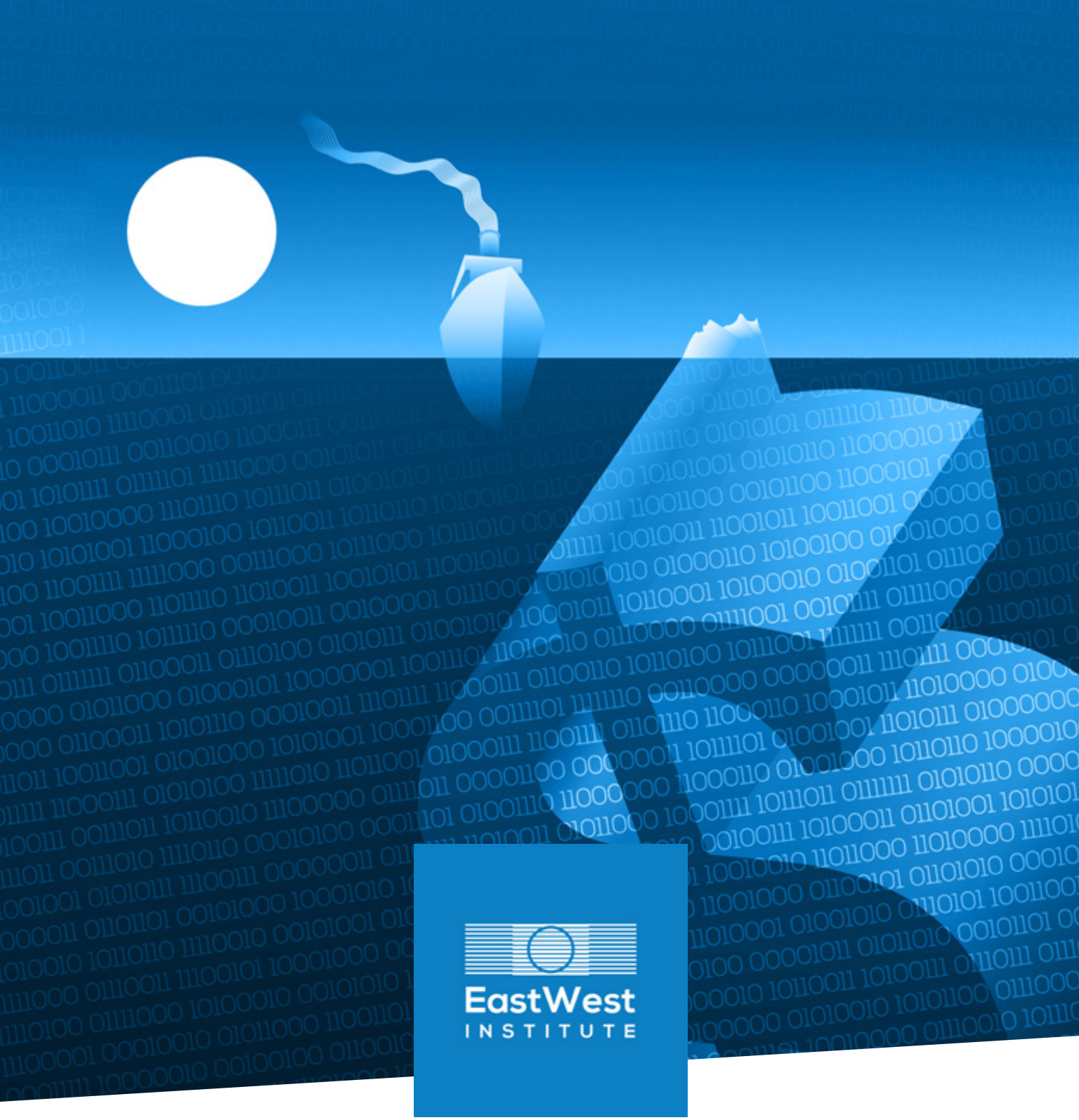


EastWest
INSTITUTE

Cyber Insurance and Systemic Market Risk

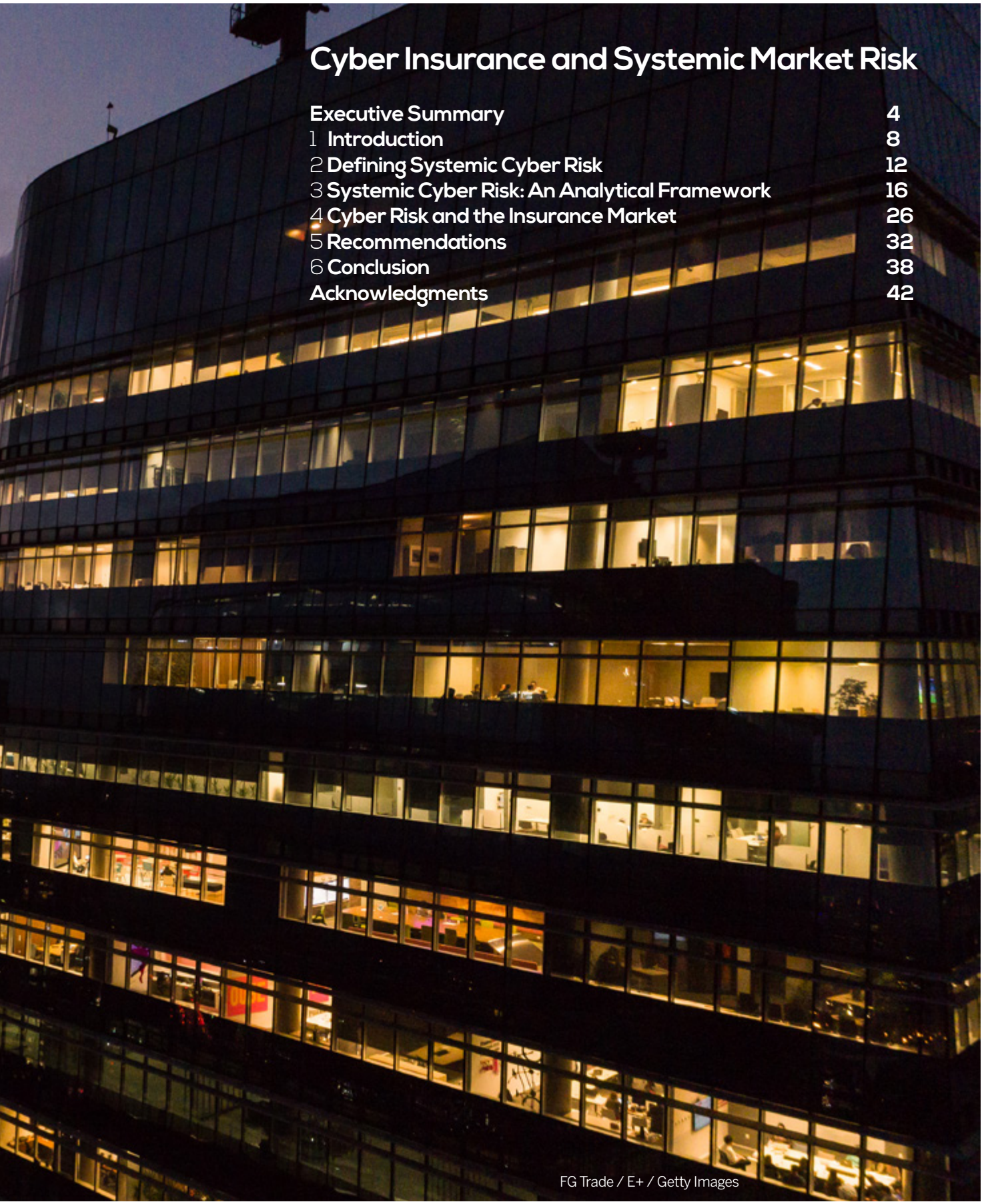
DATE:	EVENT:
June 2017	**NotPetya**
DAMAGE: **$10 billion**	A malware that encrypted hard drives and overwrote the master boot record, making the infected computers unusable.

Reported losses from NotPetya:

$870,000,000
Pharmaceutical company Merck
$400,000,000
Delivery company FedEx (through European subsidiary TNT Express)
$384,000,000
French construction company Saint-Gobain
$300,000,000
Danish shipping company Maersk
$188,000,000
Snack company Mondelez
$129,000,000
British manufacturer Reckitt Benckiser

$10 billion
Total damages from NotPetya, as estimated by the White House

Cyber Insurance and Systemic Market Risk



FG Trade / E+ / Getty Images

Executive Summary

The purpose of this report is to examine the systemic nature of cyber risks, particularly from the vantage point of the insurance industry as a central actor seeking to quantify these risks. It proposes several recommendations to help the market mature in a healthy, stable way that leads to increased cyber resilience and cybersecurity for all.

As advancements in technology enhance productivity, create new business models and spur economic growth, malicious actors also continue to innovate and improve, exploiting technology for criminal and geopolitical purposes. The increasing complexity and interdependency of the digital systems we all depend on also expand the potential for large-scale system failures.

In response to these risks, enterprises are improving their security, sharing information and enhancing their risk management practices. In addition, many are deciding to transfer some cyber risks by purchasing cyber insurance.

Insurance coverage for losses due to cyber incidents represents a principal area of growth for the insurance industry, with premiums projected to reach 7.5 billion USD by 2020. However, there is a shortage of rigorous tools to model and measure cyber risks, which are inherently complex, interconnected and forever changing with evolving technologies. Considering that the cyber insurance industry is still quite new and dynamic, there is concern about the insurance market's ability to absorb losses in the event of a catastrophic, systemic cyber incident.

The purpose of this report is to examine the systemic nature of cyber risks, particularly from the vantage point of the insurance industry as a central actor seeking to quantify these risks. The report offers a definition and framework to understand systemic cyber risk. It also aims to provide an overview of the current state of the cyber insurance market and proposes several recommendations to help the market mature in a healthy, stable way that leads to increased cyber resilience and cybersecurity for all.

