Journal of Cyber Policy

ISSN: 2373-8871 (Print) 2373-8898 (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

Cyber risk and the changing role of insurance

Mark Camillo

To cite this article: Mark Camillo (2017) Cyber risk and the changing role of insurance, Journal of Cyber Policy, 2:1, 53-63, DOI: 10.1080/23738871.2017.1296878

To link to this article: https://doi.org/10.1080/23738871.2017.1296878

Published online: 27 Mar 2017.

JOURNAL OF CYBER POLICY, 2017
VOL. 2, NO. 1, 53–63
http://dx.doi.org/10.1080/23738871.2017.1296878

Routledge
Taylor & Francis Group

Cyber risk and the changing role of insurance

Mark Camillo

EMEA, American International Group, London, UK

ABSTRACT

A brief look at how the cyber risk landscape is evolving and what this means from a risk and insurance perspective, particularly as businesses accept they cannot hope to prevent all cyber intrusions regardless of the sophistication of their IT security. While cyber insurance is currently a stand-alone product, we are moving to a future where all classes of risk and insurance will be touched by cyber. Meanwhile, the rapid pace of technological change, increasing connectivity through the internet of Things and the changing MO of cyberattackers introduce new vulnerabilities and increase the potential for systemic and risk aggregation complexities that will need to be measured and monitored by insurers. As cyber underwriters scrutinise the IT security of firms seeking insurance, they also have an important and growing role as a de facto regulator. They are setting the bar for the cyber hygiene standards necessary in order to qualify for insurance, and in so doing, encouraging organisations large and small to implement systems and processes that will mitigate cyber risk.

ARTICLE HISTORY
Received 22 November 2016
Revised 15 February 2017
Accepted 15 February 2017

KEYWORDS
Cyber insurance; internet of Things; data breach; system failure; ransomware; cyber extortion

Part one: A surprisingly long history

Cyber insurance has been available since the late 1970s,[1] with the market growing out of the tech risk/tech errors and omissions (E&O) space. In the 1980s, the first tech E&O policies that included cybersecurity insurance were introduced, designed primarily for financial institutions and blue chip organisations. Cyber insurance as a stand-alone product began to take off in response to Y2K[2] concerns and was designed to fill gaps in traditional property and casualty (P&C) products. The number of insurance providers offering the product gradually expanded, although it remained a niche and specialised market during these early days.

Following Y2K, the dotcom crash and the 9/11 attacks, interest in cyber insurance grew.[3] There was a growing realisation that the virtual world did not necessarily fit within the scope of many traditional covers/classes of insurance. Organisations' initial concerns surrounded the spreading of viruses and other types of malware and their potential legal liability. There was also a recognition that virtual events could cause substantial business interruption losses that were unlikely to be covered under traditional property business interruption policies.

CONTACT Mark Camillo mark.camillo@aig.com

However, a growing appreciation of cyber vulnerabilities did not immediately translate into demand for insurance. Most corporate expenditures during the late 1990s and early 2000s focused on loss mitigation and network security. Meanwhile, insurers grappling with this emerging risk area were reluctant to offer significant line sizes for a product that was largely untested and where there was a dearth of historical loss data upon which to measure and price the risk. There was a feeling among corporate risk and insurance buyers that the cyber insurance market remained a niche area, lacking the scope and capacity they required.

The next wave of growth was driven by new privacy regulation in the U.S., which followed a spike in identity theft and mass data breaches. This prompted the first data breach notification law in California, which was enacted in 2002 and became effective on 1 July 2003. Other states followed, mandating that companies had to immediately disclose a breach to customers, usually in writing, in addition to the regulatory authorities.[4] In the EU, E-Privacy Regulations were introduced in 2009 for telecommunication companies and internet service providers, while financial regulators have demonstrated their willingness to impose fines on banks and insurers for data failings.[5]

Cyber insurance products underwent a shift in response to these new notification requirements towards indemnifying the costs associated with a major data breach. The market gained quickest momentum in the U.S., where notification rules applied to all sectors. As news of major corporate breaches began to hit the headlines and information about the costs associated with breaches (including regulatory penalties, loss of business and reputational damage) became increasingly available, demand for cyber insurance coverage grew and the market began to take off.

