# Cyber Insurance and Risk Management: Challenges and Opportunities

## A new playground for underwriters?

**Corporate boards** the world over are scrambling to address the unique challenges of the COVID-19 global pandemic – particularly the impact of social distancing. In addition to the obvious problems this causes for any front-facing business, many organisations have had to move large workforces to a 'work-from-home' setting overnight.

Business critical systems are now running 24/7 on the same WiFi networks that our teenagers are quietly using to download pirated films from websites riddled with malware. Employees are making difficult choices about whether to prioritise getting their work done and supporting important business functions or to prioritise following the same kind of strict security protocols put in place for the occasional day spent working outside the office. The cost of this will become apparent eventually. For now, it's a crisis waiting to emerge.

One of the mechanisms that boards are deploying to deal with cyber risk is insurance – and for good reasons. In the UK over the past four months, there have been 2950 breaches relating to COVID-19 reported to the ICO (ICO, 2020). Globally, there has been a 30% increase in ransomware attacks in the same period with the ransom averaging $100,000 USD (Marsh, 2019). However, while Covid-19 may act as a catalyst for the uptake of cyber insurance, the unique circumstances might challenge or even limit the responsiveness of insurance providers.

The cyber insurance market is still relatively immature and the ability to accurately model cyber risk is quite limited. However, resources do exist which outline cyber security considerations and guide organisations thinking about taking out cyber insurance (National Cyber Security Centre, 2020). Insuring against cyber incidents requires understanding business risks and this often gets left off the table when the chief information security officer

### About the authors

**Kristen Kuhn** is a Researcher in Maritime Cybersecurity in the Systems Security Group at the Institute of Future Transport and Cities at Coventry University. She specialises in cybersecurity decision-making and the maritime industry. Her current work includes how corporate boards assess cyber-risk and make investment decisions about cybersecurity.

**Srinidhi Vasudevan** is a researcher in the Cyber Readiness for Boards project at UCL. She specialises in data-driven modelling of risk behaviour using a network approach. Her current work focuses on evaluating board decision-making and board engagement pertaining to cybersecurity.

**Madeline Carr** is the Director of RISCS and the Principal Investigator of the Cyber Readiness for Board Project. She is a Professor of Global Politics and Cyber Security at UCL's Science, Technology, Engineering and Public Policy.

(CISO) / chief information officer (CIO) meet the board. Technological solutions are an important element of any organisation's approach to cyber resilience, but equally important are those human and organisational factors that are at the heart of business processes and these are much more difficult to quantify for insurance purposes.

The cyber insurance market is predicted to grow to $20bn by 2025 (Allianz, 2015). Amidst the ongoing development of cyber insurance, some of the challenges around cyber risk that the market faces today include a lack of experience with cyber incidents, confusion around premiums, accumulated risk, missing metrics, and weak governance.

- **Lack of experience with cyber incidents.** Due to a lack of first-hand experience, and despite the proliferation of cyber capabilities, many organisations underestimate or straight up ignore cyber risk (Jalali, 2019). A 2019 study on the private sector found that experiencing a cyber incident is the main trigger for increases in cyber risk management investments (Marsh and Microsoft, 2019). Another study demonstrates that firms that have experienced a cyber attack – like AP Moller-Maersk – are the most likely to purchase insurance (Shackelford, 2012). Even if the decision to purchase cyber insurance is taken, a considerable proportion of traditional policies do not affirmatively include or exclude cyber coverage (Woods and Moore, 2019). The resulting ambiguity is known as "silent cyber" (Woods and Simpson , 2017). The industry is currently working to remove this ambiguity to avoid confusion around premiums.
- **Confusion around premiums.** A key question is how to set premiums for the development of a mature cyber insurance market. Setting premiums is particularly challenging for cyber risk, due to limited information sharing with respect to cyber incidents, leading to a lack of actuarial data from past events and a lack of normative standards (Toregas, 2014). There is a tendency for firms to under-report information about breaches or cyber incidents to avoid negatively impacting consumer trust, corporate reputation, and market confidence. This is, however, a missing link in measuring potential damage and impact associated with cyber incidents for the purpose of insuring them. Despite this challenge, the income from the cyber risk insurance premium is estimated to be over $8bn in 2020 (de Azevedo, 2020).
- **Accumulated risk.** Many developments including the Internet of Things have led to increased connectedness, where risks are cascaded (Tanczer, 2018). Similarly, interconnectedness threatens cyber supply chains, where software and hardware components are vulnerable. It is difficult to accurately model risk accumulation given the complexity of corporate footprints, identifying all dependencies among risks, and assessing the severity of the impact of cascading risks on the organisation. In case of cyber risks, the probability of one risk triggering several policies resulting in larger total claims is high. The geographic boundaries for cyber are

not well-defined and this is exacerbated by organisations using external services, such as cloud services, which lead to risk accumulation. Smaller events could reverberate throughout the organisation as a consequence of processes and systems being hyperconnected. Accumulation also occurs as a result of reputational damage, regulatory ramifications or through other costs (Cyber insurance accumulation risk, 2016).

