encourage firms to invest in cyber security in order to widen the insurance pool and reduce associated premiums. At the same time, detractors highlight that enforcing such a regime, if not impossible, would be administratively burdensome. Furthermore, some worry that it would create moral hazard, with companies relying on their insurance rather than investing in improved security. Requiring insurers to purchase cyber insurance from competitors could also raise questions about market effectiveness and integrity.

[117] See "Cyber-insurance: Is it necessary? Should it be mandatory?" *techtalkgfi.com*, 4 December 2014, http://www.gfi.com/blog/cyber-insurance-is-it-necessary-should-it-be-mandatory/

[118] Swiss Re/IBM, op. cit.

Other legal initiatives such as statutory limits to liability may promote increased cyber insurance penetration.

Other policy initiatives may be helpful in promoting increased cyber insurance penetration as they have in other lines. In particular, providing a means for companies to cap their legal liability if they pursue enhanced security measures may encourage insurers to offer improved terms and conditions, making cyber insurance more affordable. By way of analogy, in the US, under the SAFETY Act adopted in the wake of the 9/11 attack, firms can limit legal damages that result from a failure of a particular anti-terrorism technology if it has been approved by the Department of Homeland Security (DHS).[119] Insurance brokers tend to believe that similar government measures including tax credits on premiums, a cyber incident data repository and formal guidelines for safeguarding information could help support the availability of cyber coverage systems.[120] Legislation can also help eliminate some of the legal uncertainties over potential liability that could result from sharing cyber threat intelligence.[121]

Governments might also enable the establishment of insurance pools to cover cyber risks.

Governments can also be instrumental in setting up insurance pools that enable private re/insurers to share exposures to a particular peril and underwrite each others' risk. The insurability of some cyber risks can be improved if the risks of the market participants are pooled, not least because of the diversification benefits that may be achieved.[122] Public-sector involvement can facilitate collaboration and information exchange among market participants and potentially take on some of the administration costs. Government-sponsored insurance pools can also safeguard any pooling arrangements from contravening applicable competition laws.

[119] The SAFETY Act requires DHS to set the limit of liability for each applicant based on the amount of insurance available and the burden to purchase coverage up to that limit.

[120] CIAB, op. cit.

[121] This is true for example with the act in the US Cybersecurity Information Sharing Act CISA. See also, A. Nolan, *Cyber Security and Information Sharing: Legal Challenges and Solutions*, Congressional Research Service, March 2015.

[122] M. Eling and J. H. Wirfs, *Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class*, Institute of Insurance Economics, University of St. Gallen in collaboration with Swiss Re, March 2016.

Conclusion

Cyber risk awareness is growing although this has yet to translate into institutionalised risk management.

Cyber risk is a growing concern for companies. Recent high-profile cyber attacks have demonstrated the threats that security breaches pose, and how ill-prepared some firms are to cope with such an event. Moreover, the costs of a cyber breach are no longer confined to dealing with the fallout from lost or corrupted data but increasingly include potential damage to a firm's reputation and physical property, as well as disruption to regular business operations. So far, however, relatively few companies have implemented widespread improvements in mainstream risk management practices and cyber defences.

Firms need to increase investment in their cyber defences, especially given heightened regulatory scrutiny.

Regulation could yet be a catalyst for change. Legislation is coming on-stream in many jurisdictions that will compel firms to introduce enhanced safeguards for their customers' private information or face sanctions should they fall short of the required standards. But firms cannot afford to wait for changes in laws: greater investment in cyber security architecture is needed now in order to develop robust pre-and post-loss risk management procedures and capabilities. This is true of both large and small firms, with the latter increasingly targeted by cyber attackers.

Insurance and alternative risk transfer mechanisms are developing.

Transferring cyber-related risks to insurers and capital market investors will increasingly become a viable solution, particularly those linked to failures in routine cyber hygiene such as maintaining the integrity of customer and network security. Dedicated cyber insurance is developing and many insurers are looking to innovate and expand cyber policies to cover losses beyond data privacy breaches. Likewise, there are nascent initiatives to develop insurance-linked securities that cover operational-type risks like cyber, although significant hurdles need to be overcome before such alternative risk transfer mechanisms become mainstream.

But further innovation is needed to monitor and quantify cyber risks.

Cyber risks are complex to understand and quantify, especially given the potential for losses to accumulate. New ways of thinking are 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 are looking to develop measurement frameworks and metrics that are sufficiently flexible to take into account rapid changes in the technological and business environment, although further progress is required. By the same token, firms are becoming more comfortable sharing information, which will be crucial if insurers are to do a better job at assessing and underwriting the risks.

By cooperating, insurers and the insured can expand insurability.

