The Insurance Business in Transition to the Cyber-Physical Market: Communication, Coordination and Harmonization of Cyber Risk Coverages

July 1, 2018 Version (Draft)

W. Jean Kwon
School of Risk Management
St. John’s University
New York, NY
Facpub.stjohns.edu/~KwonW/

This version (July 1, 2018) is a draft and subject to revision. The author continues to gather comments from the academia, the industry and the public sector.

Please do not reproduce this draft paper. Permission of the author is required for quotation of this and all other versions.

All comments can be directed to KwonW@stjohns.edu.
Table of Contents

1 Abstract 3
2 Executive Summary 3
3 Acknowledgement 4
4 Physical Risk and Cyber Risk 5
5 Consumer Protection in the Cyber World 6
6 Cybersecurity and Cyber Risk 8
7 Cyber Risk Quantification and Data Quality 11
8 Cyber Insurance Coverages 14
9 The Insurance Market in Transition 18
10 Communication, Coordination and Standardization 21
11 A 2017 Survey of Cyber Insurance Underwriters 23
12 Regulation and Self-regulation 27
13 The Business of Insurance in Transition to the Cyber-Physical World of Risk 28
14 References 29

15 Table 1: Findings from Cybersecurity Surveys of Risk Bearers ............................................................. 9
16 Table 2: Selected Academic Studies Covering Cyber Risk Measurement and Pricing Models ............... 12
17 Table 3; Key Findings from Cyber Insurance (Market) Studies (Selected) .................................................. 14
18 Table 4: A Summary of the U.S. Cyber Insurance Market (2015-2016) ...................................................... 15
19 Table 5: Cross-industry Comparison of Cyber Loss Exposure Classification .............................................. 22
20 Table 6: Insurance Policy Comparison (Selected Definitions) ...................................................................... 25
21
22 Figure 1: Distribution of Cyber Insurance Premiums in the U.S. for Data Year 2016 ($ Million) .......... 16
23 Figure 2: Conventional and Cyber Insurance Coverages ............................................................................ 20
24
25
26
Abstract

This study discusses extensively cyber risk as a family of risks and whether there is a commonality in the perception – thus management – of the risk in the academic, risk management, insurance and policymaking communities. We find that cyber breach is perceived as “critical” due in part to its own nature and, importantly, in part to the weak understanding of its impact and our preparedness. Variations in cyberattack distributions and probabilities exist depending on who conducts the study (survey) and also on the composition of the study sample. Some variations are by industry or region, while others are about the weight of internal human errors vs. external attacks. We add examination of how the insurance market has been dealing with cyber risk (as well as all other critical risks in the past) to this study to strengthen our contention that we need to build up an infrastructure to continue our operations in the physical-cyber world of risk. Thus, there rises the responsibility of the insurance industry for assisting individuals and organizations in the management of the risks.

Executive Summary

From a historical perspective, the business of insurance began to deal with a variety of causes of that we could observe. They include natural catastrophes and other calamities as long as the loss outcome would not compromise the sustainability of the industry, at least in principle. The industry then added coverages for intangible causes of loss – liability risks – of which loss outcome includes not only property damages and bodily injuries. It also include personal injuries. With the commercialization of information technology, we witness that human and business activities are increasingly intertwined and interconnected in the cyberspace. We witness the rise of non-physical, cyber causes of loss as well. Damages arising from the resulting loss events during the early stage of the information technology were limited in the scope and amount, and the industry found solutions by expanding business interruption provisions in the property insurance market. Advances in robotic process automation, cognitive automation (including artificial intelligence and machine learning), Internet of Things (IoT) and the blockchain keep the world more interconnected and the world of cyber risk expanding.

The regulatory measures in the cyberspace are thus far primarily about privacy protection and data management. Like in the physical world, government regulation in the cyber world is to manage risks at the societal or economic community level. Thus far, no countries are known to have a law that subjects the regulated firm to any specific tools to control or finance cyber risk.

This study analyzes the nature of cyber risk (cyberattacks) from a risk management perspective and then from an insurance business perspective. Specifically, it examines extensively the perception of it as a risk and the level of preparedness by the risk bearers as well as whether there is a commonality in the perception by the members in academic, risk management, insurance and policymaking communities. We find that cyber breach is perceived as “critical” due in part to its own nature and, importantly, in part to the weak understanding of its impact and our preparedness. Variations in cyberattack distributions and probabilities exist depending on who conducts the study (survey) and also on the composition of the study sample. Some variations are by industry or region, while others are about the weight of internal human errors vs. external attacks. Reasonable consistency in the sample throughout the study period is essential for generalization of the findings. Nonetheless, existing studies strongly suggest that an insight into employee vigilance and training of all employees remains critical in cyber risk management.

A constant search for statistically useful data for every emerging risk a norm in risk management. Conversely, a lack of understanding of the risk can lead to non-collection of the data or ineffectiveness in the use of collected data. A weak coordination for standardization of the risk among different players reduces efficiency in data management. Studies about quantification of cyber risk are found but commonly are based on theory or simulated-based approaches, including but not limited to modified Bayesian model, information asymmetry theory, utility theory and unifying framework. The question of how to measure performance in cybersecurity is still largely unanswered.
It seems there is a widespread tendency to treat all cyber loss exposures as “a single risk” rather than “risks” in the cyberspace. This study offers a logical reasoning why it is about the multiplicity of the risk—

with respect to the causes and also to the resulting damages. Accordingly, we propose that the insurance industry develops a portfolio of coverages—rather than a coverage—for operations in the cyber world of risk along the side of their operations in the conventional physical world of risk.

We support this proposal with the examination of how the insurance market has been dealing with cyber risk (as well as all other critical risks in the past). Two approaches are employed at this stage. One is an analysis of the existing studies along with the historical development of the insurance market. It seems that the industry employs a cycle of adjustment from an initial denial (or extension) of coverage to the modification of coverages (for example, exclusions and coverage limits) and finally to the market adjustment (for example, an introduction of a new policy or line of business). The industry’s response is somewhere between the modification and the final adjustment stages.

There remains a concern about whether there is an appropriate channel of communication between the experts in insurance and those in risk management, whether there is a reasonable coordination of efforts within the insurance industry in the attempt to reach the final stage of the above-noted cycle, and whether existing cyber insurance policies show some harmonization in the structure from the consumer’s viewpoint. We find a gap of communication between risk managers and insurance underwriters, as evidenced by wide differences in loss exposure classification. We find a wide gap in the list of definitions and the way insurance companies offer their definitions of the contractual terms relevant to cyber risk. In conclusion, it appears that the shapes of cyber insurance policies converge but the contents are so different. The presence of a gap between the cybersecurity community and the cyber insurance community often makes it difficult for the members to find a common basis for the development of reasonable standards of security and insurability. Standardization is critical not only to help the cyber insurance market further developed. It is equally to other stakeholders. Consumers need a guideline for comparison of policies and consumption of the coverages right in scope and limit. Standardization is critical for governments to properly promote cyber risk management and insurance within their domestic economies and cross border.

Finally, the insurance industry might be too eager to commoditize the risk, yet without fully understanding it. The market might be developing too fast to allow insurance companies to come up with properly designed coverages. The cyber world is expanding. It is adding artificial intelligence-based, machine learning elements and becomes more complex as existing and new elements are increasingly interconnected. This expansion will certainly add values to society. It will also change the nature of existing risks and add new risks, thus increasing the responsibility of the insurance industry for assisting individuals and organizations in the management of the risk. Accordingly, we need to build up an infrastructure to continue our operations in the physical-cyber world of risk.

Acknowledgement

The author extends his sincere thanks to the following persons for their in-depth comments to this study: William Henriques (Aon Benfield), Paul Miskovich (Axis Insurance), Jill Salmon (Berkshire Hathaway), Kurtis Suhs (Ironshore), Eric Nordman (formerly, the NAIC), Kawa Owens (Markel), Phil Fraim (Oklahoma Attorneys Mutual), Steven Anderson (QBE) and Lauren Markowski (TransRe). His sincere thanks are also extended to the respondents of the 2017 survey for this study: Dan DeLoof (Allianz), William Kelly (Argo Pro), Paul Miskovich (Axis Insurance), Jill Salmon (Berkshire Hathaway), Dan Zureich (Lawyers Mutual Liability of North Carolina), Phil Fraim (Oklahoma Attorneys Mutual), Sean Letz (Marsh), Phillip Fraim (Oklahoma Attorneys Mutual), Evan Fenaroli (Philadelphia Insurance), Steven Anderson (QBE), Elissa Doroff (XLCatlin) and other participants who wish to remain anonymous.
Physical Risk and Cyber Risk

The world of risk continues to change. It reshapes the nature of existing risks and adds new elements. So has been the responses of the insurance industry. This dynamic industry keeps adjusting it business dimensions in tune with the changes in the world of risk. Such adjustments often call for innovation in the management and financing of the risks effectively and efficiently not only for its own sustainability and growth but also for the society and economic community it serves. Indeed, the insurance industry has generally been dynamic, responsive and innovative. Increasingly, it becomes proactive.

From a historical perspective, the business of insurance began to deal with a variety of causes of that we could observe. They include natural catastrophes and other calamities as long as the loss outcome would not compromise the sustainability of the industry, at least in principle. The coverages against physically observable causes – and indemnification of the victims for their property damages and bodily injuries – still a main line of business in today’s insurance market.

The industry has gradually added coverages for intangible causes of loss – liability risks – which root mainly from statutory developments, contractual obligations as well as human errors and misbehaviors.\(^1\)

The loss outcome now includes not only property damages and bodily injuries. It also include personal injuries. In retrospect, the liability line of business was unwavering and was not much subject to significant variations. However, the liability crisis in the early 1980s – caused by the expansion of the tort doctrine and the rising frequency and generosity of court decisions in favor of victims of civil wrongdoing in the middle of the volatile economic period – led to a distortion in the insurance market. There were wide-spread coverage availability and affordability issues in selected lines of business. The industry needed time to adjust its business dimension. It began to expand coverage exclusions, restrict per-occurrence and aggregate coverages and introduce claims-made policies. A series of reforms in its infrastructure has led the market to be more responsive to the changes in the world of liability risk. Such reforms continue as the world of risk is never constant.

