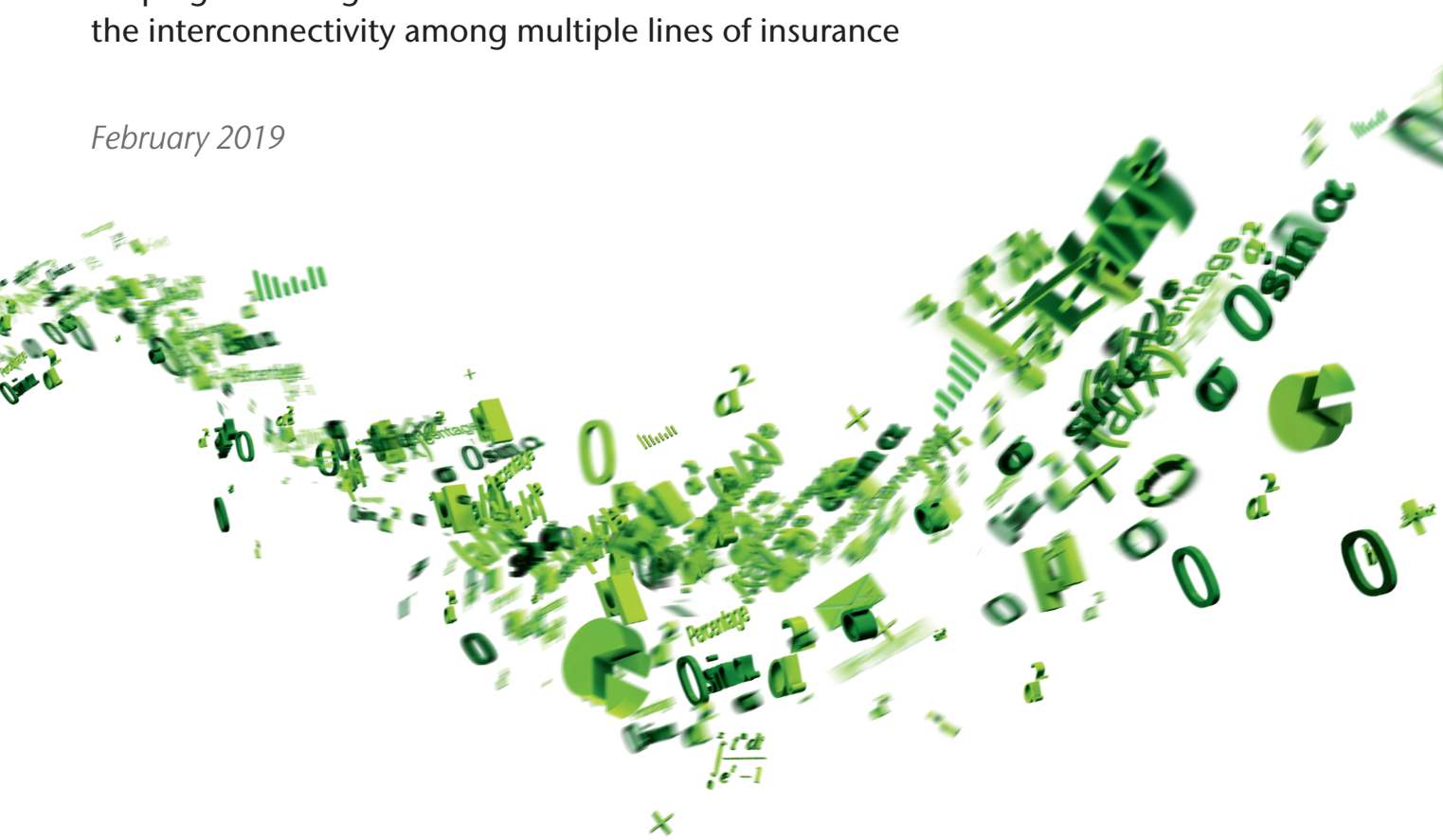
Cyber Perils in a Growing Market

Helping EMEA organisations better understand the interconnectivity among multiple lines of insurance

February 2019



AON
Empower Results®

Table of Contents

Daily news reports disclose the latest technology developments and related cyber perils. The risk industry has to keep up with a constantly evolving environment in an everyday battle for relevance. The cyber insurance market in Europe is growing to meet this demand. However, there are lessons to be learned from the maturity of the US market.

1. Progress, but just scratching the surface

Insurance, including any form of cyber insurance, should be complementary to a robust cyber resiliency risk management approach.

Linking asset and risk data analytics will lower an organisation's Total Cost of Risk (TCoR is the sum of an organisation's risk mitigation costs, insurance premium costs, retained losses <deductibles/ uninsured losses> and value degradation).[1] Each organisation should identify and protect its critical intangible assets by aligning cyber enterprise risk management strategy with corporate culture and risk tolerance, protecting against unbudgeted loss and balance sheet volatility. Despite growing challenges along the way [2], standalone cyber insurance has, or could have, responded to the majority of Personally Identifiable Information (PII), Payment Card Industry (PCI) and Personal Health Information (PHI) type privacy and security incidents listed in Table 1 below.[3]

Table 1 – Notable Data Breach / Privacy Commercial Impacts (Publicly available information as of February 7, 2019)

Organisation	Commercial Impact	Financial Components	Source
Anthem	$278 million	Gross Expenses ($148 million) Security Improvements ($115 million) HIPAA Settlement ($16 million)	Regulator Settlement U.S. District Court HHS OCR
Equifax	$430.5 million $514 million £500,000	Gross Expenses to Date Total Estimated Gross Expenses ICO Fine (DPA 1998)	Q3 2018 Earnings Release Q3 2018 Financials ICO Notice
Facebook	£500,000	ICO Fine (DPA 1998)	ICO Notice
The Home Depot	$298 million	Gross Expenses	10-K Filing 2017
Target Corporation	$292 million	Gross Expenses	10-K Filing 2017
Uber	$148 million €400,000 €600,000 £385,000	U.S. Attorney General Settlement French CNIL Fine Dutch DPA Fine ICO Fine (DPA 1998)	U.S. AG Settlement CNIL Notice Dutch DPA Notice ICO Notice
Yahoo! Inc. (Altaba Inc.)	$350 million $85 million $35 million $80 million $29 million £250,000	Reduced Acquisition Price Customer Class Action SEC Fine Securities Class Action Shareholder Derivative ICO Fine (DPA 1998)	Verizon Press Release U.S. District Court SEC Press Release U.S. District Court U.S. District Court ICO Notice

[1] *Analytics have the potential to streamline cyber insurance similar to how FICO credit scores facilitate individual risk management – at least with respect to PII/ PHI cyber incidents. Applying scores to cyber insurance underwriting: https://www.propertycasualty360.com/2018/08/29/applying-scores-to-cyber-insurance-underwriting/*