A Systemic Cyber Risk Framework

In 2017, the NotPetya cyber attack spread from a Ukrainian accounting software to cripple global shipping, pharmaceutical, construction, energy and communications companies, food processors, hospitals, and even a chocolate factory. Damages from the attack may have reached 10 billion USD.[i] NotPetya is often cited as the worst cyber attack to date, and illustrates how the interconnectedness of cyber systems, along with advancements in designing attacks and cyber weapons, can put the global economy at risk. The effects of the attack were felt across multiple sectors, and cascaded downstream to impact even those who had not had their devices damaged by the NotPetya malware directly (e.g., businesses relying on deliveries of products that were stuck in ports controlled by a crippled shipping company). Given the catastrophic impact for some individual global companies and the hefty price tag, it is not difficult to imagine a scenario in which such an attack causes a global crisis, for example, if a large global bank or financial services firm were to be infected, halting global trading or causing a loss of confidence in the banks. That a cyber event can have such consequences, even removed from its initial target, illustrates the systemic nature of cyber risks that this report explores.

To begin, the report defines "systemic cyber risk" as:

> The potential for a cyber incident, event or shock to the digital ecosystem to cause broad-based disruption in information and communications technology services resulting in a loss of trust and capital. This breakdown will then cascade to other sectors of the economy, causing significant adverse effects to public health or safety, the economy or national security.

A determining characteristic of systemic cyber risk is the probability of "contagion," that is, effects that cascade across multiple sectors of the economy. Elements of contagion can be seen in NotPetya, described above, or in a hypothetical incident that begins in the energy sector, spreads to the transportation sector and produces damage in the financial sector, potentially having a significant impact on the global economy. There are two mechanisms through which damage from an incident can cascade across systems:

- **Common vulnerabilities** arise when the presence of a component or vulnerability is widespread throughout systems (e.g., a vulnerability that is present in every Linux system).
- **Concentrated dependencies** result from the widespread reliance on a single software, or small number of vendors or a critical platform (e.g., GPS, or single critical infrastructure providers). The effects of an attack on one of these critical platforms cascades because of the substantial number of entities across sectors that depend on the platform.

i Andy Greenberg (2018). "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Wired, August 22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Two sets of factors influence whether any particular incident triggers systemic effects. The first set of factors relates to the criticality, interconnectedness, resilience, and homogeneity of the affected system—the "**system attributes**." The second set of factors relates to the nature of the incident itself—"**incident attributes**"—its infectiousness, destructiveness and sophistication. System and incident attributes must be evaluated when assessing the risk of a cyber incident becoming systemic, how damages from an attack could spread, and the incident's potential impact.

These factors are described in the box below.

The Cyber Insurance Market Today

Insurance companies offering cyber coverage through stand-alone policies or add-ons to more traditional lines must understand systemic cyber risk to accurately underwrite policies and assess the aggregation of risk within their portfolios. The cyber insurance market is growing, while cyber attacks are increasing in severity. The market is now settling claims from major cyber incidents in 2017 and 2018.

System Attributes

1. Criticality: The importance of affected technical and business systems to the functioning of organizations that depend on them. Higher criticality leads to larger consequences.

2. Interconnectedness: The extent to which systems and organizations are connected to one another and to the larger economy. Greater interconnectedness through technical, functional, or geographic relationships amplifies the consequences of an event or failure.

3. Resilience: The capacity to prepare for and adapt to changing conditions and recover rapidly from disruptions, including the ability to deploy redundant, resilient systems for backup and recovery operations, switch to an alternative provider, defend against attacks or mitigate failures. Low resilience in the system allows effects to outpace response actions leading to more lasting and impactful consequences.

4. Homogeneity: The use of identical or similar components or elements (e.g., software, hardware or services) across the ecosystem. Homogeneity can turn into a critical weakness if these elements become subject to technological failure or vulnerable to exploitation. Conversely, identical or similar system components increase insight into risks, and the means to remediate those risks quickly and at scale.

Incident Attributes

1. Infectiousness: The ability to move from one system to another. High infectiousness makes it more likely that an incident propagates to other systems. Further, while propagating, the incident (and resulting failures) may adapt, evolve or change modalities, potentially reducing the responder's ability to contain the incident.

2. Destructiveness: The effects of the attack or failure on system performance. An attack that produces an annoying pop-up ad is less destructive than one that denies the owner access to data, or results in complete or lasting system breakdown.

3. Sophistication: The degree of difficulty finding and defending against the attack, or to correct a technological failure and recover to a secure state with acceptable service capacity. Sophisticated attacks or obscure code failures may be more difficult to mitigate, extending the duration and the severity of the incident.

As exposure increases, insurers are asking for more data from insureds, including detailed cybersecurity audits and information about relationships with third party vendors. Insurers are also moving to an "affirmative cyber" approach; in addition to offering stand-alone cyber policies, they are explicitly including (or excluding) cyber coverage in traditional policy lines where cyber perils were previously unacknowledged during initial underwriting.

Cyber insurance is an area of potential growth for many insurance companies, and the current competitive market has kept policy prices low. However, this nascent industry is also relying on emerging risk modeling tools, where most of the predictions about cyber incidents are drawn from past events—an approach that may be inadequate in a sector defined by constant innovation. While there has not yet been a cyber event that resulted in systemic effects and catastrophic losses for the insurance market, the inherent uncertainty around systemic cyber risk drives the need for action by the insurance industry, risk management firms and governments, to ensure the cyber insurance market can mature in a healthy, risk-informed way, and continue to provide sufficient insurance capacity.

Recommendations

This report makes four recommendations to enhance the ability of the cyber insurance market to support cyber resilience efforts, guard against systemic risk and avoid catastrophic losses:

1. **Enhance cyber insurance underwriting ability** using existing cybersecurity frameworks, leveraging data, developing in-house cyber expertise, and harmonizing underwriting questions based on international security standards or sector-specific requirements.

2. **Promote a strong and healthy market with positive impacts on society** using new models for cyber resiliency. The cyber insurance industry should develop new business models, partnering with cybersecurity and technology companies, to offer a suite of services to clients to understand and reduce their cyber risk. Insurance companies can also explore using advanced analytics, promoting loss control products and tying financial incentives to an insured's cybersecurity practices to increase overall cyber resilience.

3. **Increase transparency and uniformity in insurance language**. Policies should contain coherent language that reduces uncertainty around the definitions of cyber incidents, coverage types and policy triggers. In particular, insurers should use clear language to describe what triggers a specific exclusion in a policy and have clear and uniform definitions for key terms, such as "act of war," "state actors" and "state cyber attacks." Buyers of insurance need to look closely at the nuances in their policies to understand their coverage accurately.

4. **Increase overall capacity to handle a major, multi-market loss through the creation of a government backstop** for systemic cyber incidents, similar to those created for terrorist events (TRIA in the U.S. and Pool Re in the UK). A private reinsurance pool is imagined as the most appropriate model for cyber insurance, which could include the following: certification of an incident by a government official as eligible for coverage under the program, a requirement that all primary insurers offer cyber coverage to commercial clients, multi-line coverage, and incentives for consumers and service providers to invest in cybersecurity.

Cyber Insurance

DATE:	EVENT:
July 2017	**Equifax Data Breach**
DAMAGE: **$1.4 billion**	Hackers exploited a known yet unpatched vulnerability in the Apache Struts Web Framework (an open-source software suite used to develop web applications) to extract the personal data of 148 million people in the credit bureau's databases. In 2017, former CEO Richard Smith was called before the U.S. Congress to testify about the breach.

Mark Wilson / Staff / Getty Images

1 Introduction

Cyber defenses have grown more sophisticated, as have attackers. The possibility that a cyber incident, or series of incidents, could trigger wide ranging systemic effects that cascade through multiple industry sectors and affect the global economy is of increasing concern for societies highly dependent on networked information and communications technologies.

Cyber Insurance in Context

As cyber threats grow more common, so does their potential for disruption and financial damage. Estimates of economic damage and consequences from cyber incidents range widely, but reflect an increasing trend.[1,2] Some experts estimate that the cost of cyber crime will reach six trillion USD annually by 2021, having doubled since 2015.[3] Cyber defenses have grown more sophisticated, as have attackers. The possibility that a cyber incident, or series of incidents, could trigger wide ranging systemic effects that cascade through multiple industry sectors and affect the global economy is of increasing concern for societies highly dependent on networked information and communications technologies (ICTs).[4] Aggressive cyber actions by one government may trigger responses from other state actors, with the potential to escalate and inflict economic damage by targeting critical national systems.[5]

Although recognition of the global economy's exposure to and dependence on cyberspace is growing, there is a dearth of tested, accurate models to predict and measure the potential impacts of major cyber incidents. Enterprises continue to manage cyber risk through resilience, defense in depth and other risk-based approaches, including transferring residual risk through the purchase of insurance coverage for cyber losses.[6] Risk transfer and modeling is part of the risk management toolbox.

For any catastrophic risk, insurance is an important mechanism to offset potential losses that could threaten an organization's ability to recover from a damaging incident. With damages from cyber incidents growing, many organizations are using insurance to protect against financial losses. In addition, insurance has the potential to improve cyber resilience by strengthening the cybersecurity baseline and best practices. Historically, the insurance industry has played this role in other sectors, for instance, by establishing building codes that lowered risk, improved safety and reduced fire damage.[7] A dynamic cyber insurance market, however, creates uncertainty about risk within the market itself, particularly regarding its ability to absorb losses resulting from systemic failures caused by cyber incidents.

While the cyber insurance market continues to be a source of growth and profitability for the insurance industry, several high-profile cyber incidents over the past two years (e.g., NotPetya, WannaCry, the Marriott and Equifax data breaches, among others) have caused some to caution that "the sustainability of the cyber insurance

1 A recent RAND study estimates the global costs of cyber crime alone (direct plus systemic costs) to range from 1.1 percent to over 30 percent of global GDP. Paul Dreyer et al. (2018). "Estimating the Global Cost of Cyber Risk: Methodology and Examples." RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2299/RAND_RR2299.pdf.

2 Incidents include technology failures and attacks, each of which have many possible sources. For example, failures can stem from coding errors or bad data while attacks can be launched by criminals or states.