With the commercialization of information technology, we witness that human and business activities are increasingly intertwined and interconnected in the cyberspace. We witness the rise of non-physical, cyber causes of loss as well. Damages arising from the resulting loss events during the early stage of the information technology were limited in the scope and amount, and the industry found solutions by expanding business interruption provisions in the property insurance market. Advances in robotic process automation, cognitive automation (including artificial intelligence and machine learning), Internet of Things (IoT) and the blockchain keep the world more interconnected and the world of cyber risk expanding.

Today, business and non-business communications, financial transactions and other economic activities become less observable as they increasingly occur in the cyberspace. For example, Swiss Re (2014) treats “cloud computing security” as one of the five-high-impact risks, the impact of which could be materialized in the 0-3 year time frame. Indeed, cloud computing, despite the perceived and potential benefits to the users, could result in data concentration risk, data loss and breach, service interruption, third-party liability and reputation risk. As more organizations shift their operations to the cyberspace, they store and transmit the so-called “protected data” virtual processes and protocols.\(^2\) Besides, sensitive personal information and financial data have become a “criminal commodity” that illicit organizations target via denial-of-service attacks (Lloyd’s 2017).

As compared to the conventional physical world, the cyber world of risk possesses a number of traits from the risk management perspective. First, the cyber world of risk comprises intangible causes of loss that exist in the information technology infrastructure. Limitations in scientific knowledge, flaws in the design and execution of the system, and faults in personnel training (thus human errors) can inflate the loss

---

\(^1\) It is obvious that liability insurance does not, and should not, deal with the losses to third parties as a result of the criminal intent of the insured.

\(^2\) Protected data commonly includes clients/employees/others’ confidential commercial information (CCI), personally identifiable information (PII) and personal health information (PHI) (Jones and Yellen 2015).
probability and severity. The criminal intent and the act of extortion by individuals and organizations further inflate the loss outcome. These direct causes may result, and have resulted, in consequential losses, such as physical property damages (including business interruption and continuation expenses) as well as bodily injuries and personal injuries (albeit sporadically thus far). In numerous cases involving cyber risk, indirect losses can be substantially higher than direct losses.

Second and from a risk management viewpoint, the cyber world comprises solely of man-made causes of losses: that is, technology/artificial intelligence-driven perils created by monetary motives of human (including employees and criminals) and human mistakes. By comparison, the physical world contains both man-made and physical causes of loss. Given this overlap of man-made causes of loss in both physical and cyber world of risk, companies seem to attempt a coverage solution by building cyber risk on the side of (that is, as endorsements to) conventional coverages or using carved-out, stand-alone coverage approaches. A question arises whether it is the best solution, which warrants examination.

Third, the losses resulting from cyberattacks are basically intentional from the perspective of the causer (that is, the perpetrator or an ill-minded member of the entity). There is criminal intent to harm an entity and the loss outcome is intentional as well. Also likely are losses to the third parties such as clients of the victim entity as well as the vendors or clients of the vendors in the chain of production and distribution. Accordingly, financing cyber risk involves both first party and third-party (liability) loss exposures.

The non-static nature of the cyber world of risk demands the maintenance and constant improvement in pre-loss techniques. Stringency in cybersecurity regulation helps us better protect customers and other business partners in the chain of production risk. Post-loss solutions to the victims in the cyber world help us better manage the severity of economic losses. However, every invention in technology is an open invitation of another invention and technological advancement can expose us to a risk in the cyber world. Consumer education and personnel training helps but is likely to remain as a partial solution because we deal with the perpetrators at large in the cyber world of risk.

Consumer Protection in the Cyber World

Governments intensify their attempts to protect citizens and businesses in their cyber jurisdiction. New or revised measures of this kind commonly prescribe how the regulated entities should manage data security and privacy protection matters within their organizations as we as throughout their chain of production. Some notable measures include the EU’s General Data Protection Regulation (effectively from May 2018), Australia’s Australian Privacy Principles of 2014 which originates from the Privacy Act of 1988 (revised in 2012), Canada’s Personal Information Protection and Electronic Documents Act of 2000 and amendments, Singapore’s Personal Data Protection Act of 2012 (under revision), China’s Cybersecurity Law of 2007, Japan’s Act on the Protection of Personal Information of 2003 and its 2017 amendment, and the U.S. federal and state measures.

---

3 Increasingly, non-professional individuals and state-supported agencies add problems to the management of risks in the cyber world.

4 Mosburg et al. (2016) classified cyberattack impact factors into two groups: the “above the surface” group including but not limited to post-breach customer protection, customer breach notification, fines & penalties and cybersecurity improvements; and the “beneath the surface” group. They find that the “beneath the surface” factors in the aggregate cost 96.48% of the total cost in the case of a U.S. health insurance company (mainly, value of lost contract revenues, lost value of customer relationships and devaluation of trade name) and 99.19% in the case of a U.S. manufacturer (mainly, value of lost contract revenues, operational disruption and devaluation of trade name). Verizon (2017) reports that 60% of cyberattacked firms or so experienced revenue and customer losses rising up to 50% and that 10% of the firms even experienced their revenue loss exceeding 80%.

5 The Act on the Protection of Personal Information of Japan went into effect in April 2005, after which policies covering losses resulting from cyberattacks to their client corporations could become available (Koazuka 2016).
The General Data Protection Regulation (GDPR) affects EU organizations operating in or beyond the EU community. It is poised to be stringent in enforcement, and noncompliance may cost the firm fines up to €10 million or 2%, whichever is the greater, of its worldwide annual revenue for infringements. The fine can rise up to €20 million or 4%, whichever is the greater, of its worldwide annual revenue for serious infringements. At the time of writing, compliance issues seem to exist. A survey of over 500 respondents finds that 37% of them handled data of European citizens – thus likely being subject to the GDPR – but only 27% of them recognized they would be subject to the regular compliance. Only 17% of the respondents considered that they were ready for GDPR compliance, as compared to 42% of them that were not ready for the compliance (Infosecurity 2018). Separately, an agreement on the harmonization regarding breach notification within the EU community remains as an issue. The GDPR does not cover the handling of personal data in the insurance industry.

China’s Cybersecurity Law (effective in June 2017) treats the financial services sector a “critical information infrastructure” because a data breach in the infrastructure would compromise public welfare or national security. The law requires financial institutions to meet information technology infrastructure standards and pass certification tests; otherwise, they would face criminal charges and fines up to RMB 1 million (KPMG 2017).

It is yet U.S. centric when it comes to the extensity of laws and regulations prescribing reporting cyber incidents. In particular, the New York Department of Financial Services (NYDFS) passed cybersecurity regulation in March 2017 that require all licensed financial institutions in the state to, among others, establish a written policy, implement a structured cybersecurity program and perform periodic vulnerability tests of their systems. The U.S. National Association of Insurance Commissioners (NAIC) has adopted the Insurance Data Security Model Law in October 2017. Known to have modeled after the NYDFS regulation, this NAIC model law sets the minimum standards of cybersecurity practices for insurance companies as well as monetary penalties for noncompliance.

We note that regulatory measures in this regard are thus far primarily about privacy protection and data management. Like in the physical world, government regulation in the cyber world is to manage risks at the societal or economic community level. The regulation is to monitor and police the quality of the risk management activities of the regulated organizations, desirably permitting each regulated organization to design its own regulation-compliant, cyber risk management policy. Thus far, no countries are known to have a law that subjects the regulated firm to any specific tools to control or finance cyber risk. Finally, we note that stringency in regulation governing consumer data and privacy protection induces consumption of cyber coverages. Nonetheless, the level of consumption by large and small organizations seems to remain relatively lower than what it should be.

---

6 The GDPR – also known as Regulation (EU) 2016/679 – replaces Data Protection Directive 95/46/EC which the community adopted in 1995 to protect individuals from the unauthorized processing or movement of personal data.

7 Other respondents considered that the GDPR was not applicable to them.

8 Enforcement of the law was delayed to December 2017.

9 At the time of writing, there is no U.S. federal law governing the notification standards. The federal government maintains a wide array of statutes regarding intellectual property, cybercrime and computer privacy issues, for example, the Federal Trade Commission Act of 1914, the Fair Credit Reporting Act of 1970, the Privacy Act of 1974, the Health Insurance Portability and Accountability Act (HIPAA) of 1966, the Financial Modernization Act of 1999 and the Sarbanes-Oxley Act of 2002. From this year, all U.S. states maintain security breach notification laws or similar measures. For the summary of U.S. laws in this regard, refer to Maheu (2009), Edwards Wildman (2014), McNicholas and Mohan (2015), Rishikof and Sullivan (2017) and the National Conference of State Legislatures (2017).
Cybersecurity and Cyber Risk

Scientists have long examined network security and attacks. The Y2K risk in 1999 short-lived but its potential was strong enough for the industry to design single-event specific insurance coverages and programs. The dot.com bubble sent the industry another signal but their loss exposures per se were too speculative and sporadic to induce formal risk financing infrastructure. By comparison, the interconnected communication networks and data sharing have grown substantially in scale and scope enough to attract the attention of numerous stakeholders. This interconnected world exhibits a high degree of robustness. At the same time, it is open to errors and attacks — for example, a change or removal of one or more nodes that are vital in maintaining the network connectivity — that Albert et al. (2000) call the “generic properties” of the world.

Cyber reliance, despite its enormous benefits to society and the economy, expose us to a heightened level of uncertainty and insecurity in the cyber world. “Hidden risks” emerge from the world (Allianz 2015). Cyber risk resides in the dark web as well, thus adding problems to the risk identification process. The technology for data storing and sharing in the cyberspace advances, and well-resourced criminals twig it for stealing wealth or causing harm to the innocent. Even, the record indicates that several state and state-sponsored agencies deployed a series of (distributed) denial-of-service (DDoS, DoS) attacks targeting victims randomly and a massive scale. Their activities are apparently for financial gains but we cannot eliminate the possibility of cyberterrorism, which is to instigate psychological fear and political uncertainty in the target community. Criminals engage in both enabling activity (such as encrypted messaging and social media to promote violence) and disruptive activity (such as message manipulation and data infiltration). Cyber risk becomes a critical element in the strategic risk management programs of organizations of all sizes. It is a critical risk to society and its members.