[2] *Several cyber insurance coverage claims have been denied due to lack of a common understanding of the coverage between the insurer and the insured and/or inadequate policy wording customisation: Columbia Cas. co. v. Cottage Health Sys., C.D. Cal. No. CV 15-03432 DDP (AGRx) (filed May 7, 2015) (CNA NetProtect360 policy coverage denied by CNA due to failure of insured to meet minimum required practices, misrepresentation in the application, and other defects; declination overturned after CNA lost a decision with respect to enforceability of the ADR clause); Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., No. 2:2014cv00170—Document 45 (D. Utah 2015) (CyberFirst policy coverage denied by Travelers due to alleged intentional excluded act of withholding distribution of information by insured; denial upheld); P.F. Chang's China Bistro, Inc. v. Fed. Ins. co., 2016 U.S. Dist. LEXIS 70749 (D. Ariz. May 26, 2016) (May 2016) (coverage denied by Chubb for Payment Card Industry Fines & Penalties, which would seem to be the main cyber related vulnerability and damages that should be addressed for a restaurant that accepts payments via credit cards); New Hotel Monteleone, LLC v. Certain Underwriters at Lloyd's of London, Subscribing to Ascent Cyberpro Policy No. ASC14C00944, No. 2:16-CV-00061-1LRL-JCW (E.D. La. filed Jan. 5, 2016 (New Hotel Monteleone made claim against its insurer alleging lack of adequate limits for Payment Card Industry fines (insurer denied claim).*

[3] *Note that:*
A. Most third party liability costs, defense and indemnity from PII/PHI related cyber incidents can be addressed by some form of professional liability/technology errors & omissions or media liability insurance, as will be discussed hereinbelow; and
B. Not all of the organisations cited in Table 1 had purchased adequate cyber or professional liability insurance prior to the incidents disclosed but coverage was available to address the documented losses.

Any industry could suffer a data breach, but non-PII centric organisations typically do not possess as many personally identifiable records as PII centric organisations and the potential severity loss of PII records is lower than other potential severity losses, such as business interruption.

For example, most of the standalone cyber insurance success stories of US insureds, in which cyber insurance was purchased and the insurance carrier paid a claim, are comprised in four industries:

- ***Retail*** (5.9% value added by industry as a % of GDP as of July 20, 2018)
- ***Hospitality*** (3% value added by industry as a % of GDP as of July 20, 2018)
- ***Healthcare*** (7.3% value added by industry as a % of GDP as of July 20, 2018)
- ***Financial Institutions*** (7.5% value added by industry as a % of GDP as of July 20, 2018)

The percentage of the total US Gross Domestic Product of these four industries is approximately 23.7%.[4] However, standalone cyber insurance has had a growing adoption in the majority of the industries that comprise the remaining 76.3% of GDP, such as:

- ***Utilities*** [5]
- ***Construction***
- ***Manufacturing***
- ***Agriculture, forestry, fishing and hunting***
- ***Information***
- ***Professional and Business Services*** [6]
- ***Real Estate and rental and leasing***
- ***Arts, entertainment and recreation***
- ***Government***
- ***Educational Services***
- ***Transportation and warehousing***

Furthermore, standalone cyber insurance was initially developed to address a subset of privacy and security costs as they relate to the breach of Personally Identifiable Information (PII), and generally not intended to cover malicious funds transfers, crypto losses, bodily injury or tangible property damage type losses. The notable exceptions being some innovative cyber insurance programmes built for automobile and steel manufacturers, among others.[7] Nowadays Business Interruption (BI), due to cyber events, is a more common concern for organisations, although sometimes with sub-limits or restrictive/ exclusions with respect to dependent business interruption.

[4] *U.S. Department of Commerce, Bureau of Economic Analysis (www.bea.gov).*

[5] *Replication of cyber attacks on energy sector a threat to renewables, https://www.pv-tech.org/news/replication-of-cyber-attacks-on-energy-sector-a-threat-to-renewables*

[6] *The vast majority of professional and business services organisations, such as consulting, technology, legal, accounting, communications, information and media companies, address their third party cyber exposures via their professional liability, technology errors & omissions or media insurance policies. Over 90% of the large professional liability insurance severity case losses are due to non-cyber alleged errors, omissions and negligent acts (the Yahoo!, Equifax and Heartland cases are exceptions). For example, in Shaw v. Toshiba America Information Systems, Inc., 91 F. Supp. 2d 942 (E.D. Tex. 2000), the court approved $2.1 billion ($2,100,000,000.00) Settlement Agreement along with attorneys' fees in the amount of $147.5 million ($147,500,000.00) in a professional liability/errors & omissions case. However, there may be significant gaps and limitations in professional liability policies that could be addressed in a robust cyber insurance policy.*

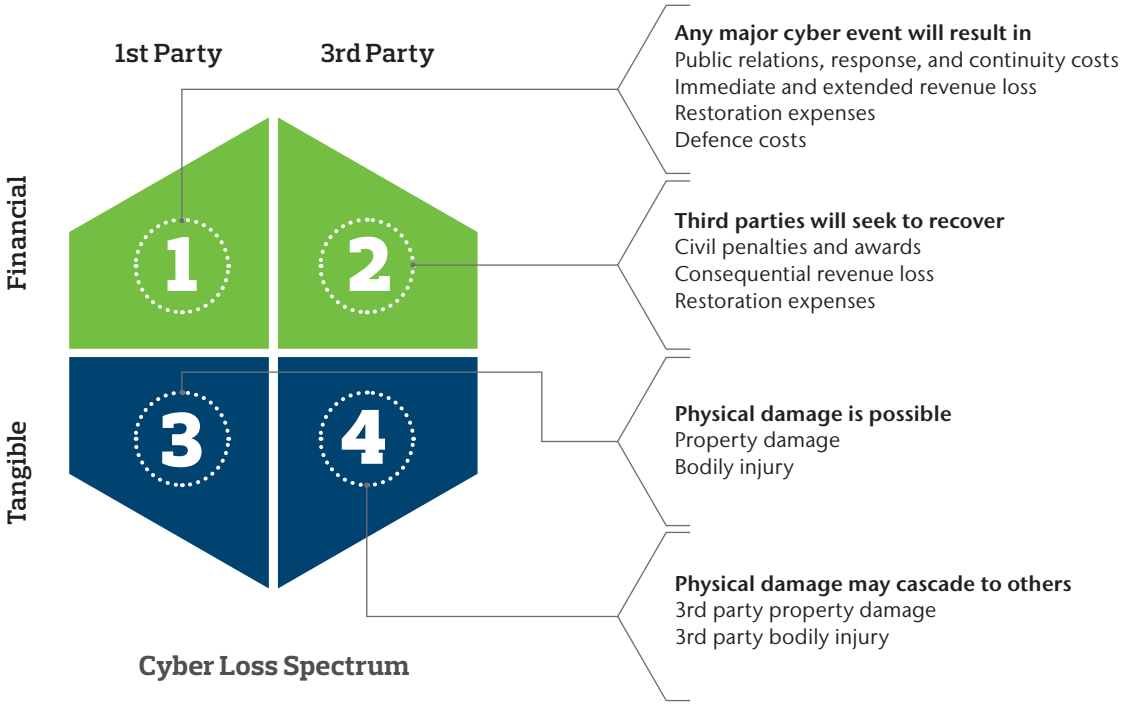
A professional liability trigger is generally an alleged error, omission, or negligent act (e.g., a demand against the insured based on the allegations) whereas a robust cyber insurance policy can be triggered by the cyber incident prior to a third party demand to help the insured respond and avoid a third party claim or limit its magnitude.