3 Herjavec Group (2019). The 2019 Official Annual Cybercrime Report. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

4 Ian Goldin and Mike Mariathasan (2014). *The Butterfly Defect: How Globalization Creates Systemic Risks, and What to Do about It*. Princeton University Press; Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly. "Identifying, understanding, and analyzing critical infrastructure interdependencies." IEEE Control Systems 21.6 (2001): 11-25.

5 Multiple efforts are attempting to moderate state practice through international cooperation among state and non-state (including private sector) actors. For example, through the Global Commission on the Stability of Cyberspace, the EastWest Institute advocates for norms that restrain offensive state behavior and conflict in cyberspace. See www.cyberstability.org.

6 Marshall Kuypers and Thomas Maillart (2018). "Designing Organizations for Cyber Security Resilience." Workshop on the Economics of Information Security (WEIS), https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2016/09/WEIS_2018_paper_50.pdf.

7 International Code Council. https://www.iccsafe.org/gr/Documents/AdoptionToolkit/04-Why_Choose_the_I-Codes.pdf.

market should not be taken for granted."[8] In particular, there is uncertainty about the market's ability to understand the way the impacts of events could potentially cascade across sectors and to price cyber risk correctly. Pricing cyber risk is inherently difficult due to the complex, heterogeneous, interconnected nature of cyber systems, constant change and evolution in the technology environment (including new types of attacks and weaponry), and a shortage of actuarial data.[9,10] As the cyber insurance market continues to grow, both the industry and its regulators need to better understand how cyber risks are correlated (i.e., which aspects of the risks are affected by the same factors) and how cyber risk may accumulate in an individual insurer's portfolio and across the insurance industry. This understanding is necessary to ensure the market can absorb and withstand a potentially major shock.[11]

This Report

Cyber Insurance and Systemic Market Risk builds on past efforts—including the 2016 World Economic Forum (WEF) White Paper "Understanding Systemic Cyber Risk"—and focuses specifically on the strength and resilience of the cyber insurance market and its capacity to mitigate systemic cyber risk.[12]

This report addresses the cyber insurance industry and its potential to act as both an actor to lessen systemic cyber risk by improving enterprise cybersecurity practices, and as a potential source of systemic risk to the broader insurance market itself, were there to be large-scale covered damages to insured entities. First, this report offers insurance companies, cybersecurity experts, policymakers and other stakeholders a framework to identify and assess systemic cyber risks for the insurance market. Second, the report suggests policy recommendations for companies and governments to help address cyber risk for the insurance industry. These recommendations are intended to limit the exposure to systemic shocks with potentially catastrophic effects for the insurance market, including through the development of a government backstop and other measures. The report contributes to improving overall cyber resilience in the face of increasing cyber threats and global connectivity.

8 Daniel Hofman, Steven Wilson and Rachel Anne Carter (2018). "Advancing Accumulation Risk Management in Cyber Insurance." The Geneva Association. August. https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/report_advancing_accumulation_risk_management_in_cyber_insurance_0.pdf.

9 Global Risk Quantification Network (2018). Quantifying Systemic Cyber Risk. Report on the "Connectedness in Cyber Risk" Workshop. San Diego. http://web.stanford.edu/~csimoiu/doc/Global_CRQ_Network_Report.pdf.

10 Maria Francesca Carfora, et al. (2017). "Cyber risk management: a new challenge for actuarial mathematics." MAF 2018. 10.1007/978-3-319-89824-7_36. https://www.iit.cnr.it/sites/default/files/cyber-risk-man.pdf.

11 Insurers look at risk accumulation in their portfolios as the potential for a single event to have widespread impact on thousands of insureds at once. For more on accumulated risk in cyber insurance, see Risk Management Solutions, Inc. (2016). "Managing Cyber Insurance Accumulation Risk." Report prepared in collaboration with and based on original research by the Centre for Risk Studies, University of Cambridge. Available at https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-rms-managing-cyber-insurance-accumulation-risk.pdf.

12 WEF (2016). "Understanding Systemic Cyber Risk: Global Agenda Council on Risk & Resilience." October. http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf. This paper recommended the creation of a definition of "systemic cyber risk," assessed the scope of unknown liability assumed by organizations and examined the implications to the global economy and other sectors resulting from an event that realizes systemic cyber risk.

2 Defining Systemic Cyber Risk

There are two broad mechanisms that can cause damage from an incident to cascade across systems: common vulnerabilities and concentrated dependencies.

Systemic risk is generally understood as risk that an event (or series of events) will result in the large-scale failure of a sector, industry or economy (catastrophic failure).[13] The definition of systemic cyber risk proposed in this report highlights the potential for the initial cyber incident to trigger shocks that lead to broader societal effects, and require a massive response effort to recover.

Definition of systemic cyber risk:

> The potential for a cyber incident, event or shock to the digital ecosystem to cause broad-based disruption in information and communications technology services resulting in a loss of trust and capital. This breakdown will then cascade to other sectors of the economy, causing significant adverse effects to public health or safety, the economy or national security.[14]

To understand systemic cyber risk, it is useful to identify the characteristics of events or shocks that could trigger systemic effects. A determining characteristic is the probability of

13 Jessica Beyer, et al. (2018). "Addressing Systemic Cybersecurity Risk." Applied Research Program, Jackson School of International Studies, University of Washington. May. https://jsis.washington.edu/wordpress/wp-content/uploads/2019/02/JSIS_ARP_Report_1_Risk_2018_FINAL.pdf.

14 This definition parallels the U.S. government's definition of critical infrastructure–vital "assets, systems and networks" for which "incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety." Whether or not a particular event is deemed "systemic" is in part a matter of perspective. For example, a government might need to make such a determination based on statutory criteria in order to trigger recovery and relief mechanisms. For the insurance industry, an event may result in catastrophic financial losses in the private sector, but if those losses are not covered in actual policies, the event is not systemic for the insurance industry.

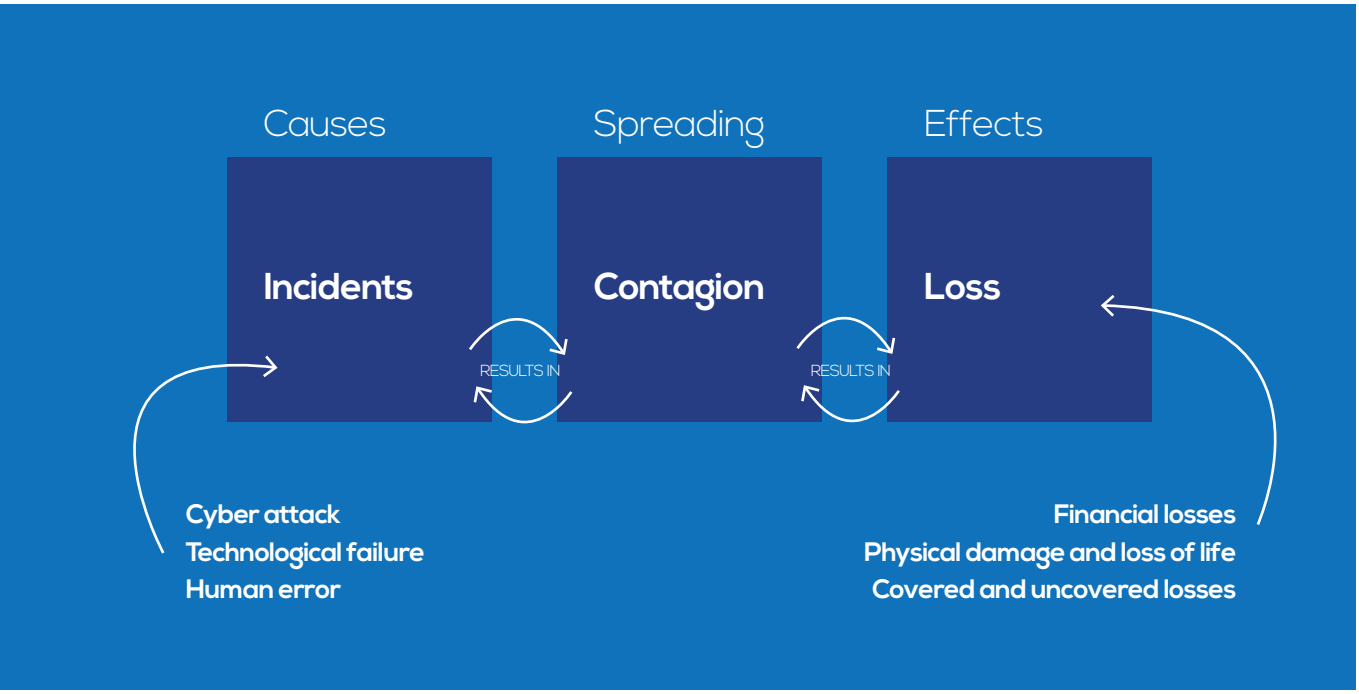


Figure 1: Incident-Contagion-Loss Relationship

"contagion," that is, effects cascading across multiple sectors of the economy.[15] There are two broad mechanisms that can cause damage from an incident to cascade across systems: common vulnerabilities and concentrated dependencies.

The risk from a "**common vulnerability**" comes from the presence of a component or vulnerability that is widespread throughout systems (e.g., a bug in the OpenSSL library in the case of Heartbleed, vulnerabilities that were exploited in the WannaCry and NotPetya cyber attacks, or a common Linux vulnerability).

The risk from "**concentrated dependency**" is created by the widespread reliance on a small number of vendors or a critical platform (e.g., GPS, a single critical infrastructure provider as in the attacks on Ukraine's power plants[16] or the failure of a common Internet service provider).[17] An oft-cited example is the market dominance of several cloud service providers. Yet, cloud service providers can also strengthen resilience as cloud infrastructure enables managing some of these risks through geodiversity and redundancy.[18]

15 See, for example the discussion on insurance's assessment of "catastrophes" and global catastrophic risks framework in Pythagoras Petratos, Anders Sandberg, Feng Zhou (2018). "Cyber Insurance." In: Carayannis E., Campbell D., Efthymiopoulos M. (eds) *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*. Springer, Cham.

16 Kim Zetter (2016). "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." Wired, April 29. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid.