Broadly, a cyberattack refers to the materialization of the insecurity instigated by ill-minded members of the society, criminals, system failure or machine learning (likely in the near future). It has already become a serious threat. World Economic Forum (2018) continues to rank it in the top-right quartile of its annually published Global Risk Landscape. It is the 3rd highest risk in terms of likelihood and the 6th in terms of impact among all risks in the report. The Cambridge Center for Risk Studies (2017) ranks it as the 7th most critical risk in its 2017 Global Risk Index. A NATO agency-sponsored study in 2015 finds that the likelihood of a recurring material data breach over the two years following the survey year is 27.7%, which is 2.1% higher than the finding from its previous survey (Brangetto and Aubyn 2015).

Cyberterrorism coverage is available in the cyber insurance market. For example, Allianz defines it as “any actual, or alleged intentional act on a computer system, including but not limited to the use of force or violence, by a natural person or entity, committed or threatened for political, religious, ideological, or similar motivation with the intention to influence, harm or instill fear in any insured or any client of any insured.” Berkshire Hathaway’s definition is “actual or threatened attacks against a computer network with the intention to cause harm in order to further political, religious or ideological objectives...[but do] not include activities that are in support of any war or military action.”

Harry and Gallagher (2017) group the disruptive activity into the following 5 cases: message manipulation (the most common), external service disruption (for example, DDoSs), internal communication interference, data attack and equipment attack.

Cyber insurance policies increasingly offer system failure coverages.

Other risks in the same quartile are extreme weather events, natural disasters, failure of climate change mitigation & adaptation, water crisis, biodiversity loss & ecosystem collapse, and large-scale involuntary migration.

The risks ranked higher than cyberattack are: market crash, interstate conflict, tropical storm, human pandemic, earthquake and flood.
A number of survey findings – as summarized in Table 1 – point that cyber breach is a critical risk due in part to its own nature and, importantly, in part to the weak understanding of its impact and our preparedness. For example, a global survey of senior executives and industry experts reveals that the most common incidents were not hacking but accidental major systems outrages (29%) and the loss of sensitive data by employees.
sensitive data by employees (27%) (The Economist 2014). It is also noted in the global survey that more than two-thirds of the survey respondents experienced a cyber incident in 2012 or 2013 but 39% of them did not have an incident response plan at the time of the survey. A 2018 survey by PwC indicates that the biggest potential consequences of a cyberattack to the respondent organization is the disruption of operations (40%), the compromise of sensitive data (39%), harm to product quality (32%), damages to physical property (29%) and harm to human life (22%) (Castelli, et al. 2018).

Variations in cyberattack distributions and probabilities exist by industry. Lloyd’s (2017) surveyed business leaders in Europe in 2016 to find: the seriousness of CEO fraud, the financial services sector being a target of cybercrime, professional service firms (for example, law firms and accounting companies) as a gateway to attack their clients, a rise in the use of ransomware and DDoS attacks in in healthcare, media and entertainment services, and public sector entities and telecommunications industry firms being susceptible to espionage-focused cyber-attacks. Swiss Re (2016) finds not only industrywide differences but also variations in risk awareness by region: for example, firms in North America and South America are apparently more concerned about cyberattacks than those in Europe and in the Middle East & Africa. It also finds that small firms are increasingly aware of cyber risk.

Reasonable consistency in the sample throughout the study period is essential for generalization of the findings. However, it is challenging to maintain such consistency in survey-based studies. For example, Ponemon Institute (2015, 2016 and 2017) cites that data breach costs fluctuate from one survey year to the next but their findings – albeit their value as a general reference for risk management – are based on the analyses of sample groups which are different in size and country of representation. Here is a summary of findings regarding the cost.17

- Its survey in 2015 (252 companies in 7 countries) shows that the annualized cost ranged from $0.31 million to $65 million, with an average of $7.7 million.18
- Its survey in 2016 (383 companies in 12 countries) indicates that the average cost rose to $4 million and that the average cost per lost or stolen record was $158 for the same year. Malicious or criminal attacks contributed to 48% of all breaches in 2016.
- Its survey in 2017 (419 companies in 13 countries) presents that the annualized average cost of data breach was $3.62 million, or an almost 10% decrease from the previous survey year. The average cost per lost or stolen records was $141, or a decrease of 11.4% from the previous year.

Some limited data is available regarding the impact of cyber incidents on the insurance industry. NetDiligence (2016) analyzed claims data of 2013-2015 from 19 insurers. They find that the majority (87%) of insurance claims were from organizations with revenues less than $2 billion. The average number of records lost was 2.04 million while the median remained at 1,339. The average insurance claims paid was $495,000 while the median was $49,000. And the average cost of breach was $665,000

15 The survey findings suggest that automated detection tools, such as the security information and event management (SIEM), could detect about one-third of incidents.

16 The U.S. Federal Bureau of Investigation (2016) reports that the losses resulting from CEO fraud – commonly in the form or phishing, executive whaling, spear phishing or social engineering – was estimated at $3.1 billion as of May 2016, or an increase of 1,300% from January 2015. Executive whaling refers to the practice of siphoning off money from account or stealing confidential information by targeting top executives; spear phishing refers to sending emails purportedly from a trusted sender to steal confidential information from targeted individuals; and social engineering means tricking people psychologically to steal confidential information or to get access to funds.

17 The institute notes that the majority of data breach incidents studied in the report happened in the previous calendar year. The cost includes both direct and indirect expenses incurred by the respondent. The direct expenses include expenditure for forensic experts, outsourcing hotline support, provision of free credit monitoring subscriptions and discounts for future products and services. The indirect expenses include in-house expenses for communications and investigations as well as the value of customer loss resulting from turnover or diminished customer loyalty.

18 The annualized cost is based on the data from fiscal years 2013-2015.
while the median stayed at $60,000. These findings support that cybersecurity breaches occur in all sizes of companies.

Failures in human risk management can induce a rise in cyber insurance claims. NetDiligence (2016), for example, finds that an inside involvement was found in 30% of insurance claims submitted and 77% of such claims was the result of “unintentional,” caused by employee errors. Only the remaining 22% was malicious in nature. The study findings are, however, inconsistent. For example, Verizon (2008, 2012 and 2017) reports that 75% of all cases in 2016 were perpetrated by outsiders (inclusive of 15% by state-affiliated actors and 51% by organized crime groups) in its 2017 report. Its findings vary by the study year. It reports that the percentage of breaches caused by external sources was 73% and 98% in the 2007 and 2011 data years, respectively.

In contrast, the University of Cambridge and RMS (2017) find data losses were increasingly caused by external actors which attributed 80% or greater of all types of attacks in 2010-2015 and again in 2016. The findings from the 2018 PwC Global State of Information Security Survey (9,500 executives in 122 countries) indicate that 44% of the respondents do not have an overall information security strategies, 48% have no employee security awareness program, and 54% are without an incident response process. (Castelli, et al. 2018). It also finds that only 39% of the respondents are very confident in their attribution capabilities.

The findings from the studies – due possibly to the differences in the composition of the contributing organizations – offer us some insight but are short of delivering a full picture for systemic risk management at the societal level. Neither could we generalize the findings of the existing study to measure the impact of human errors in cyber risk management. Together, however, they strongly suggest that an insight that employee vigilance and training of all employees – for example, practicing “cyber hygiene” – remains critical in cyber risk management.

Similar to the direction of cyber risk management at the government level, the direction of cyberattack identification process is to offer organizations broad guidelines for their technical and human risk management at the societal level. Strong correlations may exist between the cyber risk identification approaches of the government-private sector and those of private insurance companies. Nevertheless, it remains to be examined whether these approaches are based on a common standard for risk classification.

Cyber Risk Quantification and Data Quality

Simply put, availability of quality data is a critical issue in cyber risk management. The risk is new and keeps evolving. This attribute of the risk makes old data less relevant quickly. Quality cyber incident data is still insufficient and existing study findings based on the data are commonly statistically inconclusive.

---

19 Verizon defines a breach as an “incident that results in the confirmed disclosure of data to an unauthorized party” as compared to a security event referring to a “security event that compromises the integrity, confidentiality or availability of an information asset.”

20 Cyber hygiene, a generic term, is a risk mitigation technique designed for appropriate protection, maintenance and update of information technology systems and devices at the individual employee level. It is primarily to maintain the individual employee’s online health (thus security). Examples of the technique include updating software, virus definitions and passwords, securing personal data and back-up and maintaining a firewall. The best practice of it requires participation of all employees.

21 The International Organization for Standardization (ISO) and the International Electronic Committee (IEC) published jointly the ISO/IEC 27000-series – also known as the Information Security Management System (ISMS) Family of Standards – in 2013. We find resemblance in the ISO/IEC’s risk identification and classification approaches but in a way that requires ISO expertise, let alone that the family comprises 45 standards or so.
The “quick and highly dynamic nature” of cyberattacks complicate the assessment of cyber risk (Kopp, Kaffenberger and Wilson 2017).

A constant search for statistically useful data for every emerging risk is a norm in risk management. Conversely, a lack of understanding of the risk can lead to non-collection of the data or ineffectiveness in the use of collected data. A weak coordination for standardization of the risk among different players – even between risk managers and insurance professionals as further discussed in this paper – reduces efficiency in data management.