In addition to data on the average cost of a data breach, information on the average length of time hackers are inside systems before they are discovered has become available. One study found that it took an average of 170 days before a breach was discovered with this period almost doubling where an attack involved an insider.[6]

Of those breaches that are discovered (many are not), a large number are uncovered by third parties rather than the organisation itself. This can include intelligence agencies, such as the FBI and Government Communications Headquarters (GCHQ). A further 45 days following discovery of a breach is needed on average for recovery and mitigation. Therefore, it can take up to seven months between the initiation of an attack and recovery from it, with some breaches taking a year or more to resolve (Figure 1).[7]

The TJX hack[8] was a turning point. In 2007, the retailer announced that over 45 million of its customers' credit and debit cards had been compromised. Estimates suggest the breach cost the company between $1 billion and $4.5 billion. In 2014, 25 class action lawsuits were settled and the organisation paid out $177 m. The breach heightened awareness and appreciation of the potential reputational and brand damage that could result from such an incident.

Concern also mounted over the potential business interruption damages that could be incurred post-breach. The 2011 Sony PlayStation attack that exposed around 100 million user accounts brought the network down for nearly a month, resulting in losses of $170 m and fines from the UK Information Commissioner's Office (ICO) of £250,000.[9]

After the 2013 data breach of retailer Target that resulted in the leak of tens of millions of credit and debit card accounts, and the record breach at health insurer Anthem in early 2015, there was a realisation that companies could no longer hope

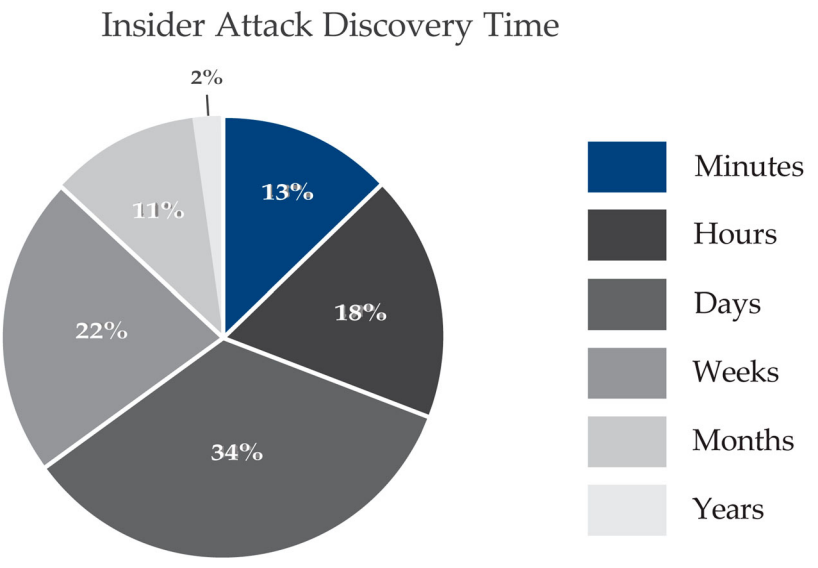

Figure 1. Insider attack discovery time. Source: Verizon Data Breach Investigations Report 2014.

to simply avoid cyberattacks through IT security. These incidents demonstrated that even organisations with robust risk mitigation and security measures were not immune. Going forward, the emphasis is on striking a balance between prevention, detection and recovery.

Part two: Cyber insurance: an increasingly sophisticated market

The cyber insurance market today has matured considerably and has become specialised and innovative. This includes products that cater to small- to medium-sized enterprises (SMEs), the mid-market sector as well as very large multinational corporations.

While the majority of cyber products have a number of features in common, there are a wide range of products and policy limits (i.e. how much cyber insurance cover can be bought) available in the market. The lack of standardisation reflects the fact that cyber insurance is a relatively new cover, its evolution out of existing products (e.g. tech E&O and property insurance) and the competitive nature of the business (there is a bespoke nature to many classes of commercial insurance).