Professional liability policies are not intended to address first party business interruption or extra expense costs to the insured due to cyber incidents that knock out or cause degradation to the computer system of the insured, whereas cyber policies can have specific affirmative coverage grants for such perils and damages.

[7] *Aon debuts industry first cyber solution: https://ir.aon.com/about-aon/investor-relations/investor-news/news-release-details/2016/Amid-evolving-cyber-risks-Aon-introduces-first-of-its-kind-enterprise-wide-cyber-solution-for-all-industries/default.aspx*

Cyber exposures related to Personally Identifiable Information (PII) generally result in non-tangible damages (i.e. purely economic or financial type losses). However, cyber exposures could end up with bodily injury and tangible property damages.

Organisations must identify cyber perils and model potential cyber related losses based upon their unique set of business operations. This should incorporate an enterprise wide approach to understanding mission critical assets and the potential relevant attack paths that could result in a material incident. The cyber loss spectrum is not identical for each organisation. Therefore, the analysis of which lines of insurance could cover a cyber loss is not identical for each organisation.



Organisations of all sizes, geographies and industries are increasing their reliance on data analytics and technology [8], such as cloud computing [9], artificial intelligence [10], 5G , Internet of Things [11], mobile devices, automated supply chains [12] and distributed ledger/blockchain.[13] Each of these advancements adds new and different cyber exposures.[14]

For example, almost every large organisation, and most middle-size organisations, will have some reliance/dependency on distributed ledger technology within the next few years – either directly or via one of their third party suppliers, distributors, vendors, partners or customers.[15] Insurance carriers are just starting to consider the coverage grants and exclusions required to properly address such distributed ledger exposures.

[8] *Dollars From Data: The Value of Emerging Tech, http://theonebrief.com/dollars-from-data-the-value-of-emerging-tech/*

[9] *An August 2018 Gartner survey states that cloud computing remains the top emerging risk. Gartner Risk Management Leadership Council Top 10 Emerging Risks of Q2 2018.*

[10] *5G Wireless Technology Raises Security Fears, Wall Street Journal, September 12, 2018. Cyber security attacks could accelerate with 5G technology, which will connect far more devices than today's networks.*

[11] *With the proliferation of IoT devices in the enterprise, managing third party risks to sensitive and confidential data has become a herculean task. Companies are deeply concerned that failure to prevent a cyber attack could have catastrophic consequences. The Second Annual Study on the Internet of Things (IoT): A New Era of Third-Party Risk. March 2018.*

[12] *Supply chain-related cyber attacks rise 200%: Report, https://www.businessinsurance.com/article/20180917/STORY/912324028/Supply-chain-related-cyber-attacks-rise-200-Report*

[13] *Insuring the Blockchain. September 17, 2018.*

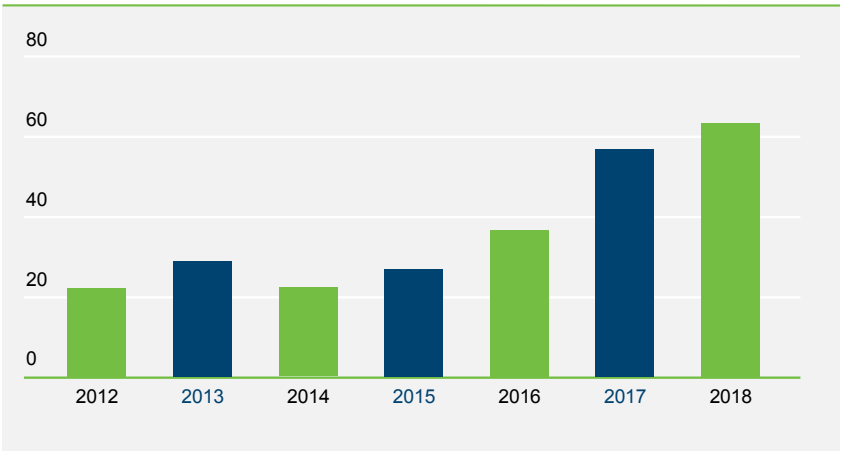
[14] *Some of the new and different cyber exposures can improve risk mitigation and lower the Total Cost of Risk. If XYZ widget manufacturing company outsources a portion of its IT system to a top cloud provider, such as IBM, Microsoft or Alphabet, security would theoretically improve because the cloud provider can spend 24/7/365 attention on security issues, compared to if XYZ widget manufacture tried to figure out and keep up with all IT security issues on its own.*

[15] *Three fourths of business leaders see 'compelling' case for blockchain: https://www.medtechdive.com/news/three-fourths-of-business-leaders-see-compelling-case-for-blockchain/530902/*

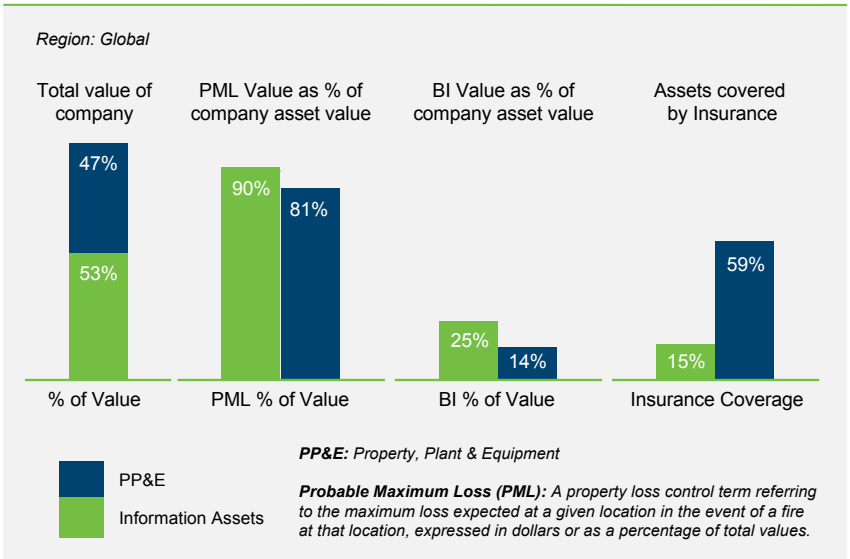
2. Increasing recognition of the financial statement impact

According to the Risk and Insurance Management Society, organisations' Total Cost of Risk declined for the fourth year in a row in 2017, but cyber costs moved in the opposite direction, rising 33%.[16]

The number of cyber incidents with losses of more than $1 million: [17]



Most boards of directors and management now include cyber perils and solutions in corporate governance discussions as they learn more regarding the potential financial statement impact of high profile cyber incidents.[18] Yet, many organisations still only insure a relatively small portion of their intangible assets compared to insurance coverage for legacy tangible assets.[19]