17 WEF (2016).

18 A compromise in the confidentiality, integrity or availability of the data stored or processed by cloud service providers is likely to not only be felt by their direct customers and their businesses, but eventually the customers of the cloud-enabled businesses. However, it is important to note that multiple data centers and redundancies in the cloud infrastructure reduce the risk of a cloud service provider going down. See also WEF (2016).

Concentrated dependencies also occur in the physical world. For example, the small number of ports able to handle the largest container ships means that a cyber attack on one of these port's systems could have reverberating consequences for shipping globally, resulting in a significant economic impact.[19, 20]

Of course, the categories of common vulnerability and concentrated dependency are not mutually exclusive. Exploitation of a common vulnerability present across a major cloud platform's infrastructure could lead to a concentrated risk scenario—a consequence of cascading effects. Cyber systems are complex, highly interconnected and layered, with ambiguous borders between systems. There will always be uncertainty about the risk.[21]

Contagion

Contagion, which is the propagation of adverse effects within and across sectors, happens when the digital interconnection of critical systems and the underlying technical, functional, economic and financial dependencies are of sufficient depth to allow the incident to breach the cyber realm and affect the broader economy and society.[22] High criticality (e.g., critical infrastructure or critical technical components in systems), high levels of digital interconnectedness and high functional dependencies each increase systemic cyber risk. Furthermore, when contagion occurs and the understanding of risk increasingly shifts from objective measurement to subjective perception, trust in systems and institutions is undermined. Individuals and the public may take actions and decisions based on incomplete or malicious information (e.g., disinformation or rumors) that increase the damaging effects.[23]

Figure 1 illustrates the three major components—incidents, contagion and loss—of systemic risk and the dynamics among these intertwined components. In this model, the processes and effects do not unfold in a linear manner.

Increased Attention to Systemic Risk

With increased globalization, continued technological change and digitalization, systemic risk is an issue that is being actively studied and addressed in many other fields, including the financial sector, global supply chains, terrorism, global public health and infectious disease, and climate.[24] Climate scientists are examining systemic risks that "arise from the

19 WEF (2016).

20 The financial services sector is a particularly significant potential vehicle for such a cascade due to its interoperability and the critical role it plays in the global economy.

21 Aaron Clark-Ginsberg, Leili Abolhassani and Elahe Azam Rahmati (2018). "Comparing networked and linear risk assessments: From theory to evidence." International Journal of Disaster Risk Reduction.

22 The term "contagion threshold" has been used in some epidemiological and network propagation analyses to denote a level below which an effect is unlikely to spread to other populations or nodes.

23 Losses can be the result of direct effects (i.e., first order consequences), such as the outage of a critical system due to a cyber attack, or indirect effects (i.e., second and third order consequences) such as downstream effects in the supply chain due to business interruption of a critical supplier due to a cyber attack resulting in one's own inability to continue production and financial loss, physical destruction or loss of life.

24 For example, Ian Goldin and Mike Mariathasan (2014). *The Butterfly Defect: How Globalization Creates Systemic Risks, and What to Do about It*. Princeton University Press. For more on global systemic risk assessments and research, see the Princeton Institute for International and Regional Studies Global Systemic Risk Research Community: https://risk.princeton.edu/.

interaction of climate change with human social and economic systems," including supply chains, global food markets, transportation, trade networks and international security.[25] The study of the spread of infectious disease and modeling outbreaks offers lessons that can be applied to understanding systemic cyber risk and how cyber "viruses" spread.[26] The fields of terrorism insurance and risk analysis also offer lessons for policymakers and insurance companies in cyberspace, as explained in the recommendations in Section 5.

This report's understanding of systemic cyber risk is informed by the close parallels between cyber systemic risk and systemic risk in the financial services sector.[27] The financial sector, which has matured its risk understanding after major global events, is deeply interconnected across the globe, affected by political, social and geopolitical factors, and must deal with a high level of systemic risk—compounded by cyber risks given the sector's dependence on digital tools and platforms.

The 2008 global financial crisis, where excessive trading and poor underwriting practices in the mortgage-backed securities industry led to a series of bank failures and a global economic recession, provides a lens to observe systemic cyber risk. Some would draw a more ominous parallel. A 2014 report from Zurich Insurance Group and the Atlantic Council uses the label "cyber sub-prime" to describe "aggregated global cyber risk as analogous to those risks that were overlooked in the U.S. sub-prime mortgage market prior to the 2008 financial crisis."[28] The manner in which the 2008 crisis cascaded beyond the United States illustrates the impact of interconnectedness, which is especially applicable to cyber risk. The wide range of public and private organizations (e.g., the U.S. Financial Stability Oversight Council, the U.S. Consumer Financial Protection Bureau, the European Banking Authority and the European Securities and Markets Authority) established to manage the crisis as it was happening and build processes to avoid further crises, could serve as a template for future policy work on managing systemic cyber risk.

25 David King, et al. (2015). "Climate Change: A Risk Assessment." Edited by James Hynard and Tom Rodger, Centre for Science and Policy. University of Cambridge. http://www.csap.cam.ac.uk/projects/climate-change-risk-assessment/.

26 There are many studies that draw the link between infectious disease and epidemiology, and cyber "health." Models for the spread of malware are based on disease epidemic spread. See for example, Bao Nguyen (2017). "Modelling Cyber Vulnerability using Epidemic Models." DOI: 10.5220/0006401902320239. https://www.scitepress.org/papers/2017/64019/64019.pdf; R. David Parker and Csilla Farkas (2011). "Modeling Estimated Risk for Cyber Attacks: Merging Public Health and Cyber Security." Information Assurance and Security Letters, Volume 2: 32-36. https://cse.sc.edu/~farkas/publications/j18.pdf. For more on how lessons from cyber risk could be applied to public health and infectious disease, see: Frank L. Smith, III (2016). "Malware and Disease: Lessons from Cyber Intelligence for Public Health Surveillance." Health Security, 14 (5): 305-314. October 1. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5041502/.

27 For more discussion on applying the lessons of systemic (financial) risk to the understanding of systemic cyber risk, see Jessica Beyer, et al (2018). "Addressing Systemic Cybersecurity Risk." Applied Research Program, Jackson School of International Studies, University of Washington. May. https://jsis.washington.edu/wordpress/wp-content/uploads/2019/02/JSIS_ARP_Report_1_Risk_2018_FINAL.pdf.

28 Zurich (2014). "Beyond data breaches: global interconnections of cyber risk." Risk Nexus Report of Zurich Insurance Group and Atlantic Council. http://www.atlanticcouncil.org/images/publications/Zurich_Cyber_Risk_April_2014.pdf.

3 Systemic Cyber Risk: An Analytical Framework

This section uses two case scenarios to illustrate a framework for analyzing systemic cyber risk, addressing when a cyber incident could trigger a shock to the digital ecosystem that produces systemic effects. The section concludes with a discussion of the circumstances under which systemic effects could produce catastrophic losses for the cyber insurance industry.

What Can Trigger a Systemic Shock?

Under what circumstances is a "cyber incident, event or shock to the digital ecosystem" likely to produce adverse, systemic effects? Two classes of attributes are necessary in combination to trigger systemic shocks:

- the state of the technological/ business system—and the organizations that depend on these systems—that experiences the shock, or the "system attributes," and
- the severity of the incident that causes the disruption and triggers a shock—the "incident attributes."

System Attributes include two elements that increase risk (criticality and interconnectedness), one that decreases risk (resilience) and one that could potentially do either (homogeneity).

1. **Criticality:** The importance of affected technical and business systems to the functioning of organizations that depend on them. Higher criticality leads to larger consequences.
2. **Interconnectedness:** The extent to which systems and organizations are connected to one another and to the larger economy. Greater interconnectedness through technical, functional or geographic relationships amplifies the consequences of an event or failure.[29]

29 Interconnection and dependency are synergistic. See, ENISA (2018). "Good practice on interdependencies between OES and DSPs." November. https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps.

DATE:	EVENT:
Nov. 2018	**Marriott Data Breach**
DAMAGE: **$72 million**	An unpublicized vulnerability allowed hackers to access Marriott guest records, exposing personal information of 383 million customers over a period of four years.

Scott Olson / Staff / Getty Images

Figure 2: Potential Systemic Impact of Large-Scale Cyber Incidents

3. **Resilience:** The capacity to prepare for and adapt to changing conditions and recover rapidly from disruptions. Resilience further includes the ability to deploy redundant systems for backup and recovery operations, switch to an alternative provider, defend against attacks, or mitigate failures. Low resilience in the system allows effects to outpace response actions, leading to more lasting and impactful consequences.
4. **Homogeneity:** The use of identical or similar components or elements (e.g., software, hardware or services) across the ecosystem. Homogeneity can turn into a critical weakness if these elements become subject to technological failure or vulnerable to exploitation.[30] Conversely, identical or similar components increase insight into risks, and the means to remediate those risks quickly and at scale.

Incident Attributes also include three elements: infectiousness, destructiveness and sophistication, which increase the danger from a failure or attack. These attributes are more difficult for system owners to control than system attributes.

30 Aggregated distributed risk arises when multiple entities depend on a common operating system (e.g., Linux), whereas concentrated risk arises when large numbers of entities depend upon a central provider of critical services (e.g., Amazon Web Services, Salesforce).

1. **Infectiousness:** The ability to move from one system to another. High infectiousness makes it more likely that an incident is propagated to other systems. Infecting other systems can take place in a targeted or widespread manner (precision of propagation) and more or less rapidly (speed of propagation). Further, while propagating, the incident (and resulting failures) may adapt, evolve or change modalities, possibly reducing the ability to contain the incident.
2. **Destructiveness:** The effects of the attack or failure on system performance. An incident that results in an annoying pop-up ad is less destructive than one that denies the owner access to data, or results in complete or lasting system breakdown. Similarly, a failure that causes detectable, downstream changes in financial data may be less destructive than one which crashes a critical system or distorts data used in other systems.
3. **Sophistication:** The ability to exploit system vulnerabilities—and shift targets as incidents and responses unfold—to inflict the most damage while minimizing the defenders' ability to respond. This includes how difficult it is to identify and defend against attacks, or to correct a technological failure and recover to a secure state with acceptable service capacity. Sophisticated attacks or obscure code failures may be more difficult to mitigate, extending the duration and the severity of the incident, and likely increasing its consequences.