Among the features included in most cyber insurance policies are cover for first- and third-party exposures, including loss or damage to digital assets, data recovery, business interruption, notification costs, liability in respect of data breaches, multimedia liability, employee dishonesty, cyber extortion and regulatory defence costs. Insurers also offer a number of services to their insureds (customers), most notably crisis management, forensic IT, security advice and legal consultation.

Many carriers have partnered with third-party vendors to offer 24-hour incident response services and, increasingly, pre-loss consulting and post-breach planning. Products have also adapted to encompass new and growing threats, including the potential for physical damage arising from a cyberattack. While there are currently only a few

examples of cyber intrusions that have caused damage to property and equipment, this exposure is expected to grow in the future as the threat environment evolves.

The insurance industry and regulators are questioning the potential for cyber risk aggregation, or systemic risk, whereby one event triggers multiple losses for multiple insurance companies. The industry is seeking to better model extreme scenarios in an effort to understand how insurance and reinsurance companies should be treating the exposure from a capital perspective.

According to one study,[10] Europe's Solvency II framework massively underestimates the threat to insurers from operational cyber risk and suggests that capital requirements are only sufficient if carriers are underwriting a significantly large and well-diversified book of business.

Of particular concern from an aggregation perspective are the activities of state-sponsored or terrorist attackers, who may not be motivated by monetary gain but by the desire to cause damage and disruption to national infrastructure and economies. Major events, such as a cyberattack on the U.S. power grid, as set out in a 2015 study by Lloyd's and the University of Cambridge's Centre for Risk Studies, could trigger catastrophic and far-reaching losses.

In this hypothetical scenario, which envisages hackers shutting down parts of the U.S. power grid, plunging 15 U.S. states and Washington, D.C. into darkness, the total impact on the U.S. economy was estimated at $243 billion, rising to over $1 trillion in the most extreme scenario.[11] 'As insurers, we need to think about these sorts of complex and interconnected risks and ensure that we provide innovative and comprehensive cyber insurance to protect businesses and governments', said former Lloyd's director of performance management Tom Bolt.[12]

Interconnected world

Having established the increasing complexity of cyber insurance over the past decades, the situation is further complicated by the unceasing proliferation of technology, the increase in network speed and an explosion of data. Taken together, these developments are multiplying the potential attack surface for malicious actors, with predictions that 20.8 billion connected things will be in use globally by 2020, up from 6.4 billion today.[13] The growth of the internet of Things (IoT) has introduced new vulnerabilities, as not all connected devices are currently designed with security in mind.

The Distributed Denial of Service (DDoS) attack against DNS service provider Dyn, which used the Mirai botnet coordinated through tens of millions of connected devices including surveillance cameras, webcams, smart thermostats and baby monitors, has focused the minds of cybersecurity experts to the threat posed by IoT. The audacious and coordinated cyberattack, which occurred on 21 October 2016, brought down websites including Twitter, Netflix, Reddit, CNN and many others in the U.S. and Europe.

It followed a similar DDoS attack in September that targeted security news portal KrebsOnSecurity, which turned IoT devices into 'digital cannons'[14] in order to bombard the website with as much as 620 gigabits per second of junk data. This was an immense amount of traffic – many orders of magnitude greater than is typically needed to knock most sites offline[15] – blocking the way for legitimate users.

In early November 2016, the same tactics were used to wage multiple attacks against Liberia's internet infrastructure, taking an entire country offline over the course of a week. Liberia was particularly susceptible to attack due to its reliance on a single submarine cable to supply all of its internet needs.[16]

The potential for physical damage and bodily injury arising from the exploitation of IoT by hackers is of growing concern. In 2015, hackers Charlie Miller and Chris Valasek demonstrated how they could remotely access the control systems of a Jeep Cherokee,[17] sending commands through the vehicle's entertainment system to control its dashboard functions, steering, brakes and transmission.