Table 2: Selected Academic Studies Covering Cyber Risk Measurement and Pricing Models

<table>
<thead>
<tr>
<th>Author</th>
<th>Model Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wang (2017)</td>
<td>Annual loss expectancy model for quantification of the combined effect of investments in addressing cyber threats and vulnerability to derive the annual loss expectancy of the residual cyber risk (or insurance premium for full risk transfer)</td>
</tr>
<tr>
<td>Sommerstad et al. (2010); Munoz-Gonzalez et al. (2016)</td>
<td>Bayesian attacks (defense graphs; architectural) model which uses prior knowledge about vulnerabilities and network connectivity to reason the threats and their risks in a formal way; Focus on the most-effective threats for production of countermeasures selection via static analysis</td>
</tr>
<tr>
<td>Nie et al. (2016)</td>
<td>Ruin theory for application to assess the dynamic change in monetary value or capital position of an insurance portfolio, assuming that a ruin event is similar to a failure in cyber defense.</td>
</tr>
<tr>
<td>Hubbard and Sieresen (2016)</td>
<td>Foundation and theoretical application for the measurement of cybersecurity risk, including the human (subjective probability) factor, a risk matrix methodology, and a data decomposition-based decision analysis</td>
</tr>
<tr>
<td>Sonnenreich et al. (2006); Brangetto and Aubyn (2015)</td>
<td>Return on Security Investment (RoSI) model, a modified RoI model in which the monetary value of security investment is compared with that of risk reduction, alternatively to evaluate the amount of potential loss that can be saved by the investment</td>
</tr>
<tr>
<td>Mukhopadhyay et al. (2013)</td>
<td>Copula-aided Bayesian Belief Network (CBBN) model for cyber vulnerability assessment and expected loss computation; utility based preferential pricing (UBPP) model to compute cyber insurance premium</td>
</tr>
<tr>
<td>Aissa et al. (2010); Aissa et al. (2012)</td>
<td>Mean Failure Cost (MFC) model, which is a cascade linear model, to quantify security threat in terms of loss that results from system vulnerabilities by computing the loss of operation for each stakeholder of the system; application to e-commerce</td>
</tr>
<tr>
<td>Öğüt et al. (2011)</td>
<td>Application of a utility model to examine the effect of correlated risks and unprovable losses on self-protection and insurance consumption of firms from a public policy perspective</td>
</tr>
<tr>
<td>Bohme and Schwartz (2010)</td>
<td>Unifying framework (theoretical) approach for, and application to, analytical models, the framework of which is divided into factors specific to cyber risk and cyber insurance</td>
</tr>
<tr>
<td>Bandypadhyay et al. (2009)</td>
<td>Information asymmetry theory-based, schematic approach to prove that cyber insurance is probably overpriced with high deductible and/or lower coverage limit</td>
</tr>
<tr>
<td>Mukhopadhyay et al. (2005)</td>
<td>Application of a utility theory to model the expected premium an insured entity is required to pay, which is also a function of its risk profile</td>
</tr>
</tbody>
</table>

Source: Author compilation

Studies about quantification of cyber risk are found. Aissa et al. (2010, 2012), for example, suggest that quantification of the risk requires two input variables – the probability of a threat occurrence and the loss resulting from a successful attack – for the Mean Failure Cost (MFC) model. The MFC can be more than a cybersecurity metric because it quantifies the monetary value of per unit of operational time as well as measures the amount of risk each stakeholder incurs as a result of a security threat or vulnerability (Rjaibi and Rabai 2015). Modified Bayesian models have been applied – for example, by Sommerstad et al. (2010) and Munoz-Gonzalez et al. (2016) – to create attack graphs and defense mechanisms on the same graph, thus generating enhanced knowledge about, and countermeasures to, attacks. Other

---

22 Allianz (2015) estimates that the annual cost of cybercrime to the global economy is $445 billion.
studies include but are not limited to application of ruin theory (Mukhopadhyay et al. 2005; Nie et al. 2016), information asymmetry theory (Bandyopadhyay et al. 2009), utility theory (Öğüt et al. 2011), unifying framework approach (Bohme and Schwartz 2010), Copula-aided Bayesian Belief Network (Mukhopadhyay et al. 2013) and annual loss expectancy model (Wang 2017). Table 2 presents a summary of selected academic study findings.

The question of how to measure performance in cybersecurity is still largely unanswered. Various attempts were made with a return-on-investment framework for cybersecurity, a process that often fails because of the difficulty in quantifying the gains with any reliability (Brangetto and Aubyn 2015). The absence of quality data makes it challenging for insurance companies to estimate the capital cushion they should hold against the risk (van Liebergen and Boer 2017).

There is a lack of quality loss data in the cyber world but the insurance industry dealt with similar cases with then-emerging risks in the past, such as satellite risk, political risk and terrorism risk. What matters is how we gather and classify data for risk pricing and underwriting purposes. It is also how to standardize the classification of cyber risks. Cyber risk is unique in many aspects but does not necessarily require an invention of a new assessment technique. We can revise existing statistical, heuristic and simulation methods to improve our predictability of cyber loss exposures. Data availability certainly an issue but, fortunately or not, more data is on the way.

As alluded to above, it is the human factor that makes cyber risk assessment challenging. It is the unknown identity of the criminals, whose capacity and behavior remain unpredictable. It is the negligence or malicious intent of the people that causes losses to the organizations they are affiliated. For example, Ponemon Institute (2017) identifies three root causes of data breach and finds that the per capita cost was $155.6 for malicious and criminal attacks, $128.1 for system glitches and $125.8 for human errors.

Neither are professionals always reasonable as the prudent person theory suggests. Psychological accounting, behavioral biases and other human behavioral factors can cause them to deviate from other rational decision-making. Professionals could overestimate the probability of a successful cyber-attack or underestimate its financial impact (de Smidt and Botzen 2017). Presence of such behavioral traits would then explain some of the reluctance of organizations to consume cyber insurance. de Smidt and Botzen also find that the availability of information influences risk perception and there is a positive correlation between the use of information sources and the perceived possibility of a cyberattack.

The culture of an organization, which is manifested by a mix of values, decision styles and interactions between employees and others who have access to the organization, can affect the cybersecurity of the organization (Todade 2017). Cybersecurity is social, cultural and behavioral issues, measurement of which requires a different set of tools, such as simulation of employee behaviors, auditing and, where possible, data analytics. Use of stringent regulation governing data and privacy security at the government level is a risk control approach.

Finally, there is a tendency to treat all cyber loss exposures as “a single risk” rather than “risks” in the cyberspace. The more we examine the risk, the more it becomes clear that we are examining the cyber world of risk. Conversely, the majority of decision makers – professionals, consumers and governments –

23. Biener et al. (2015) also offer an extensive list of academic studies covering cyber security and insurance issues.

24. Examples of security risk measurement models that scientists use include but are not limited to the mean failure cost (cascade of linear) model, the automated risk and utility management (AURUM) model, the Bayesian defense graphs and architectural model and the single loss expectancy. See Rjaibi and Rabai (2015) for a description of these models.

25. It is noted that the sample for this survey was drawn from the client database of Aon Risk Solutions in the Netherlands. 172 out of 1,891 professionals in the sample responded to the survey.

26. The Human Impact Management for Information Security (HIMIS) can be an approach in this regard (Todade 2017).
seem to view cyber risk as a macro-level phenomenon or, as Hubbard and Seiersen (2016) note, treat the risk from a “global attack surface” perspective. They add that this macro-level phenomenon is driven by one of four causes – increasing users worldwide, a variety of users worldwide, growth in discovered and exploited vulnerabilities per user and per use, and organizations more interconnected – in which an earlier causer magnifies a later causer. Hence, we may assume that “attack surface and breach are correlated” and a big storm in cybersecurity breach today signals a bigger storm to come. Indeed, commercialization of cybercrime, along with interconnectivity and globalization, drives greater frequency and severity cyber incidents (Allianz 2015). Accordingly, we propose that the insurance industry develops a portfolio of coverages – rather than a coverage – for operations in the cyber world of risk along the side of their operations in the conventional physical world of risk.

Cyber Insurance Coverages

Data about cyber insurance consumption is available but still limited at this relatively early stage for market development. It is fast developing in Australia with the market premium volume around AUD 25 million. Cyber insurance became available in Canada from the late 1990s with a market premium of about CAD 21 million and a loss ratio of 25% in 2015. Europe’s cyber risk-bearing capacity is estimated to be greater than €366 million, with an additional capacity of €100 million from the London market (AXCO n.d.).

Table 3: Key Findings from Cyber Insurance (Market) Studies (Selected)

<table>
<thead>
<tr>
<th>Surveyor and Year</th>
<th>Method/Survey (Target Groups)</th>
<th>Key Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Willis Re (2017)</td>
<td>Silent Cyber Risk Outlook</td>
<td>• The mean of the risk factor of the “silent cyber loss” to property policies is 1.074 (that is, the likelihood of 1.074 cyber-related losses per 100 non-cyber-related losses)</td>
</tr>
</tbody>
</table>
| Romanosky et al. (2017) | Survey of insurance companies | • Less than expected variations in the listing of “coverage topics” but the variations more significant in the listing of “coverage exclusions”  
• Significant variations in premium rating methodologies |
| Aon (2017)          | Global Cyber Market Overview 2017 | • 59% of the premium revenues in the U.S. cyber insurance market are from financial transaction-driven entities; 17% from entities that store personal data and are exposed to operational risks; 17% from entities that store personal data only; and the balance of 8% from entities exposed to operational risk only.  
• Lloyd’s share of U.S. cyber insurance premiums at approximately 30% |
| OECD (2017b)        | OECD Survey 2016              | • The level of cyber risk is perceived “high” by insurers, reinsurers and intermediaries but “moderate” by insurance authorities. |
| NetDiligence (2016) | Cyber Claims Study 2016       | • During the 2013-2015 data year, 87% of insurance claims are from organizations with revenues less than $2 billion  
• Average number of records lost was 2.04 million (median at 1,339)  
• Average insurance claims paid was $495,000 (median at $49,000)  
• Average cost of breach was $665,000 (median at $60,000) |

Source: Author compilation

---

27 Scheier (2003) also contends that [cyber] risk is about the “likelihood of the threat and the seriousness of its successful attack.”

28 All financial institutions in Australia are recommended by the APRA to have appropriate cyber coverages.

29 Anderson (2016) adds that regulation in the field of information technology, especially cyber security, is “still fairly nascent.”
An estimated $100 billion was invested for cyber risk management worldwide in 2016 (Aon, 2017), of which $93.7 billion was for risk mitigation (for example, diagnostic/risk assessment and software/hardware solutions). The share of risk transfer cost was relatively small at $2.2 billion, comprising insurance premiums of $1.7 billion and reinsurance premiums of $0.4 billion. Table 3 offers key findings from selected studies about cyber insurance markets.