Both dimensions—system attributes and incident attributes—are critical in describing contagion, that is, the ability for a shock to be transmitted across the ecosystem and multiple sectors, and pushing an incident into the "Systemic Impact Zone." Interconnectedness and homogeneity are, in particular, critical enablers of contagion.

Figure 2 on page 18 illustrates the relationship between the two classes of attributes. Since historical data is mostly lacking for events in the "Systemic Impact Zone," risk modelers use counterfactual analysis to estimate risk based on historical events in the "Known Zone" and then explore what perturbations to the events might have shifted them into the "Systematic Impact Zone."[31]

Scenarios

Using the framework outlined above, the next section analyzes system and incident attributes by examining two scenarios—common vulnerabilities and concentrated dependencies—that can cause cyber incidents to cascade and create systemic effects.[32]

Note that the scenarios presented here are illustrative. In reality, incidents are likely to exhibit hybrid characteristics. A common vulnerability embedded in a critical infrastructure system could result in a concentrated dependency scenario—the failure of numerous dependent downstream entities or processes. As previously noted, the categories of common vulnerability and concentrated dependency are not mutually exclusive.

31 Lloyd's of London and RMS (2017). "Reimagining History – Counter factual risk analysis." Emerging Risk Report. https://www.lloyds.com/news-and-risk-insight/risk-reports/library/understanding-risk/reimagining-history.

32 For details on these and other scenarios—data exfiltration, denial of service attacks, financial transaction interference, and failures of counterparties or suppliers—see Chapter 2 "Preparing for Cyber Attacks" in Andrew Colburn, Eireann Leverett and Gordon Woo (2019). *Solving Cyber Risk: Protecting your company and society.* Hoboken, NJ: John Wiley & Sons, Inc.

Scenario 1: Common Vulnerabilities

Common vulnerabilities can create a systemic cyber risk, as vulnerabilities in software used by a large number of users leaves them subject to an attack if a vulnerability becomes known and exploited. As these systems all share the same vulnerability, they do not need to be directly interconnected to result in large-scale exploitation. Fixing widespread vulnerabilities is difficult as patching is often at the discretion of system owners, especially at the corporate level.[33] From an insurance perspective, it is difficult to evaluate the risk from common vulnerabilities due to the large number of widely-used software and hardware platforms. Vulnerabilities are numerous. Novel, unforeseen exploits are constantly developed. When new types of vulnerabilities or exploits are discovered, beliefs and assumptions about the security of systems can be challenged (e.g., in the case of Meltdown and Spectre), and require the insurance industry to rethink how it conceptualizes and assesses cyber risk. Looking to past attacks or exposed vulnerabilities is not sufficient.

An example of a cyber attack that exploited a common vulnerability is the NotPetya malware that permanently rendered critical data inaccessible ("wiperware"). NotPetya used the EternalBlue exploit to target a Windows vulnerability and destroy data and systems by encrypting entire hard drives and then overwriting the master reboot record, resulting in the interruption of global operations and need for hardware replacement in several corporations. Other cases in this category include the Heartbleed vulnerability, Meltdown and Spectre, as well as the Mirai and WannaCry attacks.

System Attributes

> *Criticality*: NotPetya affected corporations worldwide, including global logistics giants Maersk and FedEx, the pharmaceutical company Merck, and many others.
> *Interconnectedness*: The systems affected were not significantly interconnected outside the affected organizations.
> *Resilience*: Poorly secured and unpatched systems helped facilitate the spread of NotPetya.[34]
> *Homogeneity*: NotPetya exploited a vulnerability in Windows, a widely used platform with a very high degree of homogeneity. Certain versions of the operating system were more susceptible than others; those where patches were not deployed were the most vulnerable.

Incident Attributes

> *Infectiousness*: The malware was effective at propagating within affected organizations' systems due to interconnections within corporate networks (e.g., FedEx operating in Ukraine via its TNT subsidiary contracted the malware, which then spread to FedEx's other networks).
> *Destructiveness*: The malware caused complete failure of the affected systems and rendered them inoperable. Damage occurred at many organizational levels, across several geographic regions.
> *Sophistication*: The malware targeted a specific common vulnerability and showed significant sophistication in its delivery and propagation mechanism; recovery from the incident required considerable time and resources.

33 I.e., automatic software updates increasingly help to push security patches to large numbers of individual users.

34 Andy Greenberg (2018). "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Wired, August 22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

DATE: **Jan. 2018**	EVENTS: **Spectre and Meltdown**
DAMAGE: **$10-$25 billion**	Spectre and Meltdown are considered "catastrophic" hardware vulnerabilities in microprocessors. The design flaws expose billions of devices to have their system security protections bypassed and sensitive data stolen out of nearly any computer's memory.

Jasmin Merdan / Getty Images

DATE:
Dec. 2015 and Dec. 2016

EVENT:
Ukraine Power Grid Attacks

DAMAGE:
Unknown

Two cyber attacks were carried out on Ukraine's electrical grid in 2015 and 2016. The 2015 attack targeted dozens of power substations and left over 230,000 Ukrainians without power for up to six hours. The attack also disabled backup power generators at two out of the three main distribution centers, prevented customers from reporting outages via denial of service attacks against call centers, inserted malicious firmware and wiped data from operators' substations, putting those out of service for months. The attack in 2016 targeted a Kiev transmission station, taking down a fifth of Kiev's power capacity for an hour.

Brendan Hoffman / Stringer / Getty Images

Scenario 2: Concentrated Dependencies

Market dominance—the concentration of a single or a few dominant vendors or providers—leads to high criticality of central systems. The criticality of these services or vendors also creates an inherent lack of resilience, as few alternatives (e.g., multi-provider strategies, redundant capacity, backup solutions and failback options) exist to mitigate downside risk. If managed effectively, however, entities with concentrated dependencies can push security updates and strict security requirements to a very large part of the ecosystem. From an insurance perspective, it is relevant to identify concentrated dependencies for a particular insured as well as in the aggregate of an insurer's portfolio. If a provider with concentrated dependencies is affected by a cyber attack, then it is likely that multiple insureds file claims, leading to significant losses.

An example of the exploitation of a concentrated dependency is the 2015 cyber attack on Ukraine's electrical grid that targeted dozens of power substations and left over 230,000 Ukrainians cut off electricity for as many as six hours. The attacks also disabled backup power generators at two out of the three main distribution centers, used denial of service attacks against call centers to prevent customers from reporting outages, and wiped data from substations by inserting malicious firmware, putting them out of service for months.[35] Other cases in this category include Dyn DNS services, Amazon S3 outages and CloudFlare CDN vulnerabilities.

System Attributes

> *Criticality*: Power generation is essential to the functioning of the modern world as it enables most technology, digital or otherwise. This critical infrastructure also increasingly relies on digital industrial control systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems to function, giving failures the potential for catastrophic impacts.

> *Interconnectedness*: Industrial control systems tend to be isolated. However, the processes they support can be highly interconnected at a service level, potentially resulting in significant cascading effects across multiple sectors.

> *Resilience*: Although the attacks targeted backup power generators, engineers were able to switch to manual operations.[36]

> *Homogeneity*: Some vendors account for a significant market share and are used widely across multiple infrastructures.

Incident Attributes

> *Infectiousness*: The malware authors took steps to limit the malware's infectiousness, although they were not completely successful.

> *Destructiveness*: The malware caused devastating physical damage to the affected systems, rendering some of those systems inoperable for months.

> *Sophistication*: The malware was sophisticated and took significant resources to develop and deploy.

35 Kim Zetter (2016). "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." Wired, March 3. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

36 Andy Greenberg (2017). "How An Entire Nation Became Russia's Test Lab for Cyberwar." Wired, June 20. https://www.wired.com/story/russian-hackers-attack-ukraine/.

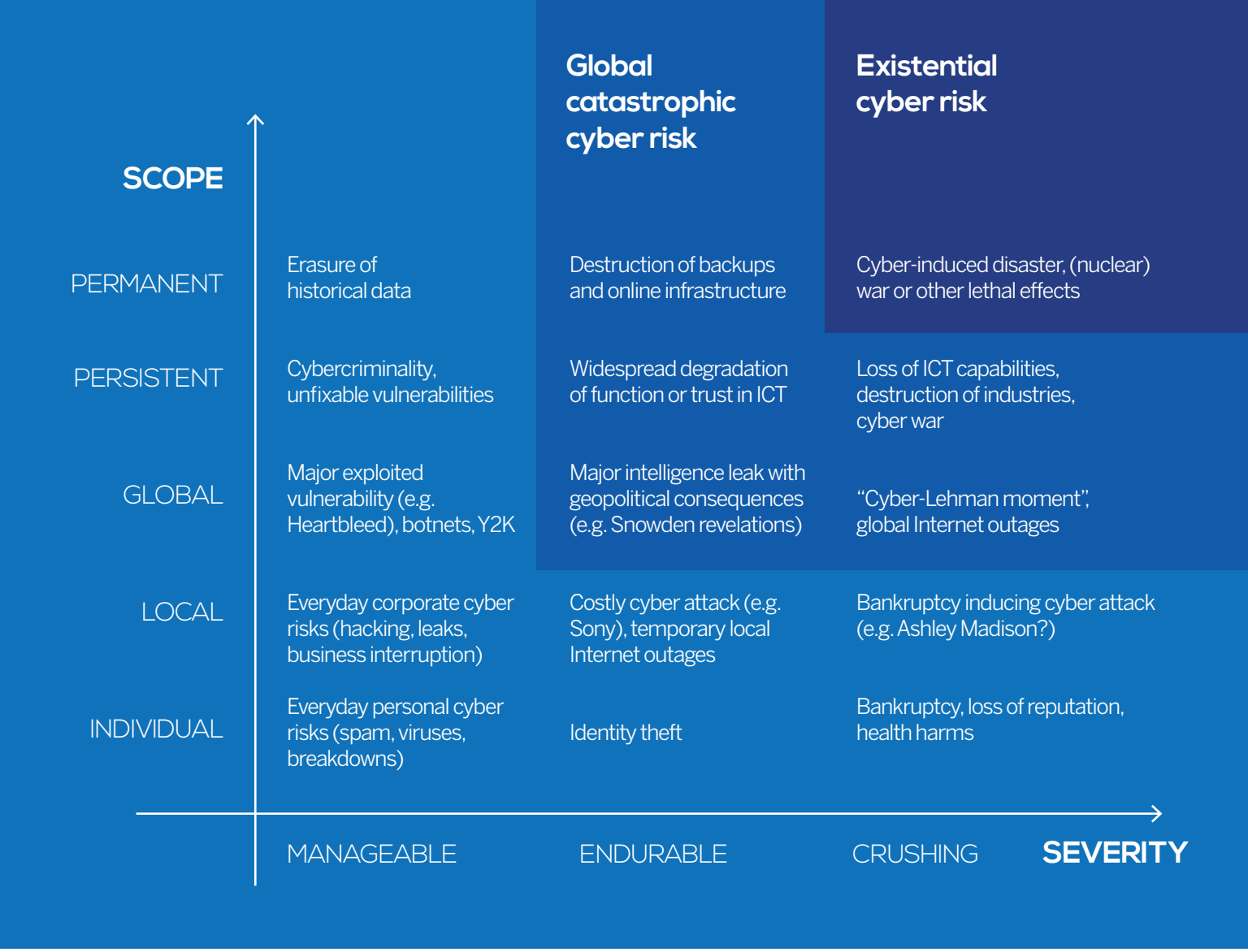


Figure 3: Qualitative Risk Categories[37]