[16] *Cyber Risk Costs Resist Overall Trend.*

[17] *Center for Strategic and International Studies. https://www.csis.org/*

[18] *"Is cyber risk a D&O risk?" https://ethicalboardroom.com/is-cyber-risk-a-do-risk/*

[19] *2017 Aon Sponsored Ponemon Institute Global and Cyber Risk Transfer Study and Comparison Reports: Information Assets vs. Property, Plant & Equipment Risk Summary. http://www.aon.com/forms/2017/2017-global-cyber-risk-transfer-comparison-report.jsp https://www.aon.com/risk-services/2017-EMEA-Cyber-Risk-Transfer-Comparison-Report.jsp*

According to a recent article in **The Economist:** ***"Companies' value lies mainly in assets that are tricky to insure,"*** [20] organisations claim to recognise that the value of their intangible assets materially exceeds the value of their tangible assets.[21] Yet, the same organisations often do not allocate resources accordingly to protect and maximise the value of the intangible assets. For instance, most organisations are unaware that patent infringement and trade secrets insurance coverage is available to supplement readily available insurance coverage to address copyright, trademark, service mark and other intellectual property exposures.

The 2017 devastating NotPetya incident [22] has taught us that even if business interruption coverage is included in a standalone cyber insurance programme, the limits available in the commercial marketplace would cover just a fraction of the potential catastrophic business interruption and related first party losses as set forth in Table 2 below. Available business interruption insurance capacity is much less under cyber policies ($100 - $500 million) than under property policies (potentially, $1 to $2 billion+). In addition, prudent insurance companies are adding "tie-in" limits and "aggregate loss" limits endorsements to both their property and cyber insurance policies to avoid the situation of "double paying" on a cyber business interruption loss for what is known as a "clash" event in insurance terms (i.e. two different insurance policies must pay for the same incident). Therefore, similar analysis may apply with respect to potential "clash" triggers between general liability and cyber/professional liability insurance policies regarding cyber perils that result in bodily injury and/or tangible property damage (as well as crime, marine, aviation, environmental, kidnap and ransom [23], product recall, Directors & Officers, and terrorism insurance). Keep in mind that the trend is for non-cyber policies to add specific exclusions to eliminate the so-called "silent cyber" exposures. "Silent cyber" exposure occurs when a non-cyber policy may intentionally, or unintentionally, omit cyber coverage exclusions.

Table 2. Notable NotPetya Business Interruption Commercial Impacts (Publicly available information as of February 7, 2019)

Organisation	Commercial Impact	Financial Components	Source
A.P. Moller – Maersk	$250-300 million	Earnings Reduction	Q4 2017 Financials
Beiersdorf AG	Minimal sales impact €15 million	€35 million sales shifted Q2 to Q3 Additional expenses	Q2 2017 Financials Q4 2017 Earnings Call
FedEx (TNT Express)	$400 million	Earnings Reduction	Q4 2018 Financials
Merck & Co.	$410 million $380 million	2017, 2018 Sales Reduction Additional Expenses	Q4 2017 Financials Q3 2018 Financials
Mondelez International	~$104 million $84 million	2017 Sales Reduction Additional Expenses	Q4 2017 Earnings Call Q4 2017 Earnings Release
Nuance Communications	$68 million $31.2 million	2017 Sales Reduction Additional Expenses	Q3 2018 Financials
Reckitt Benckiser	~£114 million	2% Q2 Sales Reduction 2% Q3 Sales Reduction	Press Release Q2 2017 Financials Q3 2017 Financials
Saint-Gobain	~€220-250 million €80 million	2017 Sales Reduction 2017 Earnings Reduction	Q3 2017 Earnings Release Q1 2018 Earnings Release

[20] *"The business of insuring intangible risks is still in its infancy." The Economist. August 23, 2018. https://www.economist.com/finance-and-economics/2018/08/25/the-business-of-insuring-intangible-risks-is-still-in-its-infancy*

[21] *"We ignore the risks that are hardest to measure, even when they pose the greatest threats to our well-being." Nate Silver, The Signal and the Noise : Why So many Predictions Fail – but Some Don't.*

[22] *Petya and NotPetya are two related pieces of malware that affected thousands of computers worldwide in 2016 and 2017. Both Petya and NotPetya aim to encrypt the hard drive of infected computers, and there are enough common features between the two that NotPetya was originally seen as just a variation on a theme. In June of 2017 a new version of the malware began spreading rapidly, with infection sites focused in Ukraine, but it also appearing across Europe and beyond. The new variant spread rapidly from computer to computer and network to network without requiring spam emails or social engineering to gain administrative access.*

[23] *The True Cost of a ransomware attack, https://www.insurancebusinessmag.com/us/news/cyber/the-true-cost-of-a-ransomware-attack-109442.aspx*

Furthermore, aggregated/correlated/systemic cyber exposures have the potential to cause damages that could add up to monetary amounts that are multiples of any loss seen to date.[24] One recent study estimates that an extreme cyber attack could cost as much as Superstorm Sandy, or in excess of $53 billion.[25] A U.S. cloud computing cyber incident could spur up to $19 billion in losses.[26] However, the insurance industry is just commencing catastrophe modeling for aggregated/correlated/systemic risk with respect to cyber perils.[27] Innovative approaches for assisting insurers concerned about aggregated, "clash" and "silent cyber" exposures are starting to emerge.[28]

In **Lights Out:** ***"A Cyber Attack, A Nation Unprepared, Surviving the Aftermath,"*** [29] author Ted Koppel suggests that a catastrophic cyber attack on America's power grid is likely and that we are unprepared. A 2015 Lloyd's of London/University of Cambridge report, Business Blackout, sets forth the insurance implications of a cyber attack on the U.S. power grid. The report estimated a hypothetical worst case scenario of $243 billion to $1,024 trillion in direct and indirect losses, with between $21.398 billion and $71.109 billion in estimated insurance industry losses.

S&P Global Ratings issued a report August 22, 2018 that stated cyber attacks heighten credit risks in the U.S. public sector.[30] While S&P has not yet downgraded a municipal issuer because of a cyber incident, repeated successful attacks may reduce credit rating over time by eroding public trust, according to the report. That would potentially make it harder for municipal issuers to increase tax rates and take other measures needing public support.[31]

[24] *Revealed: the cyber Achilles heel for huge companies, https://www.insurancebusinessmag.com/us/news/cyber/revealed-the-cyber-achilles-heel-for-huge-companies-109864.aspx*

[25] *Counting the Cost: Cyber exposure decoded.*

[26] *Cloud Down - The impacts on the US economy.*

[27] *Rethinking Systemic Cyber Risk – An Approach for Growth.*

[28] *Managing Silent Cyber, http://www.aon.com/getmedia/2b1ad492-dcf0-429e-9eda-828d49b1396a/aon-silent-cyber-solution-for-insurers.aspx*

[29] *http://tedkoppellightsout.com/*

[30] *www.standardandpoors.com*

[31] *Moody's issued similar warnings that cyber risks could impact credit ratings and that cyber perils and risk management will be higher priorities in its analysis of the creditworthiness of companies across all sectors, including healthcare and financial services (www.moodys.com).*

3. Intended scope of standalone cyber and professional liability insurance base policies are not "be all and end all" insurance solutions: potential gaps must be understood

Most non-PII/PHI catastrophic cyber perils are not intended to be covered by existing standalone base cyber policies.