Quoting multiple sources, Aon (2017) presents that an estimated total of $1.5 billion of premiums in the U.S. includes the revenues from writing risks of SMEs ($282 million), mid-market companies ($649 million) and large corporations ($567 million). In terms of the company type, financial transaction-driven companies (in retail and wholesale, financial intermediation and business and hospitality services) contributed 59% (or $876 million) to the total premiums. Companies that store personal data and are exposed to operational risks (in healthcare and transportation) shared 17% (or $256 million) of the market, and those storing personal data only (in technology, telecommunications and media, education and professional services) with 17% (or $242 million). The balance of the 8% (or $126 million) of the premiums came from companies exposed to operational risk only (in manufacturing, utilities and energy). Aon reports that Lloyd’s share of U.S. cyber insurance premiums is approximately 30% (or $450 million) of the total premiums ($1.5 billion) in the U.S. market.

### Table 4: A Summary of the U.S. Cyber Insurance Market (2015-2016)

<table>
<thead>
<tr>
<th>Finding</th>
<th>Data Year 2015</th>
<th>Data Year 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Premium and Coverage</td>
<td>• The total cyber insurance premiums written in the admitted market was estimated at $1.784 billion, and those in the surplus market at $708 billion. See Figure 1 for a detailed distribution of premiums.</td>
<td>• The direct premiums of $1.3 billion written in 2016 comprise the revenues from writing stand-alone policies (67.9%) and the balance from endorsements.</td>
</tr>
<tr>
<td>Insurance Company</td>
<td>• 128 insurance companies (alternatively, 42 insurance groups) wrote stand-alone coverages for a total of $921 in direct premiums written in 2016. Their loss ratios range from 0% to 400%. The share of the market by the top 10 and top 20 companies was 67.8% and 84.4%, respectively.</td>
<td>• The top 20 insurers wrote $1.2 billion of direct premiums in 2016, of which 73.7% were on a stand-alone basis. The top 5 insurers generated 81% of their direct written premiums ($0.70 billion) from providing stand-alone coverages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The top 5 and the top 20 insurers experienced a loss ratio of 34.0% and 35.2%, respectively, in 2016.</td>
</tr>
<tr>
<td>Other</td>
<td>• A total of 708 companies reported that they offered cyber coverage via endorsements. However, only 356 of them could separate premiums for cyber risk and others ended up reporting no premiums for this risk coverage. For identity theft protection in personal lines, there were 21.4 million coverages in the form of endorsement as compared to 0.278 million stand-alone policies.</td>
<td>• Commercial general liability (CGL), business interruption and Directors’ &amp; Officers’ (D&amp;O) policies were most commonly used as the basis for the endorsement.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A possible shift observed from the endorsement basis to the stand-alone basis due in part to insurers’ attempt to minimize court rulings in favor of policyholders and to lower their exposure to litigation.</td>
</tr>
</tbody>
</table>

Source: The NAIC (2017), A.M. Best (2017), author compilation

---

30 Aon classifies SMEs as companies with sales/revenue below $100 million, mid-market companies with up to $1 billion and large companies with higher sales/revenues. The sources for this analysis include Advisen, Marsh, Bureau van Dijk and Aon placement data.
Cyber insurance is available as a stand-alone policy or endorsement in both admitted and surplus markets in the U.S. With the NAIC’s introduction of the *Cybersecurity and Identity Theft Insurance Coverage Supplement*, the U.S. began to generate comparatively detailed information from yearend 2015. We highlight the findings from the data in Table 4.

Cyber risk, in particular, changes so fast that any definition we attempt today may even become too thin for effective management of it tomorrow. It resides in the cyber world but causes damages in the physical world. There is no known standard or broadly quoted definition of “cyber risk” (OECD 2017b), which is a position that the IAIS (2016) takes. What we term elusively as cyber risk is in fact about the risks in the cyber world, and a graduation transition of our understanding in this regard is observed in the following definitions, with an emphasis in italic:

- “[Any] risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks” (CRO Forum 2014) to “the risk of doing business in the cyber [environment]” (CRO Forum 2016).
- “[Any] risk emerging from the use of information and communication technology that compromises the confidentiality, availability or integrity of data or services” (Geneva Association 2016).
- “[Any] risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems” (Institute of Risk Management, the U.K.).

---

31 The NAIC (2017a) reports a possible shift from the endorsement basis to the stand-alone basis due in part to insurers’ attempt to minimize court rulings in favor of policyholders and to lower their exposure to expensive litigation. Nonetheless, the stand-alone policy approach can help insurers improve their pricing and reserving and the insurance industry can contribute to refinement in understanding of risk aggregation and in risk modeling (AM Best 2017).

32 The supplement requires insurance companies writing cyber security on stand-alone policies to provide: number of claims, direct premiums, direct losses, expenses, defense & cost containment expenses, and number of policies in-force. The NAIC notes that data quality has limitations and not all companies have submitted accurate data for both years.

33 In contrast, the U.S. NAIC (2017), specifically its Cybersecurity Taskforce, defines “cyber risk” more or less as a mix of the causes of loss (for example, identity theft, introduction of malicious computer code, human error), potential damages (for example, damage to the firm’s reputation) and indirect expenses (for example, business interruption). As further discussed in this paper, this type of definition exhibits that there is a communication gap even within the insurance community.

34 https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/
• “[Any] risk of financial or physical loss, disruption of services, privacy violation, or damage to the
assets or reputation of an organization through either a failure of its information or technology
systems, or a malicious act affecting their information or technology systems” (Advisen 2017).

• “Cyber” short for the [world of cyberspace] which is an interactive domain composed of digital
networks for storage, modification, information communication and other uses” (Biener, Eling and
Wirfs 2015).35

The multiplicity of cyber causes of loss as well as the diversity of the resulting damages and injuries gives
a lesson that a mere application of the risk management techniques in the physical world – which are
designed commonly for well-defined, if not fixed, risks – is incomplete for the management of cyber risk.
Cyber insurance coverages should thus be designed to reflect this multiplicity nature of the risk. The
insurance industry must not be passive but proactive in offering cyber coverages. In fact, they must be
innovative!

Cyber risk is difficult to price and underwrite for several reasons. There is a lack of historical data,
particularly in the structure suitable for the insurance industry. There is a concentration/contagion risk in
the cyber insurance and reinsurance market. There is a divergence in product coverage offering and a
lack of standardization in the coverages may not effectively induce cyber insurance consumption. Lack of
standardization could lead to coverage disputes and litigation, which may result in low insurance
consumption and even trigger a rise in the utilization of captives and other alternative risk transfers
(Freedman and Thomas 2017). Another study supports this view: only 19% of brokers and 30% of
underwriters answered that there is a common language in the cyber insurance market (Filkins 2016b). A
study by Romanosky et al. (2017) also indicates that the variations in premium rating methodologies in
the cyber insurance market are substantial, for example, 2 to 21 factors for base rating and 1-15 factors
for security rating.

The presence of conceptual gaps between the cybersecurity community and the cyber insurance
community often makes it difficult for the members to find a common basis for the development of
reasonable standards of security and insurability (Filkins 2016a). In a later study, he names four specific
areas of disagreement which actually pinpoint the problems in the cyber insurance market today (Filkins
2016b):

• The professionals in these two communities do not speak the same language risk definition and
quantification, thus leading to “different expectations, actions and justification for outcomes.”

• There is a need for agreeing on some minimum transparent standards for a risk management
framework that bridges the concerns of the communities.

• There is a communication gap. Without communication to the stakeholders in the other community,
the business decisions for insurance purchase may cause the coverage to fall short of, or exceed, the
expectation. (We add that there is likely a communication gap internal to the organization, for
example, between the Chief Risk Officer and the Chief Information Security Officer because they tend
to analyze cyber risk from their own professional society’s perspective.)

• The insurance community may not always be transparent in how they establish underwriting and
pricing criteria, whereas the buyers and their intermediaries need the information to estimate the
return on investment in cyber coverage financing.

35 Following the Solvency II convention, they classify cyber risk into four groups: actions of people, systems &
technology failures, failed internal processes, and external events.
The Insurance Market in Transition

The remaining part of this section further discusses and evaluates the responses of the insurance industry to the demand for cyber risk coverages. The discussion is U.S. centric unless otherwise noted.

Throughout the modern history of insurance, the industry has exhibited a few patterns in the initial response to new risk – for example, non-applicability of the risk to insurance coverage (including seeking advice from the civil court) and an extension of coverage due to silence in policies. The initial response is typically followed by a transitional period for a market-wide consensus or standardization of the risk coverage. The trend in today’s cyber risk underwriting some resemblance to the market response after the September 11 terrorist attacks. The then convention treated terrorism as part of the “riot, strike and civil commotion” family of risk.36 The 2001 attacks changed this view, causing the market to enter to a transitional period. Terrorism is now excluded explicitly from standard policies and insurers may offer terrorism-specific coverage by law or voluntarily. The market response to cyber risk resembles, certainly not identically, the response to terrorism or other critical risks. However, the market solution for cyber risk must be different and innovative because it is about a family of risks. We examine this matter, based mainly on the U.S. market environment.

Some conventional insurance policies explicitly cover losses resulting from cyber incidents, subject to strict restrictions on the coverage scope and limit. Some other policies clearly exclude cyber incidents – a trend we observe in the markets globally. Other policies are not so explicit regarding such coverage or are “silent” about excluding specific cyber causes of losses. A policy being silent about cyber risk implies that the insurer probably did not factor in the risk for pricing the coverage.37

Some indication about the perception of silent cyber losses can be found from the survey by Willis Re (2017) of 750 leaders and experts affiliated with 70 insurance companies or so. They find that the mean of the risk factor for such losses to property policies at 1.074 (meaning that the likelihood of 1.01 cyber-related losses per 100 non-cyber-related losses). The mean was almost same in other liability lines of insurance. However, more than 75% of the respondents estimated the risk factor as 1.01 or less in automobile liability and workers’ compensation lines. These findings evidence that lack of credible, industry-wide data may even hinder the players in the insurance market from reaching a consensus.

The Council of Insurance Agents and Brokers (CIAB) finds from its October 2016 survey that 55% of the respondent brokers answered that there is not enough clarity about cyber risk coverages. A survey by Hanover Research and the Insurance Services Office (now a Verisk) presents that underwriters value most the following four criteria in assessing cyber risk: enterprise risk management policy, nature of records or data stored, security tests and audits, and updated network security/firewall.