Systemic Cyber Risk and Catastrophic Loss

Coverage of a loss (i.e., the financial consequences of damage) depends on the contractual agreement between the insurer and the insured. Whether and to what degree a loss is covered depends on the terms, deductions, exclusions, limits and sub-limits specified in the insurance contract.

Major cyber incidents can lead to massive losses. For example, NotPetya affected corporations worldwide leading to significant financial losses[38] and costing the global economy over 10 billion USD.[39] Some of those losses were covered by insurance policies, others were not. Uninsured damages had to be absorbed by

37 See Pythagoras Petratos, Anders Sandberg, Feng Zhou (2018). "Cyber Insurance." In: Carayannis E., Campbell D., Efthymiopoulos M. (eds) *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*. Springer, Cham.

38 Lee Mathews (2017). "NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million." August 16. https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/.

39 Andy Greenberg (2018). "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." August 22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

individual corporations or society at large. The NotPetya attack produced losses that, in some instances, were covered by cyber insurance policies. Not all NotPetya victims carried cyber insurance. Some companies attempted to claim their losses based on affirmative cyber coverage in their property policies, which has resulted in coverage disputes.[40] See box to the right, "Is My Loss Covered?"

In addition, whether an event is considered "systemic" may be a matter for determination under criteria laid out in law and regulation. For example, a rule-based determination by a government official might be necessary to activate recovery and relief efforts, as is the case in a natural disaster or in a terrorist attack.[41]

Major cyber incidents such as the scenarios described above hold the potential to trigger large financial damages, and, to the extent these events are covered under cyber insurance policies, the insurance market could suffer large losses. Common vulnerabilities could produce an event affecting a substantial portion of cyber policies. If large numbers of affected policies are held by an insurer, this aggregated risk could result in catastrophic financial losses for that entity. If the event affects broad sectors of society, the impact on the insurance industry could be significant, and this impact itself could lead to uncertainty and contagion affecting broader financial markets. Figure 3 describes qualitative loss categories for cyber incidents and their damages regarding scope and severity of the damages.[42]

40 An "affirmative cyber" insurance policy is any policy that explicitly addresses cyber coverage; this includes endorsements to traditional lines of insurance, such as general liability, E&O, or property and casualty, as well as stand-alone cyber policies.

41 See footnote 14

42 For extended discussion on categorization of incidents and damages, see: Pythagoras Petratos, Anders Sandberg, Feng Zhou (2018). "Cyber Insurance." In: Carayannis E., Campbell D., Efthymiopoulos M. (eds) *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*. Springer, Cham.

Is My Loss Covered? The Messy Intersection of Cyber Insurance with Traditional Lines of Insurance

The intersection of cyber insurance policies with traditional lines is still being clarified in the marketplace. For example, after the NotPetya attack, several companies (Maersk included) filed claims for business interruption losses under their property policies from a non-physical incident.[43] Some insurance companies are moving these exposures to cyber policies and excluding non-physical business interruption liabilities from traditional property lines.

When companies are attempting to calculate their risk exposure, the cascading impact from a non-physical business like the one created by NotPetya—can be difficult. In the Maersk example, there were many downstream companies that did not receive their shipments. They lost time, customers and revenue. Whether or not these downstream companies were covered for their losses depends on the coverage they held. Their business interruption losses would most likely not be covered by a general property policy. If the provider had been a "critical service provider" such as a telecom company, electric utility or ISP, certain exclusions related to critical infrastructure might apply. Further, if the downstream company held a cyber policy that included business interruption, their losses would likely be covered.

To adequately comprehend cyber exposure, insurance companies must understand the digital and business interconnections (and potential exposures) of the insured.

43 Michael Menapace (2019). "Property Insurance, Cyber Insurance, Coverage and War: Losses from Malware May Not Be Covered Due to Your Policy's Hostile Acts Exclusion." The National Law Review. March 10. https://www.natlawreview.com/article/property-insurance-cyber-insurance-coverage-and-war-losses-malware-may-not-be-0.

4 Cyber Risk and the Insurance Market

Cyber risk can emanate from a wide array of actors, affect all industries and create both physical and economic harm. For this reason, cyber risk implicates multiple lines of insurance.

The Insurance Market Today

The potential financial impact of a cyber incident creates risk for every organization. Once the organization understands its exposure, it can determine what practices will best mitigate the risk, and then determine to accept or transfer any residual exposure. Insurance is an important mechanism to offset losses that could threaten an organization's ability to recover from a damaging incident.

Increasingly, organizations have turned to insurance as part of their risk finance and corporate resilience strategy. The cyber insurance underwriting process can serve as a key touch point for an organization to assess its cyber practices and coordinate its incident response plan. Because many carriers base premiums in part on security controls and overall exposure, insurance serves as an important incentive to drive behavioral change.[44] Thus, cyber insurance can become an important risk mitigation tool by requiring a company to identify its most vital assets and potential vulnerabilities.[45]

Cyber risk can emanate from a wide array of actors, affect all industries and create both physical and economic harm.

44 For an analytical account on how carriers assess and price cyber risk as well as a description of the insurance market, see: Sasha Romanosky, Lillian Ablon, Andreas Kuehn and Therese Jones (2019). "Content analysis of cyber insurance policies: how do carriers price cyber risk?" Journal of Cybersecurity, Volume 5, Issue 1. tyz00. https://doi.org/10.1093/cybsec/tyz002.

45 For more on the potential for insurance to play a role in risk mitigation and management, see Brandenburg Institute for Society and Security (2017). "Cyber Insurance as a Contribution to IT Risk Management: An Analysis of the Market for Cyber Insurance in Germany." BIGS Policy Paper No. 7, December. https://www.researchgate.net/publication/321938858_Cyber_Insurance_as_a_Contribution_to_IT_Risk_Management_-_An_Analysis_of_the_Market_for_Cyber_Insurance_in_Germany.

Cyber Insurance Market

Total annual cyber premiums have reached an estimated 5 billion USD in 2018. With an annual growth of 20-25 percent, industry observers expect premiums to reach 20 billion USD by 2025.[46,47]

2025
$20 billion

26%

Purchasing cyber coverage remains highest in the United States, where uptake is estimated at 26 percent of organizations (as of 2016). Accordingly, many first-time buyers are still entering the market.[49]

2020
$7.5 billion

Current policyholders are increasing their limits; high limits are available in the market placed in the form of towers between 200 and 500 million USD; **the market's total cyber capacity**—stated but not deployed—is estimated (as of 2017)[48] at

$ 1.4 billion.

2018
$5 billion

2017
$4 billion

46 The Betterley Report (2018). "Cyber/Privacy Insurance Market Survey-2018." June. https://www.irmi.com/docs/default-source/publication-tocs/betterley-report---cyber-risk-market-survey-june-2018-summary.pdf.

47 KPMG (2017). "Seizing the cyber insurance opportunity: Rethinking insurers' strategies and structures in the digital age." Global Strategy Group, KPMG International. https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/07/cyber-insurance-report.pdf.

48 Marsh (2017). Addressing Cyber Risk. https://www.treasury.gov/initiatives/fio/Documents/1-Cyber_Insurance_Market_MarshLLC.pdf.