Cyber insurance and professional liability policies are generally "named perils" policies as opposed to "all risk" policies, which means the policy wording scope and limitations is crucial to coverage. In addition to the business interruption capacity limitations referenced above, consider several recent cyber incidents, which evidence that current standalone cyber insurance programmes are generally not intended to address some cyber peril catastrophic losses.

- ***August 11, 2018:*** ATM hackers stole £10 million ($13.5 million) across 28 countries in Cosmos Bank robbery, which involved 14,800 ATM transactions.[32]
- ***August 15, 2018:*** Crypto investor sues AT & T for $224 million, claiming AT & T should be held liable for fraudsters who hijacked mobile phone numbers to steal approximately $24 million worth of cryptocurrency due to employee negligence in allowing "SIM swaps." The suit also seeks $200 million in punitive damages.

Typical standalone cyber insurance policies specifically EXCLUDE funds transfers, crypto transfers and other cash and securities monetary losses.[33] Crime policies are intended to address fund losses under specified circumstances. Similarly, payment diversion fraud coverage for "spoofing," "phishing," and other social engineering incidents is generally excluded under cyber policies, but possibly covered under crime policies. Two Federal Appellate Courts recently ruled that policyholders are entitled to crime insurance coverage for losses arising from social engineering schemes.[34]

- ***July 2018:*** Facebook investors filed two different securities lawsuits: (1) the first based on the Cambridge Analytica user data debacle; and (2) the second following Facebook's disappointing quarterly earnings release due to lower growth rate caused in part by allegedly unanticipated expenses and difficulties in complying with the European Union General Data Protection Regulation (GDPR).
- ***August 8, 2018:*** Securities class action litigation against a publicly reporting media performance ratings company disclosed in its quarterly earnings release that GDPR-related changes affected the company's growth rate, pressured the company's partners and clients, and disrupted the company's advertising "ecosystem."

[32] *One day earlier, August 10, 2018, the FBI warned that cyber criminals could be planning a highly-coordinated attack on cash machines: "The FBI has obtained unspecified reporting indicating cyber criminals are planning to conduct a global Automated Teller Machine (ATM) cash-out scheme in the coming days, likely associated with an unknown card issuer breach and commonly referred to as an 'unlimited operation'." A similar attack on the National Bank of Blacksburg resulted in losses of $2.4 million in 2016.*

[33] *Sub-limited coverage may be available in Canada under cyber policies.*

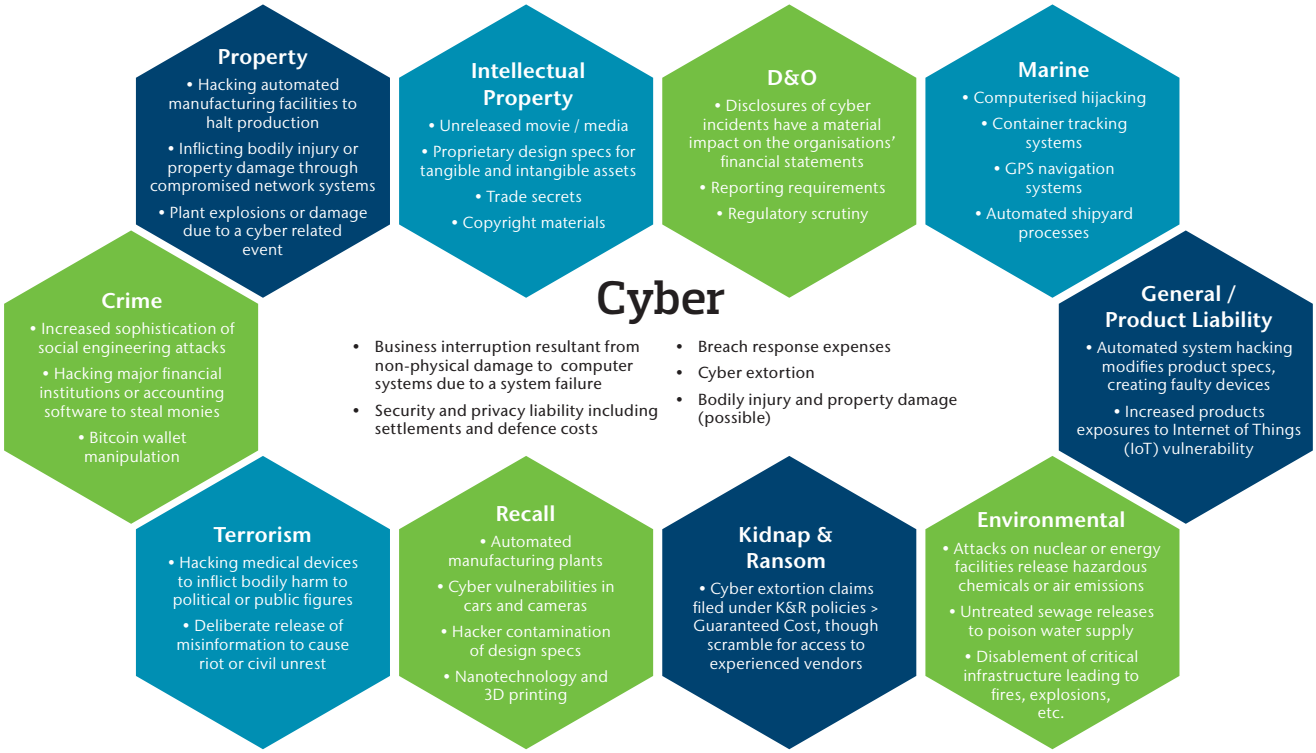
[34] *In American Tooling Center, Inc. v. Travelers Casualty and Surety Company of America, No. 17-2014, 2018 WL 3404708 (Sixth Circuit July 13, 2018), the Sixth Circuit held that Travelers was obligated to provide coverage for a loss the insured suffered when it wired $834,000 to a thief's bank account, believing that it was transmitting a payment to one of its Chinese subcontractors. This decision follows on the heels of a July 6 decision in which the Second Circuit also ruled in favor of a policyholder in a phishing coverage dispute – Medidata Sols. Inc. v. Fed. Ins. Co., No. 17-2492, 2018 WL 3339245, (2d Cir. July 6, 2018). August 2018, The Second Circuit rejected Chubb subsidiary Federal Ins. Co.'s request for reconsideration of the court's July 6, 2018 decision, confirming that the insurer must cover Medidata's $4.8 million loss under its computer fraud insurance policy.*

Typical professional liability and cyber policies specifically EXCLUDE shareholder derivative securities and similar fiduciary liability litigation, as with the three cases described above. A well crafted Directors & Officers insurance policy is necessary to provide defense and indemnity coverage for such claims. Next, consider the transformation of our buildings, roads and public transport systems. Internet connectivity, coupled with the ever advancing ability to gather and analyse data, is finding its way into the construction and transportation industries. As a result, we will live and work in structures that are "aware" and travel in cities that are "smart." [35]

- A Global Positioning System for cars, trains, trucks, ships, explorers, etc. suffers a directed attack which disables the GPS, either maliciously redirecting or leaving the users without navigation.[36]
- A healthcare facility sustains a cyber intrusion that modifies patient records and/or intrudes medical equipment resulting in improper treatment or patient monitoring. In both cases, such intrusions can result in harm to patients.[37]
- A manufacturing plant sustains an intrusion that interrupts an assembly line causing it to speed up resulting in both property damage and employee injuries.[38]
- 2018 Department of Homeland Security alert: Russian government cyber actors targeted government entities and multiple U.S. critical infrastructure sectors, including energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors.[39]

Absent extensive policy wording customisation, the typical cyber insurance policy specifically excludes all bodily injuries (with the exception of emotional distress and mental anguish only) and tangible property damage – both first party tangible property damage (own property of the insured) and third party tangible property damage (property owned by other than the insured).