It is the view of the court and the industry that there is limited coverage we can extract from traditional insurance policies.38 Commercial property insurance generally does not cover “electronic data” unless

36 A few countries had a terrorism insurance program prior to the 2001 attacks. Spain established el Consorcio de Compensacion de Seguros (CCS) in 1941 (restructured in 1991) and Israel created the Compensation Fund (specifically to assist victims of war and terrorism) in 1941 (OECD c.2016).

37 At the time of writing, the Prudential Regulation Authority (PRA) of the U.K. attempts to define “cyber insurance underwriting risk” as the losses insurance and reinsurance companies are exposed to resulting from malicious acts (for example, cyber-attack and infection of an IT system with malicious code) and non-malicious acts (for example, loss of data, accidental acts or omissions) involving both tangible and intangible assets (Prudential Regulation Authority 2017).

38 A number of studies review the legal perspectives of insurance policy applicability to first-party and liability claims arising from cyber events, for example: Gummow and Devillling (2017), Schmitt (2017), McNicholas and Mohan (2015), Jones and Yellen (2015) and Mormino and Kreiling (2014).
otherwise provided via additional coverage.\textsuperscript{39} The electronic data is not tangible, thus not considered as a type of property under the “physical damage to tangible property coverage.”\textsuperscript{3}

Claims are made regarding the possible extension of the business interruption – also known as the loss of income – endorsement to damages and injuries resulting from cyberattacks. Often, cyberattacks are made not to destroy data (Cellerini, et al. 2016). An attack would be to transmit data illegally to an unauthorized organization or for sale on the dark web or to extort money from an organization by blocking its access to the data. If a property is not damaged or destroyed, then the business interruption coverage is unlikely triggered because the loss of income and extra expenses must be consequential to a damage to an insured property. Exceptions to this argument can be made, for example, when the cyberattack has resulted in a power outage.\textsuperscript{40}

Generally, CGL’s coverage for “physical damage to tangible property” is applied stringently such that the property must be tangible. The coverage for “personal or advertising injury” is thus unlikely to apply to cases of data breaches unless privacy is violated. In sum, CGL does not cover the loss of data, loss of use of data, damage to data or inability to access data (Mormino and Kreiling 2014).\textsuperscript{41}

Directors’ & Officers’ (D&O) liability insurance leaves some room for coverage in part because of the expansion of definitions of the breach of fiduciary duty and corporate mismanagement in the U.S. The claimant, however, needs to prove that there was a breach of the prudence rule, trust or duty in the cyber attacked organization. At the same time, conventional policies commonly exclude coverage for cyber risk through an addendum or a clarification letter to the policyholder, a trend we increasingly observe in insurance markets globally.\textsuperscript{42} Other potentially applicable coverages from conventional insurance may include workers’ compensation for the bodily injury, kidnap & ransom insurance if we can apply kidnapping to data, crime and fidelity for financial theft and fraud. Figure 2 depicts full-scale cyber risk coverages overlaid on conventional insurance coverages.

The industry will continue its development of cyber policies while restricting “silent” coverages in other policies (Stroz Friedberg 2018). The industry, inclusive of the reinsurancen industry, will also need to better understand “correlated and systemic” cyber perils that could accumulate across industries and borders. Finally, management of both physical and cyber risks at the enterprise level – that is, the application of the enterprise risk management concept – will be a requisite for effective investment in cybersecurity measures and cyber insurance. Small and mid-sized enterprises (SMEs) will also need to invest more in cybersecurity management; otherwise, an attack on an SME could extend to the network of large organizations and result in catastrophic losses.

\textsuperscript{39} Company-wide variations exist, particularly in the case of manuscript policies.

\textsuperscript{40} Lloyd’s and University of Cambridge (2015) conducted a Business Blackout simulation using the US power grid infrastructure. They find that the damages could be as high as $120 billion, which would fit a catastrophic loss case with a benchmark return period of 1:1200.

\textsuperscript{41} A typical CGL policy has three main types of coverages: Coverage A to protect the insured from its liability for bodily injury and property damage it causes to the third party; Coverage B to protect the insured from its liability for personal and advertising injury; and Coverage C for medical payments to third parties regardless of the liability of the insured.

\textsuperscript{42} The Insurance Services Office in the U.S. has issued a series of exclusion endorsements, such as: \textit{Exclusion – Access or Disclosure of Confidential or Personal Information and Data-related Liability – Limited Bodily Injury Exception Not Included} (CG 21 07 05 14); and \textit{Exclusion – Access or Disclosure of Confidential or Personal Information (Coverage B Only)} (CG 21 08 05 14). The \textit{Institute Cyber Attack Exclusion Clause} (CL 380), introduced in 2003 by Lloyd’s and the International Underwriting Association, prescribes that “in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software [program], malicious code, computer virus or process or any other electronic system.”
A concern arises regarding, at least in theory, the possibility of a catastrophic loss to a community as a result of a cyberattack. If it were by a non-governmental organization largely to instigate fear to the members of the community, thereby letting victims eligible for terrorism insurance coverage. If, however, the attacker is a state or state-sponsored agency, the attack could be an outcome of a warlike operation, which is not a subject of insurance in the private market because the insurance industry is by default an element of the nation and its economy. Separately, the consensus is that "data is intangible" and "the object does not include data." The OECD (2017b) notes that cyberattacks are specifically excluded from the definition of terrorism event in Australia, Germany, Russia and the U.K. Terrorism insurance programs in France and Spain cover physical damages resulting from cyberattacks, and the program in Spain additionally covers bodily injury and probably data software loss.

43 U.S. state departments adopted to add “cyber liability” as a subline of insurance under “other liability” in the property/casualty insurer’s financial statements, thus making stand-alone cyber insurance policies qualified for the Terrorism Risk Insurance Program (U.S. Department of Treasury 2016).

44 Exceptions exist, such as ocean marine insurance in which policies commonly contain a war risk coverage clause.

45 Different views exist. For example, Vitkowsky (2017) contends that a damage to an essential civilian database such as social security data and tax records should be treated as an attack.
Communication, Coordination and Standardization

Figure 2 is a schematic presentation of the common cyber coverages under the stand-alone policy or as an endorsement. It depicts the common view of the industry that a single coverage approach is suitable to finance cyber risk. The stand-alone policy, in particular, represents the industry’s response to the exclusions of cyber-related losses from property (including business interruption), casualty and liability lines of business. The OECD (2017a) reports that the development of this single stand-alone policy approach is designed to close the gaps created by the exclusions and to cover some of the main losses resulting from privacy breaches, cyberattacks and cyber fraud. Accordingly, the area for cyber insurance in Figure 2 is a collection of gaps or better presents a cyber world of insurance being evolved. The remaining part of this section examines the key requisites for effective insurance operations in the fully-blown cyber market.

The OECD (2017b) reviewed a total of 28 stand-alone policies to find out the following distribution of loss exposure coverages (regrouped for this study purpose):

- Found in at least 80% of the policies – cyber ransom & extortion; network security failure liability; communication & media liability; business interruption; data and software loss; breach of privacy compensation; fines & penalties; regulatory & legal defense costs; and incident report costs.
- Found in less than 50% of the policies – financial theft & fraud; reputational damage; intellectual property theft; physical asset damage; and bodily injury.

This report quotes several conclusions from other studies, for example: stand-alone policies “vary significantly across providers” in the market; and the U.S. market has “at least 65 different policy forms in use” for cyber coverages. Product differentiation, on the one hand, may indicate that the market is competitive and consumers can approach the risk underwriter of their preference. On the other hand, there is a concern whether consumers can effectively differentiate the products. Consumers even may not be aware of the availability of a specific coverage in cyber insurance (OECD 2017b). A recent study by Romanosky et al. (2017) also indicate that the variations in the listing of “policy exclusions.” They needed to analyze 12 insurance policies to capture all exclusions, while they could identify all “coverage topics” from analyzing 5 policies.

In practice, no market is known to be perfect due to the presence of one or more problems of information asymmetry, externalities and market power, thus failing to provide a socially optimal level of security. Indeed, “bad incentives” are likely to cause system failures as frequently as “bad designs” do (Anderson and Moore 2006). Externalities are certainly an issue. The dominance of a particular operating system can not only induce network security externalities positively and negatively but may also create free riders. Unless proper regulation and monitoring systems are in place, the interconnectedness of

---

46 The OECD (2017a) reports that these exclusions can be grouped into three types: general exclusions of all losses resulting from cyber incidents; an exclusion of general liability in relation to data breaches; and an exclusion of losses related to data restoration.

47 For the cyber security market, Kopp et al. (2017) add misaligned incentives, coordination failures and risk concentration as the additional sources of the problems.

48 A corresponding view from the cyber insurance perspective presents that cyber insurance results in higher security investment, facilitates best practice standards (because insurers seek cyber security benchmarks for underwriting), and generates higher overall societal welfare by redressing the outcomes of IT security market failures (Kesan, Majuca and Yurcik 2004).

49 Examples of positive externalities include that each member of the community enjoys the rising value of the system and that the investment in cyber security by one player induces the investment by all other players in the community. An example of a negative externality could be the lack of investment by one player affecting the security of other players in the community. If an investment by one player results in the discouragement of another or other players, we may observe problems of free riders.
operations – alternatively, “interdependent security risk” (Kunreuther and Heal 2003) – in the cyber world is poised to inflate moral hazard problems in the physical community.

As an integral element of the market, cyber insurance must deal with problems of adverse selection, which are caused also by information asymmetry in the market. The amount of the information that is relevant to pricing the risk and available to the insurer prior to policy inception affects the quality of underwriting, thus the financial and operational soundness of the insurer. Given that the data availability and quality is still an issue, cyber insurance companies need to pay close attention to this problem of adverse selection. As alluded to above, problems of moral hazard deal mainly with the changes in insureds’ behavior regarding – or their lack of incentives to lessen – the probability of loss when they are covered by cyber insurance (ENISA 2012).