49 Ibid.

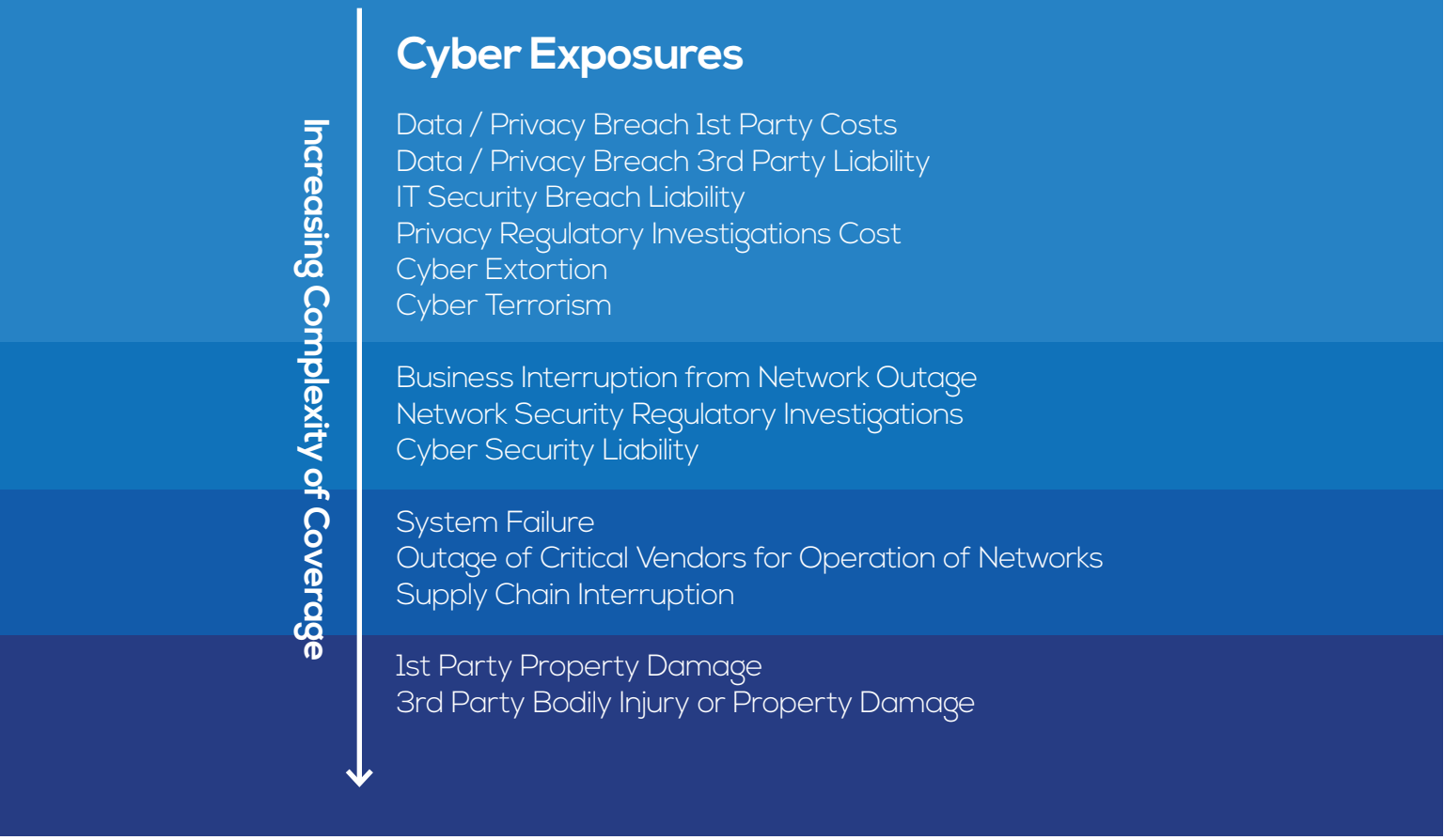


Figure 4: Evolution of Cyber Insurance Coverage (courtesy of Marsh)

For this reason, cyber risk implicates multiple lines of insurance. Insurance companies need to measure and manage aggregated risk in their portfolios, which is associated with correlated loss events and requires a better understanding of how cyber risks themselves are correlated as well as the nature of insureds' relationships with third parties. Insurance coverage can address physical loss, such as a cyber attack on an industrial control system causing a fire or an explosion, which could trigger property or casualty policies. For non-physical perils, such as destruction of data or outage of networks, companies have increasingly turned to cyber insurance to offset the potential financial impacts of business interruption caused by cyber incidents.[50] In terms of first party insurance, these expenses may come in the form of restoring encrypted or corrupted data, legal fees, forensic investigation or responding to notification requirements. Further, in terms of third-party insurance, cyber insurance may also pay defense and liability costs resulting from litigation or reimburse revenues lost or expenses incurred due to a disruption caused to a third party related to a cyber incident.

Previously, growth of the cyber insurance industry stemmed from covering costs and damages incurred by organizations in the wake of the unauthorized release of personal data, known as a "data breach." This can be attributed primarily to regulatory requirements: mandatory data breach notification requirements have historically been one of the biggest drivers for market adoption of cyber insurance in the United States. Similarly, one of the key developments in the EU that is expected to have a significant impact on the cyber insurance market

50 Marsh Risk Management Report (2016). "Benchmarking Trends: Operational Risks Drive Cyber Insurance Purchases." March. https://www.marsh.com/us/insights/research/cyber-benchmarking-trends-2016.html.

is the adoption of legislation specifically addressing information security, namely the NIS Directive and the GDPR. The NIS Directive in particular focuses not only on incidents affecting the confidentiality of data, but also on outages/unavailability of service, which is expected to shape the emphasis of cybersecurity measures—and cyber insurance demand—accordingly.[51] As cyber threats continue to multiply and evolve, cyber coverages have developed to account for new exposures and legal or regulatory complexity. Accordingly, growth in the purchasing of cyber insurance has been facilitated by and will continue to depend on the willingness of leading insurance carriers to adapt coverages to specific risk.

One emerging and quickly expanding coverage in the cyber insurance market is reimbursement for lost revenue or extra expenses resulting from network disruptions of vendors that support the operation of an organization's information technology and the business partners that fulfill essential roles in the insured's supply chain. Over the past few years, a number of insurance carriers have expanded their offerings to include additional services related to building up their customers' cybersecurity posture (e.g., cyber risk assessments and penetration testing) or to support post-incident actions (e.g., incident response services and post-incident communications) and cover related costs. As a result, cyber insurance carriers are requiring additional data on the insured's relationships with these third parties. These include which vendors are most critical to the insured, if the insured has redundancy plans should they lose access to those vendors and how the insured otherwise limits risk by contractual terms. Figure 4 on page 28 summarizes the evolution of cyber insurance offerings.

51 European Union Agency for Network and Information Security (ENISA) (2017). "Commonality of risk assessment language in cyber insurance." November 15. https://www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance.

Systemic Cyber Risk

Managing factors that contribute to systemic cyber risk is a key challenge for the emergent cyber insurance market. Considering the interdisciplinary nature of cyber risk, there is not a coherent pool of expertise with the capability to fully understand and research the market's problem set.[52]

The combination of increasing uptake of cyber insurance as a component of cyber risk management strategies and in the wake of prominent breaches is causing underwriting guidelines to tighten. In particular, changes in the market are occurring following a string of high-profile, high-impact events such as the Equifax data breach and NotPetya cyber attack in 2017, the 2018 Marriott Hotel data breach and others.[53]

Some carriers may limit their appetite for certain critical economic or infrastructure sectors, and many are requesting more information and performing deeper analysis of an insured's perimeter defense, anomaly detection, incident response and business continuity plans. Increasingly, underwriter analysis also reaches beyond technical cyber solutions. For example, underwriters may seek to examine workforce culture and training, which may influence cyber risk as much as security

52 There is an effort underway at Stanford University to bring together various academic disciplines to solve some of the most important questions the cyber insurance sector is facing. See: Falco et. al. (2019). "A Research Agenda for Cyber Risk and Cyber Insurance". The 2019 Workshop on the Economics of Information Security. June.

53 Note that this view is not universally shared; a survey following the 2016 Dyn DDoS attack and the 2017 WannaCry ransomware attack found that for 71 percent of the respondents these events had slight to no impact on underwriting and/or pricing of cyber risk. However, since the 2017 survey, several high-profile cyber attacks have generated insurance claims, which may have an impact on the assessment and underwriting of cyber risks. See: Advisen (2017), "2017 Survey of Cyber Insurance Market Trends," https://partnerre.com/wp-content/uploads/2017/10/PartnerRe-2017-Survey-of-Cyber-Insurance-Market-Trends.pdf.

investment or corporate governance.[54]

Insurers have also started to address the issue of "silent" or "non-affirmative" cyber risk. These are potential cyber-induced losses within traditional lines of insurance that do not explicitly offer cyber coverage. Often, these policies have not excluded cyber perils, and thus could have to pay out for a cyber event that may not have been accurately included in the risk assessment, underwriting and pricing of the traditional policy. As a result, insurers are moving to explicitly include or exclude cyber perils in traditional insurance policies or offer stand-alone policies for cyber coverage ("affirmative cyber").[55]

The cyber market is a principal source of growth for insurance companies. Many carriers are looking to claim a piece. The growing supply drives down policy prices as a natural result of competition. Due to the uncertainty around systemic cyber risk, it is possible that current premiums may not be adequate to cover losses in the event of a catastrophic scenario. Much of the data and modeling for cyber risks draws on past events (as is typical in many other sectors). However, because cyber risk is a rapidly evolving area, predicting loss scenarios on past performance creates uncertainty around the true risk exposure of the cyber insurance market. To deal with this inherent challenge, many insurers and reinsurers are looking for innovative ways to improve their underwriting and risk modeling methodologies.

DATE: **May 2017**	EVENT: **WannaCry**
DAMAGE: **$4 billion**	A ransomware attack that exploited a Microsoft software vulnerability, deploying the EternalBlue exploit code stolen from the U.S. National Security Agency. WannaCry encrypted hundreds of thousands of computers in more than 150 countries.

Mario Tama / Staff / Getty Images

54 European Union Agency for Network and Information Security (ENISA) (2016). "Cyber Insurance: Recent Advances, Good Practices and Challenges." November 7. https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges.

55 Aon (2018). "Managing Silent Cyber A new solution for insurers." https://www.aon.com/getmedia/2b1ad492-dcf0-429e-9eda-828d49b1396a/aon-silent-cyber-solution-for-insurers.aspx.


WANTED
BY THE FBI
PARK JIN H
Conspiracy to Commit Wire Fraud; Conspiracy to Co
(Computer Intrusion)
DESCRIPTION
Aliases: Pak Jin Hek, Jin Hyok Park
Place of Birth: Democratic People's Republic of Korea (North Korea)
Eyes: Brown
Race: Asian
Hair: Black

5 Recommendations

This section contains four recommendations to help the cyber insurance market mature in a healthy, stable manner while promoting increased cybersecurity and resilience.

This report looks to enhance the ability of the cyber insurance market to support cyber resilience efforts, guard against systemic risk and avoid catastrophic losses, by offering the following recommendations:

1. Enhance cyber insurance underwriting ability;
2. Promote a strong and healthy market with positive impacts on society (encouraging new models for cyber resiliency);
3. Increase transparency and uniformity in insurance language; and
4. Increase overall capacity to handle a major, multi-market loss (create a backstop program).