In a world where connected cars and homes are becoming the norm, stunts such as these raise questions about the ability to exploit thermostats, wearable devices and internet-connected heating, and ventilation and air conditions systems. This last is thought to have been the weak link that led to the massive data hack of retailer Target in 2013.

In 2014, a blast furnace at a German steel mill was damaged following a cyberattack at the plant's network. Attackers had used stolen logins that gain access to the mill's control systems, according to the annual report of the German Federal Office for Information Security (BSI). The intrusion led to parts of the plant failing, meaning that the blast furnace could not be shut down as normal, resulting in significant damage. 'The know-how of the attacker was very pronounced, not only in conventional IT security but extended to detailed knowledge of applied industrial controls and production processes', the report states.[18]

NATO and other defence bodies have stated their concern that politically motivated incidents, such as the December 2015 Ukraine power grid attack and the 2010 Stuxnet attack on Bushehr Nuclear Power Plant in Iran, will become more common as cyberspace becomes the new domain of warfare.[19] In 2011, CIA Chief Leon Panetta warned that the 'next Pearl Harbor could be a cyberattack that cripples' America's electrical grid, its security and financial systems.[20]

Cyberattacks are increasingly a national security issue. In the U.K., the GCHQ has set up a National Cyber Security Centre (NCSC) in an effort to protect government sites and industries regarded as central to national security. In September 2016, it revealed that the number of detected cybersecurity incidents had doubled year-on-year to 200 per month[21] and is offering to widen its scope to include major private companies.

Inevitably, technological breakthroughs that are intended to benefit society also have the potential to be compromised by cybercriminals. 'With new opportunities come new vulnerabilities', NCSC chief executive Ciaran Martin told the Billington Cyber Security Summit in Washington, D.C. on 13 September 2016. 'So alongside the ability to transact, process and store data on an unprecedented mind scale so comes the risk of being compromised on an unprecedented scale.'

Trillion-dollar business

Cybercrime has become an industry led by organised criminal networks, costing the global economy approximately $445 billion a year,[22] potentially reaching $1 trillion within the next decade.[23] Hostile states, terrorists, hacktivists and lone operators are also among the rich web of hostile actors looking to compromise the digital environment to achieve a variety of outcomes, from commercial gain through to destructive attack. Data theft

remains a major concern for the corporate world with the cost of data breach steadily rising and increasingly stringent data protection laws needing to be complied with.

There is a recognition that organisations can no longer hope to build a fortress to keep the cybercriminals out. The emphasis from a cybersecurity perspective has shifted to focus on risk mitigation, data loss prevention software and the ability to detect and contain intruders. 'There are only two types of companies, those that have been hacked and those that will be hacked', said former FBI director Robert Mueller.[24]

In 2016, the average cost of a data breach rose to $4 m, according to IBM and the Ponemon Institute, up by 29% since 2013.[25] The study found that regulated industries, such as healthcare and financial services, have the most costly breaches because of fines and a higher-than-average rate of lost business and customers. Given its strict data protection laws and tort environment, the U.S. remains the country with the most costly data breaches (with an average cost of $7 m), followed by Germany, with an average cost of $5 m (Figure 2).