### Table 5: Cross-industry Comparison of Cyber Loss Exposure Classification

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Interruption (BI) of operations</td>
<td>Business interruption</td>
<td>Business interruption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contingent BI for non-physical damage</td>
<td>Dependent business interruption</td>
<td></td>
<td>Contingent business interruption</td>
<td></td>
</tr>
<tr>
<td>Data and software loss</td>
<td>Data breach/restoration</td>
<td>Data and software loss</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial theft and/or fraud</td>
<td>Fund transfer fraud/social engineering</td>
<td>Financial theft and fraud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber ransom and extortion</td>
<td>Cyber extortion</td>
<td>Cyber ransom and extortion</td>
<td>Cyber extortion</td>
<td></td>
</tr>
<tr>
<td>Intellectual property theft</td>
<td>Intellectual property theft</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident response costs</td>
<td>Incident response costs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breach of privacy</td>
<td>Breach of privacy compensation</td>
<td>Breach of privacy compensation</td>
<td>Privacy breaches</td>
<td></td>
</tr>
<tr>
<td>Network security/security failure (liability)</td>
<td>System failure</td>
<td>Network security failure</td>
<td>Network, IT security failure/ network liability</td>
<td></td>
</tr>
<tr>
<td>Reputational damage (excluding legal protection)</td>
<td>Reputational damage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory &amp; legal defense costs (excluding fines and penalties)</td>
<td>Regulatory fines &amp; penalties</td>
<td>Regulatory &amp; legal defense cost</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fine and penalties</td>
<td>Fine and penalties</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication and media</td>
<td>Internet media</td>
<td>Communication and media</td>
<td>Media</td>
<td></td>
</tr>
<tr>
<td>Legal protection – lawyer fees</td>
<td>Regulatory &amp; legal defense</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assistance coverage – psychological support</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Products (liability)</td>
<td>D&amp;O</td>
<td>E&amp;O</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| D&O                                                   | T
| Tech E&O                                             | Professional services E&O, Professional indemnity | E&O |               |
| Environmental damage                                  |                                      |                                      |               |                 |
| Physical asset damage                                 | Property damage | Physical asset damage |               |                 |
| Bodily injury and death                               | Bodily injury | Bodily injury |               |                 |

* This OECD report also contains the list for CRO Forum (2016).
** The classification is derived from its annual surveys, which has an “other” category.
We find some evidence by comparing the cyber loss exposure classifications by selected organizations. Loosely, the organizations in the table represent the risk management industry, the intergovernmental group, a database organization and the insurance industry. The listing in Table 5 begins with the classification by the CRO Forum, a group of risk management professionals in the insurance industry. The forum’s listing is most extensive of all organizations in the table and represents the need for cyber insurance coverage by risk management professionals. The Advisen-PartnerRe’s listing (from their surveys in 2016 and 2017) is a mix of the demand for and supply of cyber insurance coverages because their survey population includes both buyers and sellers in the cyber insurance market. The OECD’s listing is based on their analysis of dozens of insurance policies. Finally, the Swiss Re’s listing is from the reinsurance’s study in 2017.

The four classifications indicate that there is a meaningful harmony when it comes to dissecting cyber risks for risk management or insurance purposes. At the same time, it demonstrates that there is a need for communication improvement to minimize the gaps between the consumers and suppliers in the cyber insurance market. Corporate clients that wish for an insurance protection against a range or cyber risks but may not be able to locate the corresponding coverages unless there is a clear communication channel with their insurance underwriters. Swiss Re (2016) finds that organizations that rank cyber as a critical risk are likely to consume twice more cyber coverages than those that do not. However, consumption of cyber insurance policies remains lower than expected due probably to the “illusion of protection” from conventional property and liability policies or “lack of clarity” in the applications of the policies to cyber risks. Swiss Re notes that those organizations without a specific cyber policy have not examined the coverages (main reason) or prefer self-insurance.

A 2017 Survey of Cyber Insurance Underwriters

Diversity in policy forms is a common tool that companies use to differentiate their products from competitors in a market economy. Excessive diversity, however, could confuse consumers, create a new kind of knowledge gap in coverages and may make lead to disputes in claims and litigation (Freedman and Thomas 2017). Insurance intermediaries can be confused in a market in which risk underwriters offer their own version of policy forms. Diversity, desirably within a reasonable boundary, in policy wording is also expected.

We conducted a short survey with two specific objectives. One is to assess the cyber market environment broadly, and the other to compare policy wordings (particularly, definitions) in cyber coverages. Using several resources, we identified a total of 38 target companies which include a number of leading cyber risk writers in the primary market, niche-segment writers (for example, law professionals), reinsurers and intermediaries. The survey was disseminated via email to the lead underwriters in mid-2017 and we secured 32 valid responses. We did not collect data other than sample policies that several respondents

---

50 Small to mid-sized organizations may value risk management services equally to the risk coverage services that their insurers provide. Nonetheless, coverage affordability still matters to them.

51 Advisen and PartnerRe (2016, 2017) survey findings indicate that 38% and 62% respondent-insurance intermediaries in the 2016 and 2017 surveys, respectively, observe convergence in cyber insurance coverages but still experience difficulties in comparing policies.

52 The sources include but are not limited to several cyber risk/insurance conference participants and the 2015 participants of the survey by the American Bar Association (2016). The lists are merged for refinement for this survey purpose also for identification of a lead underwriter in each of the companies.

opted to submit in lieu of answers to the questions about policy wording. Below is the summary of the findings and short-answer responses from this survey.

- It seems *flexibility* in offering a combination of coverages (for example, social engineering option) and coverage limits is the benefit to the insurer and their clients from arranging stand-alone policies.
- Mixed views are observed regarding whether or not convergence in coverage limit and scope is observed. A number of respondents express that there seems some convergence, albeit slowly, when it comes to listing coverage types or finding common exclusions, which is in line with a conclusion by Romanosky et al. (2017), and offering a high limit of insurance (particularly among leading insurers with large underwriting capacity).

When it comes to the policy forms and apparently policy wording, many respondents – particularly those in brokerage and reinsurance – express that there is not enough convergence and the market needs standardization of the forms. The market seems to become more competitive, consequently leading to wide differences in premium rates.

Many respondents view that government intervention is redundant at this early stage of market development while noting the probable benefit of the U.S. Treasury Department’s addition of stand-alone cyber insurance to the TRIP. Others express the need for standardization of the breach notification laws (across the U.S. states) or the expansion of the companies subject to the laws.\(^{54}\)

- Many respondents view that government intervention is redundant at this early stage of market development while noting the probable benefit of the U.S. Treasury Department’s addition of stand-alone cyber insurance to the TRIP. Others express the need for standardization of the breach notification laws (across the U.S. states) or the expansion of the companies subject to the laws.\(^{55}\)
- Consumer education, improvement in the industry’s understanding of the magnitude of cyber risk, higher underwriting capacity, adaption to the rapidly growing market, innovation in product design and aggregation of quality data are also the views we observe in survey responses.

Given that there is no standard definition of “cyber risk” as noted earlier in this report, we are interested whether there is a kind of language common in insurance policies. For this, we have examined critical definitions in the “definitions section” of sample stand-alone policies from leading insurance companies.\(^{56}\)

The examination is limited in scope to selected definitions relevant to cyber risk, rather than the insuring agreements by each specific coverage.

---

\(^{54}\) We note that there is a significant amount of commonalities in the compliance regulation among almost all the U.S. state laws. Nonetheless, the regulated entity still needs to prepare the compliance work for each individual state.

\(^{55}\) We note that there is a significant amount of commonalities in the compliance regulation among almost all the U.S. state laws. Nonetheless, the regulated entity still needs to prepare the compliance work for each individual state.

\(^{56}\) We note that an insurance company may offer several versions of cyber insurance policies. We have selected the one that the survey respondent submitted, where possible, or that the company markets in its website.
<table>
<thead>
<tr>
<th>Definition</th>
<th>Insurer A</th>
<th>Insurer B</th>
<th>Insurer C</th>
<th>Insurer D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer System</td>
<td>[Computer network] a connected network of computer hardware, software, and any associated components leased, owned, operated or controlled by the Company</td>
<td>[Computer] a device or group of devices that by manipulation of electronic, magnetic, optical or electromechanical impulses pursuant to a computer program can perform operations on Data.</td>
<td>[System] a Computer; and (A) any input, output, processing, storage and communication devices controlled, supervised or accessed by the operating systems that are proprietary to, or licensed to, the owner of the Computer; and (B) Media</td>
<td>[Computer system] any information technology or operational technology</td>
</tr>
<tr>
<td>Cyberattack</td>
<td>[Breach] the failure of the Insured or others on behalf of the Insured to prevent or protect against the following: 1. the disclosure of Confidential Information by an Insured or a third party for whom the Insured is legally responsible; 2. unauthorized access to the Computer Network; 3. unauthorized use of the Computer Network in a denial of service (DoS) attack directed against a third party; 5. transmission of malicious code from the Computer Network causing harm to a third party; 6. denial of access to Computer Network; 7. physical theft of hardware on which data is stored; or 8. the failure to disclose the aforementioned in violation of Privacy Breach Notice Law</td>
<td>[Cyberattack] the transmission of fraudulent or unauthorized Data that is designed to modify, alter, damage, destroy, delete, record or transmit information within a System without authorization, including Data that is self-replicating or self-propagating and is designed to contaminate other computer programs or legitimate computer Data, consume computer resources or in some fashion usurp the normal operation of a System</td>
<td>[Denial-of-service attack] a malicious attack by a third party which is designed to slow or completely interrupt access to a targeted computer system or website by other third parties authorized to gain access to that computer system or website</td>
<td>[Denial-of-service attack] a malicious attack by a third party which is designed to slow or completely interrupt access to a targeted computer system or website by other third parties authorized to gain access to that computer system or website</td>
</tr>
<tr>
<td>Data</td>
<td>[Electronic data] any data stored electronically on a Computer Network, including Confidential Information</td>
<td>[Data] a representation of information, knowledge, facts, concepts, or instructions which are being processed or have been processed in a Computer</td>
<td>[Electronic data] information that exists in electronic form, including Personal Information; provided, however, [it] does not include Software.</td>
<td>[Data] Any electronic information or record of a form readily usable or readable by a Computer Program</td>
</tr>
<tr>
<td>Digital assets</td>
<td>[Electronic content] digital media including advertising and promotional material that is published, disseminated, released, gathered, distributed or transmitted in electronic or digital format on behalf of the Insured or by the Insured for themselves or for others, Electronic Content shall not include: 1. computer software except to the extent that it displays digital content; or 2. any actual products or services described, illustrated or displayed in such Electronic Content.</td>
<td>[Digital assets] electronic data, software, audio files, and image files stored on the company’s computer system, and the capacity of such computer system. Digital assets do not include accounts, bills, evidences of debts, money, valuable papers, records, abstracts, deeds, manuscripts or other documents, except if they have been converted to electronic data, and then only in that form</td>
<td>[Media content] any information, including words, sounds, numbers, images or graphics and shall include advertising, video, streaming content, webcasting, online forums, bulletin board and chatroom contents, in any format, but does not include computer software or the actual goods, products, or services disabled,</td>
<td></td>
</tr>
<tr>
<td>Definition</td>
<td>Insurer A</td>
<td>Insurer B</td>
<td>Insurer C</td>
<td>Insurer D</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cyber activity/Network</td>
<td>[Cyber activity] the electronic display, electronic transmission, or electronic dissemination of information through a Network or through an Insured’s System</td>
<td>[Network] any services provided by or through the facilities of any electronic or computer communication system, including any shared networks, Internet access facilities, or other similar facilities for such systems, in which an Insured participates, allowing the input, output, examination, or transfer of Data or programs from one computer to an Insured’s Computer</td>
<td>[Network security] the use of hardware, software, firmware and written security policies and procedures by insureds, or by others on behalf of the company, to protect against unauthorized access to or the unauthorized use of the company’s computer system including the use of the company’s computer system in a denial of service attack</td>
<td>Illustrated or displayed in such media content</td>
</tr>
<tr>
<td>Security failure/threat</td>
<td>[Threat] …access to an Insured’s System and intends to: (A) cause an Insured to transfer, pay or deliver any funds or property using an Insured’s System; (B) sell or disclose a Record to another natural person or to an entity; (C) alter, damage or destroy an Insured’s Data while stored within an Insured’s System; (D) alter, damage, or destroy an Insured’s Data through a Cyber-attack; or (E) impair or deny an Insured’s Services, where there exists a demand for an extortion payment or a series of such payments as condition for the mitigation or removal of such Threat</td>
<td>[Privacy event] (A) an unauthorized disclosure or loss of: (A1) personal information in the care, custody or control of any insured or service provider; or (A2) corporate information in the care, custody or control of any insured or service provider that is specifically identified as confidential and protected under a nondisclosure agreement or similar contract; or (B) a violation of any privacy regulation</td>
<td>[Security event] security event means any unauthorized access to, unauthorized use of, introduction of malicious code into, or denial of service attack upon, the company’s computer system, that results in: (A) an interruption of service; or (B) the alteration, corruption or destruction of digital assets or other corporate information in the care, custody or control of any insured that is specifically identified as confidential and protected under a nondisclosure agreement or similar contract</td>
<td></td>
</tr>
<tr>
<td>Other terms defined (selected)</td>
<td>Extortion threat; Rogue employee; Cyberterrorism</td>
<td>E-threat expenses, E-vandalism expenses, Crisis management expenses, Record</td>
<td>Extortion expenses</td>
<td>Outsourced service provider, E-discovery consultant services, Cyberterrorism</td>
</tr>
</tbody>
</table>