To create a viable private cyber insurance market, the insureds and their insurers will need to cooperate in creating sustainable products. Government also has a role to play by encouraging information capture and dissemination about cyber threats, and setting the accompanying legal framework. Ultimately, however, some cyber risks, especially those related to extreme catastrophic loss events such as a disruption to critical infrastructure or networks, may be uninsurable. The ambiguity over the likelihood of a loss event and/or its magnitude together with the potential for significant accumulated losses mean that there are natural limits on the risk absorbing capacity of private insurers and investors.

Recent *sigma* publications

2017	No 1	Cyber: getting to grips with a complex risk
2016	No 1	Natural catastrophes and man-made disasters in 2015: Asia suffers substantial losses
	No 2	Insuring the frontier markets
	No 3	World insurance 2015: steady growth amid regional disparities
	No 4	Mutual insurance in the 21st century: back to the future?
	No 5	Strategic reinsurance and insurance: the increasing trend of customised solutions
2015	No 1	Keeping healthy in emerging markets: insurance can help
	No 2	Natural catastrophes and man-made disasters in 2014: convective and winter storms generate most losses
	No 3	M&A in insurance: start of a new wave?
	No 4	World insurance in 2014: back to life
	No 5	Underinsurance of property risks: closing the gap
	No 6	Life insurance in the digital age: fundamental transformation ahead
2014	No 1	Natural catastrophes and man-made disasters in 2013: large losses from floods and hail; Haiyan hits the Philippines
	No 2	Digital distribution in insurance: a quiet revolution
	No 3	World insurance in 2013: steering towards recovery
	No 4	Liability claims trends: emerging risks and rebounding economic drivers
	No 5	How will we care? Finding sustainable long-term care solutions for an ageing world
2013	No 1	Partnering for food security in emerging markets
	No 2	Natural catastrophes and man-made disasters in 2012: A year of extreme weather events in the US
	No 3	World insurance 2012: Progressing on the long and winding road to recovery
	No 4	Navigating recent developments in marine and airline insurance
	No 5	Urbanisation in emerging markets: boon and bane for insurers
	No 6	Life insurance: focusing on the consumer
2012	No 1	Understanding profitability in life insurance
	No 2	Natural catastrophes and man-made disasters in 2011: historic losses surface from record earthquakes and floods
	No 3	World insurance in 2011: non-life ready for take-off
	No 4	Facing the interest rate challenge
	No 5	Insuring ever-evolving commercial risks
	No 6	Insurance accounting reform: a glass half empty or half full?
2011	No 1	Natural catastrophes and man-made disasters in 2010: a year of devastating and costly events
	No 2	World insurance in 2010
	No 3	State involvement in insurance markets
	No 4	Product innovation in non-life insurance markets: where little "i" meets big "I"
	No 5	Insurance in emerging markets: growth drivers and profitability
2010	No 1	Natural catastrophes and man-made disasters in 2009: catastrophes claim fewer victims, insured losses fall
	No 2	World insurance in 2009: premiums dipped, but industry capital improved
	No 3	Regulatory issues in insurance
	No 4	The impact of inflation on insurers
	No 5	Insurance investment in a challenging global environment
	No 6	Microinsurance — risk protection for 4 billion people
2009	No 1	Scenario analysis in insurance
	No 2	Natural catastrophes and man-made disasters in 2008: North America and Asia suffer heavy losses
	No 3	World insurance in 2008: life premiums fall in the industrialised countries — strong growth in the emerging economies

Published by
Swiss Re Institute
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
Darren Pain
Telephone +41 43 285 2504

Jonathan Anchen
Telephone +91 80 4900 2650

sigma editor
Paul Ronke
Telephone +41 43 285 2660

Editor in chief
Kurt Karl,
Head of Economic Research & Consulting,
is responsible for the sigma series.

Explore and visualise sigma data on natural catastrophes and the world insurance markets at www.sigma-explorer.com

© 2017 Swiss Re. All rights reserved.

The editorial deadline for this study was 24 January 2017.

sigma is available in English (original language), German, French, Spanish, Chinese and Japanese.

sigma is available on Swiss Re's website: www.swissre.com/sigma

The internet version may contain slightly updated information.

Translations:
German: Diction AG
French: ithaxa Communications SARL
Spanish: Traductores Asociados Valencia S.L.

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

Printing: Multicolor Print AG, Baar

MIX
Paper from responsible sources
FSC® C022369
www.fsc.org

This report is printed on sustainably produced paper. The wood used comes from forest certified to 100% by the Forest Stewardship Council (FSC).

The entire content of this *sigma* edition 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 sigma 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 "Swiss Re, *sigma* No 1/2017" 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.

Order no: 270_0117_en

Swiss Re Institute
Mythenquai 50/60
P.O. Box
8022 Zurich
Switzerland

Telephone + 41 43 285 2551
Fax +41 43 282 0075
sigma@swissre.com
www.swissre.com