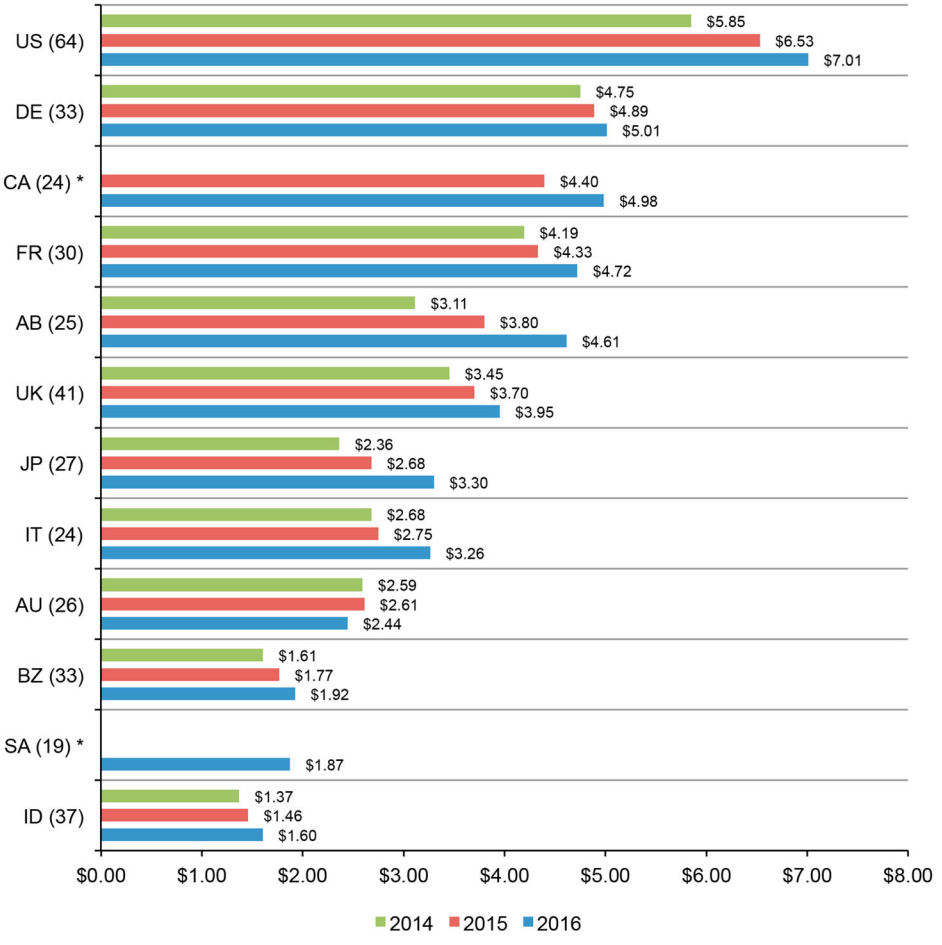

Figure 2. The average total organizational cost of a data breach over three years. Grand average for FY 2016 = $4.0, FY 2015 =$3.8, FY 2014 = $3.50. Source: 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute.

Note: *Historical data is not available in all years (FY 2016 = 383, FY 2015 = 350, FY 2014 =315). Measured in US$ (millions).

The reputational impact of a data breach or cyber intrusion is also of growing concern to risk managers and their C-suite, particularly in jurisdictions where organisations are subject to strict notification rules. Damage to reputation/brand emerged as the top-ranked risk in insurance broker Aon's Global Risk Management Survey 2015. Meanwhile, cyber risk entered the top 10 for the first time with Aon president and CEO Greg Case noting 'the connection between these two risks has been felt around the world'.

In a digitised world, corporate risk managers are increasingly concerned about business interruption arising from a cyber incident.[26] Forty-nine per cent of respondents to Neustar's Worldwide DDoS Attacks & Protection Report revealed that they could lose over $100,000 per hour during periods of business interruption, with 33% saying the cost would be $250,000 or more per hour. Thirty-nine per cent of the 1,002 C-suite executives surveyed also said it had taken their organisation three hours or more to detect a distributed denial of service attack.[27]

Cyber extortion and ransomware are also on the rise, although actual loss numbers are less easy to come by as a great many of these attacks go unreported (up to 85% of national cybercrimes are not reported, according to estimates by both the City of London Police and the FBI).[28] However, it is thought that ransomware operators running rival CryptoWall code have generated around $325 m in revenue over the past three years, according to research by the Cyber Threat Alliance,[29] while the Cryptolocker gang made over $30 m in 2015 using relatively simple ransomware.[30]