*Note: The definitions in this table are actual quotations — a few with some minor style modifications — from the policy.*
As Table 6 shows, there are not only differences in the keywords for the definitions but also disparities in the breadth of definitions within each group. For example, Insurer D defines “computer” simply as “any information technology or operational technology.” By comparison, Insurer C defines “computer” separately from “system” while other insurers define “computer network” or “computer system.”

In the four sample policies and in several other non-quoted policies, we find two kinds of definitions for data. One group defines simply “data” and the other “electronic data,” all with a varying depth for the definition. Similar observations are made in, for example, the cyberattack group (breach, cyberattack and denial-of-attack) and the digital asset group (electronic content, digital assets, media content). Incidentally, Insurers C and D have adopted the exact same definition for “denial-of-service attack.”

Standardization is critical not only to help the cyber insurance market further developed. It is equally important to other stakeholders. Consumers need a guideline for comparison of policies and consumption of the coverages right in scope and limit. Organizations of all sizes need coordination with risk managers, risk underwriters and IT experts for effective control and financing of their cyber loss exposures. Standardization is critical for governments to properly promote cyber risk management and insurance within their domestic economies and cross border.

The standardization in this context never implies uniformity of coverages in the cyber insurance market. It means a common frame of market infrastructure that can induce a reasonable degree of comparability of coverage scopes and limits, premium charges and key ancillary services while preserving competitiveness in the market.

We propose two requisites for such standardization in the cyber insurance market. One is standardization in data collection and use, and the other standardization of insurance coverages. The former is challenging as the world of cyber risk is at its infancy. Standardization of the data collection process is, nevertheless, possible and some attempts are already in progress. With the support from the industry and statistical agencies, University of Cambridge (2016) has been developing the Cyber Exposure Data Schema since early 2016.57

Regulation and Self-regulation

The importance of data sharing is recognized in the risk management and insurance community but only limited legislation exists that requires such sharing between the insurance and other industries. Swiss Re (2016) notes that the role of government in introducing laws regarding data sharing and potentially mandating it is complex and could make the cyber risk environment more complicated.

Governments exist to operationalize the collective will of their citizens – at least in theory. In general, democracies should be better at reflecting societal will, including those decisions relating to risk management, than are other forms of government. In economic terms, a democracy should have fewer principal (citizens) - agent (government) problems, at least in the long run.

In a market economy, government intervention should be limited to those circumstances for which market outcomes are, for some reason, unacceptable. This principle applies to all activities, including those relating to societal risk management. Thus, many aspects of societal risk management are best left to individuals and businesses. The government, however, has a critically important role when market outcomes are hindered by imperfections or fail societal notions of fairness. The ultimate objective of such government intervention is to influence health, safety, and environmental outcomes.

The insurance industry may fail to offer a socially optimal level of security owing to several reasons we find in the cyber world.58 First, there are problems of information asymmetries due to the complexity in structure and the presence of anonymous activities on the Internet. Second, there are

57 This project aims at establishing standardized categories for exposure segmentation for efficiency in reporting and monitoring of cyber loss exposures.

58 These points are drawn from Kopp et al. (2017).
problems of externalities in the cyber world as well, such that one firm’s behavior (for example, investment in cybersecurity) effects the net risk borne by other firms in the chain of service. Despite the potential being positive, these externalities may induce free riders and underinvestment.\textsuperscript{59} Third, there are issues of scale economies and market entry barriers in the cybersecurity market. Finally, insurance provision, currently by a relatively small number of underwriters, may even bring about concentration risk.

In a competitive market, we deem government intervention for economic purposes desirable only if all of the following three conditions exist: (1) actual or potential market imperfections exist; (2) the market imperfections do or could lead to meaningful economic inefficiency or inequity; and (3) government action can ameliorate the inefficiency or inequity. Conversely, if at least one of the three conditions is not met, no government intervention is warranted. Thus, no intervention is justified in financial service markets that exhibit no market imperfections or where imperfections exist but they do not lead to important inefficiencies or inequities. Even if market imperfections exist and they are judged to be meaningful, no intervention is justified if government’s actions could not ameliorate the imperfection.

After all, there is no guarantee that government intervention will be successful (or that government’s assessment of the imperfection is accurate). Indeed, government intervention can make matters worse. Sometimes, the best governmental reaction is no action, even for inefficient markets. Even if all three of the above conditions are met, the government still may “get it wrong” for various reasons. Just as there is no perfect competition, there is no perfect regulation. Just as market failures exist, so do government failures. And, the government is also a new student in this cyber world of risk.

The Business of Insurance in Transition to the Cyber-Physical World of Risk

Cyber risk modeling is challenging. So is cyber risk underwriting. Aggregation of quality data and underwriting experience, let alone finding experts — is challenging. There is no geographical limitation, unlike the cases of natural catastrophes, when it comes to the origin of cyberattacks. And the world is getting interconnected.

A new risk can be added as a newly covered peril to the standard policy. We have done so on numerous occasions in the past, via which a single-risk policy has been transformed into a multi-peril policy. For each occasion, we must ask if the decision is fair to all insureds in the risk pool. Generally, a standard policy is designed for the general public and covers the loss exposures typical to the majority of the insureds in the risk pool. In other words, any loss exposure to which only a few in the pool are exposed can be, and should be, carved out from the standard policy. The carved-out can become a stand-alone policy or as an endorsement with an additional premium charge. Preservation of this practice can make the standard coverage available and affordable to a reliable degree.

Cyber risks evolve. So do our minds and thoughts about restructuring our responses to protect policyholders against the risks. The norm today is offering cyber risk coverages separately from the conventional coverages and using more of stand-alone coverages. This single policy approach may be a short-term solution because the industry must also deal with risks arising from the use of artificial intelligence, machine learning-based technology in the interconnected cyberspace. What we foresee is the operation of insurance in two concurrent worlds of risks – a physical world and a cyber world.

The insurance industry might be too eager to commoditize cyber risk, yet without fully understanding the shape it will take in the near future. Today’s surplus-rich industry might be moving too fast to the cyber risk market as an attempt to generate better underwriting leverage, yet without fully understanding the complicated nature of the cyber world of risk. The cyber world is expanding. It is adding artificial intelligence-based, machine learning elements and becomes more complex as existing and new elements are increasingly interconnected. This expansion will certainly add values to society. It will also change the nature of existing risks and add new risks, thus increasing the

\textsuperscript{59} Kopp et al. (2017) argue that the cyber market is serviced by a few dominant companies which provide “similar or indistinguishable products and services.” This study finds that the existing cyber insurance policies look similar but are very different in the breadth of coverages.
responsibility of the insurance industry for assisting individuals and organizations in the management of the risk. Accordingly, we need to build up an infrastructure to continue our operations in the physical-cyber world of risk.

References


AM Best. 2017. Cyber Line Expects to be One of the Leading P/C Growth Areas (June 22) (Best's Special Report). AM Best Company.


Swiss Re and IBM. 2016. *Cyber: In Search of Resilience in an Interconnected World (October)*. Zurich: Swiss Re and IBM Institute for Business Value.

Swiss Re. 2017. *Cyber: Getting to Grips with a Complex Risk (Sigma No. 1)*. Zurich: Swiss Re.

Swiss Re. 2014. *New Emerging Risk Insights (July)*. Zurich: Swiss Re.