- **Threat metrics and coverage types**. The cyber risk threat landscape is ever-changing and this means businesses can struggle to understand the digital protection they require. Insurance coverage falls under three categories. First party coverage includes direct losses the insured would incur and comprise costs associated with cybersecurity events being mitigated. Third party loss coverage is to indemnify the liability of the company for losses to others and can include wrongful collection of information, media liability, data protection and cyber liability or violation of notification obligations. Finally, other benefits can be covered relating to assorted services and costs such as communication following damage to reputation, or first response costs such as forensic investigation costs. The cyber risk and insurance forum (CRIF) matrix shows that the threats and impact associated differ across industries. While there are industry-specific cyber coverage policies, these are not harmonised which makes it confusing for buyers (ENISA, 2017). This is further complicated because insurers often exclude types of losses or causes of incidents.
- **Governance Challenges.** Some believe that a well-defined regulatory landscape can drive convergence of cyber insurance and possibly lead to higher demand for cyber insurance (de Azevedo, 2020). In the EU, such regulation includes fines and sanctions for firms that do not disclose cyber incidents or implement adequate measures to prevent system breaches. Over time, this will inform corporate security practice and has already worked to help boards quantify cybersecurity investment against possible fines. Government regulation today, however, remains fragmented and sometimes contradictory as do taxonomies and definitions of standard terms and conditions for cyber insurance. On the flip side, the anticipated rise of the Internet of Things suggests that the insurance sector can benefit from the volume of data generated by new devices. It may use that to develop techniques to address new dynamic and accurately priced insurance demands (Tanczer et al., 2018). In this sense, the insurance sector may have a quasi-governance role to play in incentivizing cybersecurity practices.

> **The cyber insurance market is evolving and there is a mutual effect at play.** On one hand, cyber insurance needs to develop in sophistication in order to be seen as a mechanism for cyber risk mitigation. At the same time, the data generated by the IoT will impact the entire insurance value chain and enable the insurance sector to support business decision-making and to improve pricing and capital calculation (Tanczer et al., 2018).

What remains to be seen is how quickly cyber insurance will evolve to a point that it can help businesses cope with extraordinary circumstances like a global pandemic.

Published as part of the *Cyber Readiness for Boards* project

## References (APA)


Allianz, (2015). *A Guide to Cyber Risk Managing the Impact of Increasing Interconnectivity, Global Corporate & Specialty, 2015.* URL: https://www.agcs.allianz.com/news-and-insights/reports/a-guide-to-cyber-risk.html

Cyber insurance accumulation risk (2016). *Cambridge centre for risk studies.* URL: https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/cyber-risk-outlook/managing-cyber-insurance-accumulation-risk-2016/

de Azevedi, C (2020). *Cyber Insurance: The latest trends.* URL: https://www.penningtonslaw.com/news-publications/latest-news/2019/cyber-risks-insurance-the-latest-trends

ENISA (2017). *Commonality of risk assessment language in cyber insurance.* Recommendations on Cyber insurance. URL: https://www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance

ICO (2020). *COVID-19 Cyber threats.* URL: https://www.whatdotheyknow.com/request/667849/response/1591987/attach/html/2/Response.pdf.html

Jalali, M. S., Siegel, M., & Madnick, S. (2019). *Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment.* The Journal of Strategic Information Systems, 28(1), 66-82. URL: https://www.sciencedirect.com/science/article/pii/S0963868717304353

Marsh (2019). *Covid-19 Next steps for cyber insurance.* URL: https://www.marsh.com/qa/en/insights/research-briefings/covid-19-next-steps-for-cyber-insurance.html

Marsh and Microsoft (2019). *Global Cyber Risk Perception Survey.* URL: https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

National Cyber Security Centre (2020). *Is cyber insurance right for you?* URL: https://www.ncsc.gov.uk/blog-post/is-cyber-insurance-right-for-you

Shackelford, S. J. (2012). *Should your firm invest in cyber risk insurance?*. Business Horizons, 55(4), 349-356. URL: https://www.sciencedirect.com/science/article/pii/S0007681312000377

Tanczer, L., Steenmans, I., Brass, I., & Carr, M. M. (2018). *Networked world: Risks and opportunities in the Internet of Things*. URL: https://discovery.ucl.ac.uk/id/eprint/10063068/

Toregas, C., & Zahn, N. (2014). *Insurance for cyber attacks: The issue of setting premiums in context. George Washington University.* URL: https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/cyberinsurance_paper_pdf_0.pdf

Woods, D. W., & Moore, T. (2019). *Does insurance have a future in governing cybersecurity?*. IEEE Security & Privacy, 18(1), 21-27. URL: https://ieeexplore.ieee.org/abstract/document/8833500

Woods, D., & Simpson, A. (2017). *Policy measures and cyber insurance: A framework.* Journal of Cyber Policy, 2(2), 209-226. URL: https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1360927