A significant number of successful cyber intrusions have a human element, either deliberately or in error, by falling for a phishing scam for instance, or making mistakes in how individuals configure a server, application, security defences or other devices. It is thought that as many as 70–80% of cyber insurance claims result from human error or malfeasance. Hackers know that employees are often the weakest link when it comes to network security, which is why they are so often targeted by cybercriminals. Globally, business email compromise attacks have cost companies $3.1 billion since January 2015.[31]

In this way, privileged users, who hold the 'keys to the kingdom' and have unfettered access to an organisation's network, devices and servers, are often an organisation's greatest security risk. Meanwhile, evidence suggests that the methods being used to compromise such individuals are becoming more sophisticated. Spear phishing and whaling attacks, for instance, are aimed at senior executives and use personalised information (often gleaned via social media) to appear genuine.

Part three: Cyber insurance will be different in the future

Total annual cyber premiums have reached $2.5 billion, with some predicting the market could grow to $20 billion or more by 2025.[32] Key to this growth is the need for better data and analytics surrounding the underlying risk and there are currently a number of efforts underway in the market by both incumbents and insurtech start-ups to build cyber risk models.

Reinsurance (insurance for insurance companies) support will grow in response to better data and tools, supporting the overall growth of the market. Organisations seeking to take out cyber insurance will be able to access higher limits (broader insurance cover) as insurance companies will be able to transfer some of their risk onto reinsurance companies, and potentially the capital markets (via tools such as catastrophe bonds).

Legislation will continue to drive demand for cyber insurance cover, particularly surrounding data and privacy. The EU General Data Protection Regulation (GDPR) is coming into force in 2018, introducing new fines for failing to adequately protect sensitive data and mandating companies to notify the authorities and their stakeholders of a data breach, within 24 hours where feasible.

UK businesses are preparing for the new legislation, anticipating it will be adopted and continue as law after the UK exits the European Union. The ICO fined TalkTalk a record £400,000 for the 2015 breach in which the personal data of 156,959 customers was compromised. But had it occurred under the GDPR, company fines could have amounted to as much as £90 m.[33] Even in the absence of such fines, TalkTalk's share price and profits took a hit with pre-tax earnings down by half in the first quarter of 2016 (to £14 m, down from £32 m in Q1 2015).

Reputational covers offered as part of cyber insurance packages or as stand-alone products are expected to evolve. Most of the current generation of reputational products are focused around offering access to crisis management expertise. Future products are more likely to offer indemnification for loss of business arising from adverse publicity following a cyber event. The London and Lloyd's market is in the process of innovating to offer more meaningful reputational risk transfer based around business interruption-style policies.

It is also expected that pricing and limits available in the cyber insurance market will be based around the sophistication of a client's cybersecurity. Firms with ISO 27001 (the international standard relating to information security management) certification in place demonstrate, for instance, that they are managing information security risk effectively and the costs and exclusions of their cyber policies typically reflect that.

Similarly, the U.K. government's Cyber Essentials scheme is being encouraged for SMEs seeking to obtain cyber insurance coverage. It is also an important means with which to satisfy clients and suppliers that these firms have implemented best-practice information security processes.

In this way, the insurance industry will become a de facto regulator, setting the bar for the standards necessary to qualify for cyber coverage. Insureds will need to demonstrate that they have met certain cyber hygiene and pre-loss standards in order to obtain indemnification and, increasingly, these requirements will extend to the supply chain as part of the procurement process.[34]

This is not a new role for the insurance industry. In the same way that insurers drove greater safety standards in the property insurance market, setting up the first fire departments in the seventeenth century following the Great Fire of London in 1666 and later encouraging the installation of sprinkler systems and other firefighting technology, the insurance industry will help to drive best practice around cybersecurity as the twenty-first century progresses.

Insurers and insureds will continue to collaborate with external security experts for loss prevention and post-breach services. With the awareness that the first 48 hours following detection of a breach is a critical window of opportunity to contain a crisis, this is a focus for much of the current collaboration taking place in the industry. The emphasis, however, continues to shift from reactive to proactive, with pre-loss planning and services increasingly taking centre stage (Figure 3).