"Potential Cyber Perils"



Note that coverage in policy forms can vary materially from carrier to carrier, and base forms to manuscript policy forms.

[35] *http://theonebrief.com/from-blueprint-to-open-for-business-how-infratech-has-become-a-key-building-material/*

[36] *When cyber risks become physical, https://www.corporateriskandinsurance.com/news/cyber/when-cyber-risks-become-physical/110209*

[37] *Firms Lack Cyber Insurance Despite Healthcare Data Breach Costs, https://healthitsecurity.com/news/firms-lack-cyber-insurance-despite-healthcare-data-breach-costs*

[38] *Cyber attacks cost German industry €43 billion, https://www.businessinsurance.com/article/20180913/NEWS06/912323988/Cyber-attacks-cost-German-industry-almost-$50-billion-IT-sector-association-stud*

[39] *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.*

Purchasing insurance for third party bodily injury and third party property damage claims is the intent of a commercial general liability policy.

Challenge # 1:

Cyber liability exclusions contained within general liability policies (i.e. peril/trigger must be a "tangible" peril).[40] The de facto CL 380 exclusion sets forth: [41]

In no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.

Challenge # 2:

Many companies today provide some degree of professional services, and most general liability policies exclude coverage for claims arising from "professional services". A typical exclusion might read:

This insurance does not apply to any "bodily injury", "property damage", "personal and advertising injury", arising out of the rendering of, or failure to render professional services.

The intent behind this exclusion is to push professional exposures to professional liability policies. It seems straightforward enough until you realise that almost all cyber and professional liability policies contain exclusions for bodily injury and property damage (BI/PD) claims, with the intent of pushing those exposures to general liability policies. This exclusion generally reads:

The insurer shall not be liable to make any payment for loss in connection with any claim for bodily injury, sickness, death, emotional distress, mental anguish, or for damage to, destruction of, or loss of use of any tangible property.

This creates a significant gap where bodily injury/property damage claims arising from professional services are left in limbo (and uncovered) by both policies. The same holds true for cyber policies that also contain hard bodily injury/property damage exclusions. When cyber breaches affect engineering or load bearing calculations, monitoring of infrastructure related software, interference with GPS coordinates (among others), and ultimately result in bodily injury or property damage claims, coverage may be declined entirely. Therefore, the collaboration of various policies is necessary to adequately address cyber perils. Even so, it is important to understand the existing boundaries of insurable exposures, not every cyber peril is currently insurable.

[40] *Comprehensive General Liability policies may contain carve backs for bodily injury in some cases.*

[41] *The Cyber Attack Exclusion Clause - CL.380 - is incorporated into many general liability insurance and property insurance contracts and is currently accepted as the market clause for this issue.*

Industry	Key Risk 1	Key Risk 2	Key Risk 3	Key Risk 4	Key Risk 5	Key Risk 6	Key Risk 7	Key Risk 8	Key Risk 9	Key Risk 10
Construction										
Education										
Energy										
Entertainment										
FAB										
Financial Institutions										
Healthcare										
Industrial & Materials										
Life Sciences										
Power										
PSG										
Public Sector										
Real Estate										
Retail & Wholesale Trade										
Technology										
Transportation & Logistics										

Uninsurable

- Economic slowdown/ slow recovery
- Commodity price risk
- Regulatory/legislative changes
- Increasing competition
- Failure to innovate/ meet customer needs
- Major project failure
- Failure to attract or retain top talent
- Distruptive technologies/innovation
- Exchange rate fluctuation
- Growing burden and consequences of corporate governance/compliance
- Workforce shortage

Partly Insurable

- Cyber crime/hacking/viruses/ malicious codes
- Damage to reputation/brand
- Political risk/uncertainties
- Cash flow/liquidity risk
- Distribution of supply chain failure
- Loss of intellectual property/data
- Capital availability/credit risk
- Merger/acquisition/restructuring
- Technology failure/system failure

Insurable

- Property damage
- Business interruption
- Environmental risk
- Weather/natural disasters
- Third party liability (Incl. E&O)
- Directors & Officers personal liability
- Product recall
- Injury to workers

4. ''Silent'' and affirmative cyber coverage under other lines of insurance

"Silent cyber" refers to the cyber exposure lying in policies which do not specify whether losses arising from a cyber attack are affirmatively covered. Absent specific cyber coverage grants or exclusions, insurers either (a) intentionally provide non-affirmative cyber coverage; or (b) unintentionally provide non-affirmative coverage due to the lack of specific exclusions. In other words, silent cyber strikes when a court's findings are in favor of a policy owner because the policy does not clearly grant or exclude cyber coverage. When cyber exposure losses first emerged, insurers had not priced cyber risks into their broadly worded legacy policies, such as property and general liability. Once the risk was realised, some insurers either excluded or sub-limited the risk from new standard policies and renewals. However, affirmatively granting full cyber limits coverage for an additional premium in legacy policies, although rare, is growing fast.[42] For instance, it was not until December 2016 that the U.S. Treasury Department confirmed that standalone cyber liability insurance policies are classified as "cyber liability" (rather than excluded professional errors and omissions liability) for state regulatory purposes and thus, are included in the Terrorism Risk Insurance Programme.[43]

As set forth in the scenarios and case citation above, insurance coverage for cyber perils can be found under other non-cyber specific lines of insurance, such as crime (i.e. funds transfers/social engineering, etc.), general liability (i.e. third party tangible property damage and bodily injury) and kidnap and ransom (i.e. cyber extortion related to ransomware). Such data becomes more significant when we consider that many aggregated/correlated/systemic risk models used to calculate worst case cyber scenarios, such as the recent A.M. Best/Guidewire study, do not take in to account potential cyber coverage under non-cyber insurance (i.e. "Silent Cyber") lines of coverage.[44] Two scenarios described in a Lloyd's 2017 emerging risk report were used for the 2018 A.M. Best/Guidewire stress test: one in which numerous cloud-based customer servers fail and cause widespread service and business interruption, and one in which a common software application is compromised and exploited on a global scale.