In partnership with cybersecurity firms, insurers and brokers can carry out simulated cyberattacks – or cyber war-gaming – to test their clients' systems and breach response.

To reduce damage and impact, organisations need the ability to:
• Efficiently assess and determine the scope of the event;
• Act decisively to contain the impact and preserve forensic information;
• Determine when to engage or report to law enforcement and/or regulatory bodies;
• Manage communications to control public and investor perception;
• Activate business continuity and recovery mechanisms.

Figure 3. Source: Deloitte.

Such exercises help management improve their understanding of the potential impact of a cyber incident and help them to hone their decision-making skills, learning firsthand how difficult this can be in a stressful situation. They are also useful for staff as anecdotal evidence suggests simulated phishing attacks can make individuals more alert in the future.

Security education can improve phishing defence by 64%, according to one independently conducted study by Ponemon and Wombat Security.[35] The authors of the report noted that mock phishing attacks were one of the best ways of determining how susceptible employees are to social engineering tricks from cybercriminals.

Looking further into the future, it is possible that insurance companies will be able to tailor and adjust the coverage they provide based on their clients' changing risk profile. Significant advances in anomaly detection and other methods of monitoring cyber hygiene, for example, putting sensors on networks, will enable the growth of 'cybermatics'/dynamic risk management. Just as telematics captures driving behaviour, helping insurers set premiums up or down based on usage and safety, this will be possible with constant insight into clients' risk posture and cybermatics scores.

As discussed, the IoT will create numerous opportunities within retail and commercial sectors but will also introduce new vulnerabilities. Analysis from a Symantec honeypot, which collects IoT malware samples, found that the highest number of IoT attacks originated in China (34%), followed by the U.S. (26%) and Russia (9%). 'The current IoT threat landscape shows that it does not require much to exploit an embedded device', noted the cybersecurity firm.[36]

Regulators are likely to put more pressure on product manufacturers to ensure security is a priority at the R&D stage and not an afterthought. Some organisations have traditionally relied on 'air gapping' as protection from cyber threats – which involves taking all possible steps to isolate and disconnect their networks from the outside world. However, such organisations – including those with Industrial Control Systems or supervisory control and data acquisition systems – may need to reconsider this approach in a hyper-connected world. Even where they are making use of air gapping, IoT presents new opportunities to compromise the previously infallible perimeter.

Will cyber continue to require stand-alone cover?

There is a growing realisation that many traditional classes of insurance are exposed to cyber risk, an exposure that may not currently be priced or excluded. This includes directors and officers (D&O), environmental liability, healthcare, motor and property insurance, among others. When traditional insurance products unintentionally extend cover to cyber-related losses, it may, however, be limited in scope.

A number of claims in the U.S. have demonstrated how cyber liability has the potential to cross over into D&O, for instance as a result of derivative actions brought by shareholders against company directors in the aftermath of a data breach. Litigation against Target and Wyndham targeted the companies' directors and officers for breach of fiduciary duty, among other things. The explosion of the IoT could exacerbate the crossover of cyber into other classes of business.

Insurance could evolve so that all traditional insurance policies will adapt to include cyber wordings, and for this exposure to be considered and priced by underwriters. The other, more likely, scenario is that cyber exclusions will become more commonplace within traditional classes of business as insurers seek to better manage their total exposure. For this to happen, stand-alone cyber insurance will need to further evolve as the main source of comprehensive cyber liability cover, encompassing physical damage and bodily injury.

Due to concerns over aggregation, many insurers are currently reluctant to offer substantial limits for cyber terrorism, or cyberattack as it is termed in Lloyd's market. As time passes, and a historical claims record builds up, the concepts and wordings within cyber policies will be put to the test. This will result in an increased pool of premium dedicated to a broad range of cyber exposures, with higher limits available and greater diversity of risk. Whereas available limits from many cyber insurance carriers were just $10 m three years ago, today insurance brokers are able to place $500 m programmes.