Consider modern manufacturing systems.[45] The interconnectedness of Industry 4.0 driven operations, such as those that involve industrial control systems, along with the escalating deployment of industrial Internet of Things (IoT) devices, has created a massive attack surface that manufacturers must protect.[46]

For business reasons, most manufacturers do not invest heavily in security access controls. Some controls can interrupt and isolate manufacturing systems that are critical for lean production lines and digital supply chain processes. However, property and general liability/product liability insurance carrier underwriters that consider cyber related coverage will want to understand the network visibility and real-time monitoring of interconnected systems, which are essential to identify the earliest signs of attacker behaviors in the manufacturing infrastructure. While organisations have limited resources to address unlimited risks, threats and attackers, the time spent to meet the various lines of insurance minimum cyber resiliency standards could provide the manufacturer with options to add insurance to protect its balance sheet from cyber related losses. Cyber insurance will remain an important component part of the overall enterprise wide security posture.

[42] *For example, Allianz announced November 2018, that it intended to move cyber related tangible property damage and bodily injury damages in to traditional property and casualty policies and out of standalone cyber insurance for a variety of reasons. AIG already offers to certain applicable cyber perils in either property, casualty or standalone cyber policies for an additional premium.*

[43] *US Treasury Makes Standalone Cyber Insurance Policies More Valuable: http://www.aon.com/attachments/risk-services/cyber/TRIA-2017Update.pdf*

[44] *Cyber Insurers May Lose 119% Of Policyholders Surplus In Single Event –Report: https://independent.ng/cyber-insurers-may-lose-119-of-policyholders-surplus-in-single-event-report/ "However, the report also did not take into consideration the silent cyber exposure of these companies, which A.M. Best warned could also potentially be significant."*

[45] *Threatlist: Attacks on Industrial Control Systems on the Rise, https://threatpost.com/threatlist-attacks-on-industrial-control-systems-on-the-rise/137251/*

[46] *Industrial IoT Escalates Risk of Global Cyber Attacks: https://www.industryweek.com/technology-and-iiot/industrial-iot-escalates-risk-global-cyberattacks*

Although some commercial property policies may cover some aspect of a loss due to a computer virus, standard coverage offers limited protection unless the data [47] is physically destroyed or corrupted.[48] General liability policies typically only address physical injury to persons or tangible property, as well as the insured's liability arising from the publication of material that violates a person's right to privacy. Policies such as the Surety and Fidelity Computer Crime Policies, which are sometimes assumed to provide coverage for cyber claims, generally exclude losses resulting directly or indirectly from the theft of confidential information, indirect consequential loss of any nature, and loss of potential income, including but not limited to interest and dividends.

In order to navigate around these grey areas of insurance coverage to address cyber perils, there are a few options:

A. Obtain a general liability insurance policy that does not contain a cyber or professional services exclusion (even if an organisation is required to pay additional premium to obtain affirmative cyber coverage). Otherwise, ensure the exclusions are narrow enough (or include carve backs) to be acceptable.

B. For every organisation that does not provide professional or business services, purchase a separate cyber insurance policy that provides contingent bodily injury/property damage coverage. Some insurance carriers are developing cyber difference in condition policies that sit on top of other lines of insurance policies in order to fill cyber coverage gaps.

C. For professional and business services organisations (or entities that offer services, information, etc. in addition to tangible products), purchase a professional liability policy that contains 1) a broad definition of professional services, 2) contingent bodily injury/property damage coverage and 3) is extended to include costs to the organisation to assist in managing a cyber incident (including but not limited to business interruption and cyber extortion).

D. All organisations of every size, industry and geography should consider cyber business interruption coverage, starting with an analysis of potential coverage under other existing policies (specifically cyber).

Since multiple insurance policies may apply to a cyber incident, it is important to draft the "Other Insurance" clause in all policies in a consistent manner to ensure that the order of coverage application is clear and unambiguous, and maximises coverage. For instance, it is usually advisable to have the cyber policy's first party coverages, particularly the breach expenses, be primary (respond and pay first) and have the professional liability policy be considered excess (respond second and pay after the cyber policy). This enables the cyber carrier to bring its expertise to a cyber incident and make resources available to the insured that will mitigate, or even prevent, a negligence claim from being made— benefits not included if the professional liability policy was primary and the response is led by a professional liability claims adjuster who is not a cyber insurance expert. The liability coverages available under the cyber policy would then be available on a "difference in conditions basis," which means responding on a primary basis where the professional liability policy is not triggered, such as when the insured's employment data is breached. Maintaining the insured's professional liability policy as primary (responds first before the cyber policy) for data breaches that essentially equate to negligence for alleged failure to maintain confidentiality ensures that an insured's professional liability carrier remains the primary claims coordinator for negligence claims (where they have greater expertise than cyber carriers). Furthermore, a potentially lower premium may be available on the cyber policy while eliminating a coverage overlap with the professional policy if the "Other Insurance" clause clarifies which policy responds and pays first (primary) and which policy responds and pays second (excess).

[47] *Note that this applies only if "data" is defined as a tangible asset.*

[48] *Except of ransomware attack methods, bad actors rarely destroy data because they do not want to leave a trace in your system. Instead, they just copy the data.*

5. Next steps

When considering insurance protection for cyber risks, organisations should make an informed decision as to how much and what type of insurance to purchase, and how that insurance mitigates larger cyber risks.

Insurers will consider the applicant's cybersecurity maturity (e.g. prevention, detection, and response controls) when underwriting and pricing the cyber policy. Alignment with best practice standards will help organisations withstand cyberattacks and can also result in more favourable insurance terms and conditions, because insurers favourably consider proactive cybersecurity when underwriting cyber risks. It is therefore important to meet with your insurance professional and discuss the coverages available in the context of the wider enterprise risks. While the insurance professional will have his or her approach to assessing cyber risk, it may prove useful to consider the following:

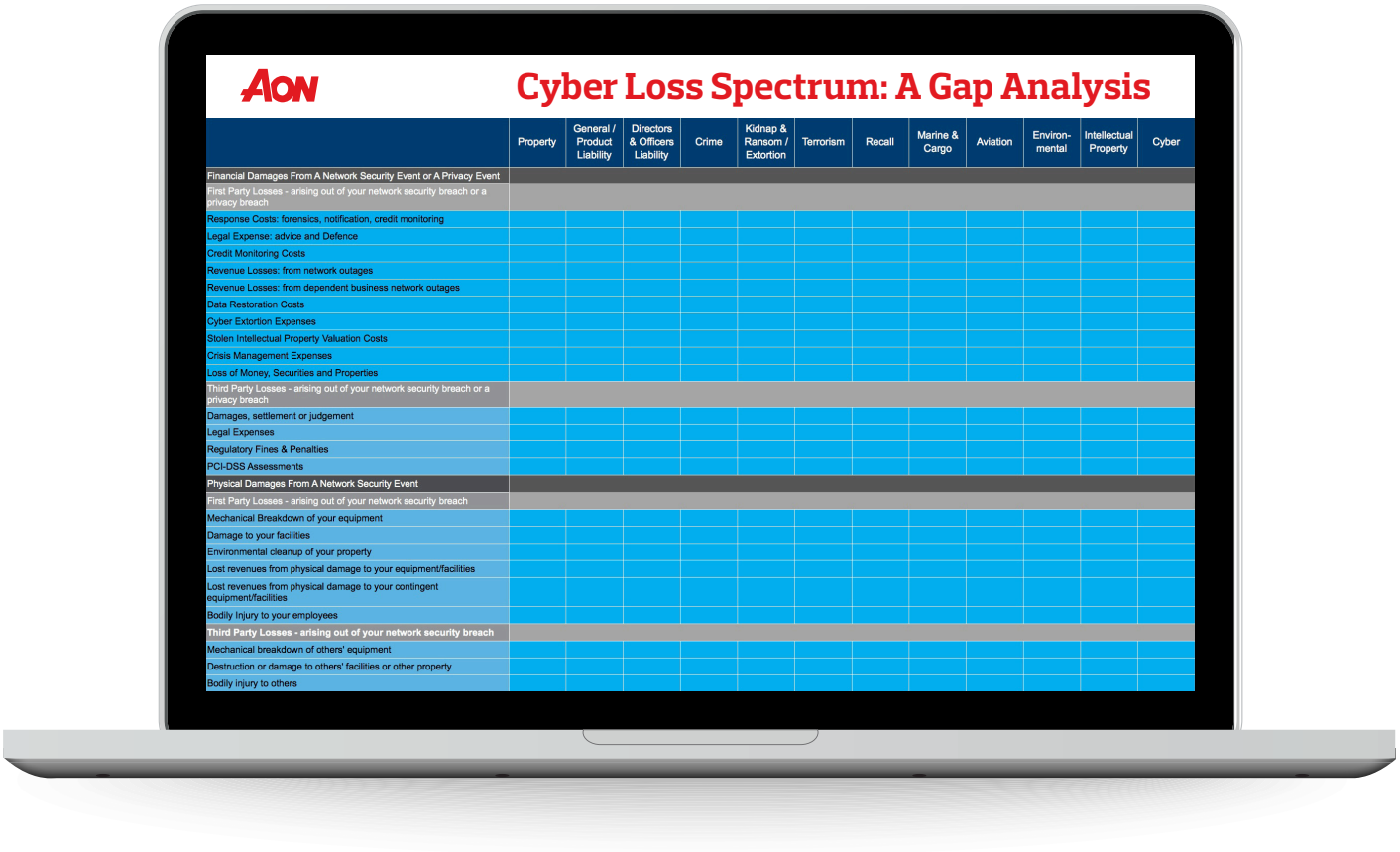
1. Ensure your organisation's leadership has an appropriate governance structure, particularly in regard to a reporting protocol for insurable and non-insurable cyber risk magnitude.

2. Position cyber insurance treatment solutions as a subset of enterprise risk management system capabilities for the organisation to enable a firm-wide cyber risk management culture. The question to model for your organisation - how does your Total Cost of Risk compare between cyber exposures and other material exposures?

3. Understand specific cyber vulnerabilities associated with operations, including the legal liabilities and financial exposure from IT systems and related customer and vendor contracts. This should include a review of vendors and the supply chain to evaluate potential insurance coverage and contractual indemnities from the insured's vendors.

4. Determine cyber coverage protection and gaps within your current insurance policies.

5. Analyse various scenarios in connection with potential coverage and gaps under all existing insurance policies, comparing first- and third-party coverages from potential insurers based on your firm's defined needs.



	Property	General / Product Liability	Directors & Officers Liability	Crime	Kidnap & Ransom / Extortion	Terrorism	Recall	Marine & Cargo	Aviation	Environ-mental	Intellectual Property	Cyber
Financial Damages From A Network Security Event or A Privacy Event												
First Party Losses - arising out of your network security breach or a privacy breach												
Response Costs: forensics, notification, credit monitoring												
Legal Expense: advice and Defence												
Credit Monitoring Costs												
Revenue Losses: from network outages												
Revenue Losses: from dependent business network outages												
Data Restoration Costs												
Cyber Extortion Expenses												
Stolen Intellectual Property Valuation Costs												
Crisis Management Expenses												
Loss of Money, Securities and Properties												
Third Party Losses - arising out of your network security breach or a privacy breach												
Damages, settlement or judgement												
Legal Expenses												
Regulatory Fines & Penalties												
PCI-DSS Assessments												
Physical Damages From A Network Security Event												
First Party Losses - arising out of your network security breach												
Mechanical Breakdown of your equipment												
Damage to your facilities												
Environmental cleanup of your property												
Lost revenues from physical damage to your equipment/facilities												
Lost revenues from physical damage to your contingent equipment/facilities												
Bodily Injury to your employees												
Third Party Losses - arising out of your network security breach												
Mechanical breakdown of others' equipment												
Destruction or damage to others' facilities or other property												
Bodily injury to others												

6. Consider alternative risk transfer strategies, including use of a captive, which could facilitate enhanced customisation and potentially increased limits capacity via access to re-insurance markets.

7. Satisfy minimum loss mitigation governance standards such as:

a. EU GDPR, violations of which could subject an organisation to fines up to €20 million or, if higher, 4% of an organisation's annual global turnover;
b. Industry specific standards, such as PCI, SWIFT, NIST and ISO.

8. Articulate the scope of responsibilities for individuals engaged in any cyber response plan, including consideration of protecting attorney-client privilege in communications.

9. Prepare the mechanisms for filing a cyber claim well in advance of any such event. Such claim mechanisms should be agreed upon in advance with the insurance carriers (including vetting of insurance carrier rating and claims paying experience) and set forth in the applicable insurance policies. Considerations should include:

a. Retention or deductible figure your organisation is comfortable retaining;
b. Selection of legal counsel, forensics experts, cyber assessment firms, PR, and credit monitoring firms (if necessary);
c. Business interruption "proof of loss" form and calculation.

10. Stay informed of insurance market trends to address cyber perils, particularly for coverage capacity, policy wording customisation and regulatory constraints. Cyber exposures and solutions are dynamic and fluid.

Contacts

EMEA

Onno Janssen
Chief Executive Officer EMEA
onno.janssen@aon.com
+49 (4) 03 605 3608

Vanessa Leemans
Chief Commercial Officer EMEA
vanessa.leemans@aon.co.uk
+44 (0) 20 7086 4465

Spencer Lynch
Managing Director – Cyber Security
spencer.lynch@aon.co.uk
+44 (0) 20 7061 2304

Roger Francis
Vice President – Cyber Security
roger.francis1@aon.co.uk
+44 (0) 20 7061 2312

David Molony
Director – Cyber Risk
david.molony@aon.co.uk
+44 (0) 20 7086 7043

Shannan Fort
Cyber Insurance Leader Global Broking Centre
shannan.fort@aon.com
+44 (0)20 7086 7135

Authored by Kevin P. Kalinich, Esq.
Edited by Shannan Fort, David Molony,
Roger Francis and Vanessa Leemans

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

www.aon.com

Empower Results®