This requires increasing support from reinsurers. Efforts to standardise cyber risk data and develop models will assist the reinsurance market as it looks to increase its support of the cyber insurance market. The better cyber insurers are able to measure and monitor their accumulation risk, the more reinsurance coverage they will be able to access. It is possible that the liquidity and depth of the capital markets may be necessary for some catastrophic cyber risk scenarios, with the risk transferred via instruments such as catastrophe bonds.

In the absence of traditional and alternative risk transfer mechanisms, the financial cost of major cyber incidents will be borne by governments, corporates and their shareholders. However, it is increasingly likely that shareholders and regulatory authorities will mandate the purchase of comprehensive cyber insurance in an effort to close the gap between economic and insured cyber losses.

Notes

1. https://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf
2. The Y2K problem, otherwise known as the Millennium bug, arose because programmers represented the four-digit year with only the final two digits.
3. http://www.insuranceinstitute.ca/en/resources/insights-research/cyber-risks.aspx
4. https://en.wikipedia.org/wiki/Security_breach_notification_laws
5. http://www.computerweekly.com/opinion/The-only-way-is-tough-the-future-of-data-protection-law
6. http://www.csoonline.com/article/2837805/malware-cybercrime/your-business-can-t-afford-the-cost-of-cyber-crime.html
7. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN
8. http://www.computerweekly.com/news/2240080607/TJX-hack-the-biggest-in-history
9. http://www.bbc.com/news/technology-21160818

10. http://aria.org/Annual_Meeting/2016/Papers/Session6/VI-C/Does%20Insurance%20Regulation%20Adequately%20Reflect%20Cyber%20Risk-An%20Analysis%20of%20Solvency%20II%20and%20the%20Swiss%20Solvency%20Test.pdf
11. http://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout
12. https://www.lloyds.com/news-and-insight/press-centre/press-releases/2015/07/business-blackout
13. http://www.gartner.com/newsroom/id/3165317
14. https://arstechnica.co.uk/security/2016/09/why-the-silencing-of-krebsonsecurity-opens-a-troubling-chapter-for-the-net/
15. https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
16. http://www.express.co.uk/life-style/science-technology/728816/liberia-internet-offline-massive-cyber-attack-ddos-mirai-botnet-dyn
17. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
18. https://www.wired.com/wp-content/uploads/2015/01/Lagebericht2014.pdf
19. http://www.nato.int/cps/en/natohq/topics_78170.htm
20. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html
21. https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk
22. http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf
23. https://www.bnymellon.com/emea/en/our-thinking/insurance-linked-securities-cyber-risk-and-the-capital-markets.jsp
24. https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies
25. https://securityintelligence.com/cost-of-a-data-breach-2016/
26. http://aon.mediaroom.com/news-releases?item=137400
27. https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it-security/ddos/2016-fall-ddos-report.pdf
28. *Cyber Extortion Risk Report 2015*, NYA International, Oct 2015.
29. https://cyberthreatalliance.org/pr/pr-102915.html
30. http://www.pcworld.com/article/2082204/crime-pays-very-well-cryptolocker-grosses-up-to-30-million-in-ransom.html
31. https://www.proofpoint.com/us/corporate-blog/post/FBI-Warning-Business-Email-Compromise-Attacks-Increase
32. http://www.willis.com/documents/publications/Industries/construction/MR%20Spring%20Update%20Final.pdf
33. http://www.itproportal.com/2016/07/17/the-eu-gdpr-the-clock-is-ticking-for-uk-businesses/
34. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-best-practices-in-cyber-supply-chain-risk-management.pdf
35. https://www.wombatsecurity.com/press-releases/new-ponemon-research-shows-wombat-delivers-roi
36. https://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributor

Mark Camillo joined AIG in 2001 and is Head of Cyber, EMEA, having previously led the cyber team for the Americas. He has held positions across the organisation including in Affinity Group, Accident & Health, Professional Liability and the Fidelity team. Prior to AIG, Mark worked in sales, marketing and product development for Dun & Bradstreet (D&B) and SITEL Corporation. He has an MBA from SUNY Buffalo and a B.Sc. from the University of Wyoming.