Recommendation 1: Enhance Cyber Insurance Underwriting Ability

Due to the low volume of high-impact claims and high interest among insureds, there has been massive growth in the cyber insurance market. While a dynamic, competitive market with new entrants can lead to greater innovation and efficiency, it can also put downward pressure on pricing and create a "launch now, patch later" approach in the interest of claiming greater market share without adequate attention to risk. The cybersecurity market faced a similar problem, where an overreliance on new technology often led to a lack of risk management strategy. Here, a public-private partnership drove the creation of the risk-based NIST Cybersecurity Framework under the Obama Administration that sought to bridge the divide between executives responsible for corporate risk and technical experts responsible for implementing IT security.[56]

Carriers should utilize a cybersecurity framework and apply it consistently in their underwriting practices. Tools like the NIST Cybersecurity Framework can be used to guide underwriting questions and better educate insureds on how to manage their own cyber risk. Attacking this problem from both the bottom up

56 National Institute for Standards and Technology (NIST) (2018). Cybersecurity Framework Version 1.1. April. https://www.nist.gov/cyberframework.

and top down is the only way to avoid the potential catastrophic losses to the insurance industry. Furthermore, several factors are expected to drive the improvement of the underwriting process as the market matures: (1) the increase in available data to support risk assessments, for instance, the voluntary sharing of insurance-relevant cyber incident and loss data in a standardized format; (2) the development of in-house cybersecurity expertise; and (3) the harmonization of underwriting language and questions on the basis of international security standards or sector-specific requirements and regulations. The cyber insurance industry should leverage these market drivers to both improve the collection of underwriting information and the risk assessment practices. Promoting secure, anonymized data sharing among stakeholders and extracting meaningful data from incident reporting schemes introduced by regulations will support these efforts.

Recommendation 2: Promote a Strong and Healthy Market with Positive Impacts on Society

With greater interest in cyber insurance, new business models are rising to meet demand. Brokers are increasingly offering risk management consultation to their clients to help them identify their cyber exposures and policy limit needs. Advanced analytics can support this conversation, by allowing underwriters to tap their claims and client datasets to provide benchmarking of financial risk for their clients. Carriers have long worked to promote "loss control" products and services to reduce claims and make their clients a lower risk investment. Some carriers, technology and cybersecurity companies are now working together to bring mitigation and incident response services to their clients to limit the damage from a cyber incident and increase their policy holder's resilience.[57]

Finally, there are new entrants to the market exploring innovative models to use data from the insurance industry to tie financial incentives directly to an organization's security performance.[58] With the complex and evolving nature of cyber incidents, new approaches have the potential to change how cyber risk is addressed as the insurance market leverages advanced analytics for gathering and analyzing data that can provide continuous, real-time understanding of cyber risk.

Recommendation 3: Increase Transparency and Uniformity in Insurance Language

Currently, cyber insurance policy language and coverage varies.[59] This creates uncertainty about what is covered and reduces the effectiveness of insurance in helping companies

57 For example, Cisco, Apple, Aon and Allianz recently announced a risk management initiative integrating all their services to improve resiliency. For more information, see https://www.apple.com/de/newsroom/2018/02/cisco-apple-aon-allianz-introduce-a-first-in-cyber-risk-management/.

58 Ulrik Franke (2017). "The cyber insurance market in Sweden." Computers & Security, 68: 130-144. https://doi.org/10.1016/j.cose.2017.04.010.

59 See European Union Agency for Network and Information Security (ENISA) "Commonality of risk assessment language in cyber insurance." https://www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance.

transfer their cyber risk. Buyers of cyber insurance need to look closely at nuances of coverage when comparing policies. Harmonization in this area will drive down uncertainty and increase the insurance market's effectiveness.

In particular need of attention is the war exclusion, which limits payment for losses caused by an act of warfare and is often included in property insurance policies that can also include cyber coverage. Since there is no agreed definition of what constitutes "cyber war," insurers rely on old definitions from kinetic war and the Law of Armed Conflict. State (and state-sponsored) cyber attacks can lead to significant damages but are hard to classify as "acts of war." This ambiguity may tempt insurers to reject claims for damages caused by attacks initiated by a state actor.[60]

Some have argued that the war exclusion should not apply to cyber attacks.[61] At a minimum, insurers should use clear language to describe what triggers a given exclusion and have clear and uniform definitions for key terms such as "act of war," "state actors" and "state cyber attacks."

Recommendation 4: Increase Overall Capacity to Handle a Major, Multi-market Loss

The 9/11 terrorist attacks caused a tragic loss of life and massive destruction of property in downtown New York City, but less discussed is the effect on the insurance market. Reinsurers suffered massive losses from property claims and insurance providers began including exclusions for terrorist events in their policies. This had the potential to halt the reconstruction of Manhattan and severely affect the U.S. property market. In response, the U.S. Congress passed the Terrorism Risk Insurance Act (TRIA) to provide a backstop for insurance claims related to acts of terrorism.[62] However, no incidents in the U.S. have ever been certified as terrorist acts for the purposes of TRIA.

In December 2016, the U.S. Treasury Department determined that stand-alone cyber liability insurance policies fall under the purview of TRIA.[63] Under the new guidance, insurance providers are required to offer terrorism risk insurance and cover commercial property and casualty losses in instances of certified acts of cyber terrorism.[64]

60 The current lawsuit filed by Mondelez against Zurich American Insurance illustrates the ambiguity of the classification of acts of war in cyberspace and the potential implications for the cyber insurance industry. Zurich denied Mondelez coverage for damage caused by the NotPetya cyber attack, citing the war exclusion in the property policy held by Mondelez, which included cyber coverage. While several western intelligence agencies have publicly attributed NotPetya to the Russian government, Zurich invoking the war exclusion raises questions about whether such statements attributing a cyber attack to a state will be sufficient for insurers to deny coverage under their war exclusions, which would have significant implications for cyber insurance policies. For more see: Steve Evans (2018). "Mondelez's NotPetya cyber attack claim disputed by Zurich: Report." Reinsurance News. December 17. https://www.reinsurancene.ws/mondelezs-notpetya-cyber-attack-claim-disputed-by-zurich-report/.

61 "NotPetya Was Not Cyber 'War.'" Marsh Insights. August 2018. https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/NotPetya-Was-Not-Cyber-War-08-2018.pdf.

62 Baird Webel (2019). "The Terrorism Risk Insurance Act (TRIA)," Congressional Research Service. February. https://crsreports.congress.gov/product/pdf/IF/IF11090.

63 Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program, https://www.federalregister.gov/documents/2016/12/27/2016-31244/guidance-concerning-stand-alone-cyber-liability-insurance-policies-under-the-terrorism-risk.

64 Jason Krauss (2017). "Careful how you code: Cyberterrorism coverage under TRIA and stand-alone cyber policies." Decode Cyber Brief — Summer 2017, Willis Towers Watson. https://www.willistowerswatson.com/en-US/insights/2017/07/decode-cyber-brief-careful-how-you-code.

For certified acts of terrorism, 80 percent of losses are reinsured by the U.S. government while the remaining 20 percent are covered by the private insurance market once losses exceed 200 million USD.[65] Despite the affirmed cyber coverage under TRIA, concerns regarding the insurance market's capacity to absorb catastrophic losses are not fully addressed. Since no incident, physical or otherwise, has been certified as an act of terrorism under TRIA, it seems unlikely that a future major cyber attack will invoke TRIA coverage.

In the UK, a similar but more streamlined terrorism insurance backstop exists in the form of Pool Re, established in 1993 in response to several years of terrorist incidents related to the Northern Ireland conflict. Pool Re was formed by the insurance industry in the UK and backed by the UK government, creating a hybrid public-private sector solution to terrorism risks and insurance.[66] Under the Pool Re scheme, any insurance company can join the private pool, although membership is not mandatory. Members are required to provide terrorism coverage, and they are reinsured for material damage and business interruption (with further terms detailed in the pool's underwriting manual).[67] In the event of a terrorist attack, the UK government must certify the event to be an act of terror in order for coverage to be eligible under the Pool Re scheme. A variety of incidents have already been certified. Reinsurance for a qualifying event is limited to member companies, subject to a maximum loss rate per event and an annual aggregate limit.[68]

A similar model could work in the cyber insurance sector. For example, Singapore's Ministry of Finance announced the creation of the world's first commercial cyber risk pool in October 2018, which would commit up to 1 billion USD in capacity for cyber coverage, and is backed by traditional insurance as well as insurance linked securities (ILS).[69] Furthermore, with the future development of cyber insurance in mind, the industry should explore ILS and catastrophic bond markets as a means to strengthen the cyber insurance market and add additional capacity. ILS, through strong capital markets, can help establish new classes of insurance and provide coverage for underinsured areas.[70]

Due to the innovative and evolving nature of the insurance market, the insurance industry is not currently seeking to establish a backstop program. Nevertheless, with the increasing accumulation of cyber risk and cyber-related dependencies, incidents may result in claims beyond the insurance market's current capacity. Governments should consider creating a targeted backstop program for systemic cyber incidents, referred to here as a Cyber Risk Insurance Act (CRIA).

65 Note that the backstop to insurers decreased from 85 percent in 2015 to 80 percent in 2020, while the trigger for losses of certified events increased from 100 million USD in 2015 to 200 million USD in 2020.

66 For more information, see the Pool Re website https://www.poolre.co.uk/.

67 OECD International Platform on Terrorism Risk Insurance. United Kingdom – Terrorism Risk Insurance Programme. https://www.oecd.org/daf/fin/insurance/UK-terrorism-risk-insurance.pdf.

68 Ibid.

69 Gabriel Olano (2018). "Singapore launches first commercial cyber risk pool." Insurance Business Asia. October 31. https://www.insurancebusinessmag.com/asia/news/cyber/singapore-launches-first-commercial-cyber-risk-pool-115040.aspx.

70 Artemis (2018). "Closing the insurance gap needs capital market support." October 23. http://www.artemis.bm/news/closing-the-insurance-gap-needs-capital-market-support-lloyds/; BNY Mellon (2016). "Insurance Linked Securities – Cyber Risk, Insurers, and the Capital Markets." https://www.bnymellon.com/emea/en/_locale-assets/pdf/our-thinking/insurance-linked-securities-cyber-risk-insurers-and-the-capital-markets.pdf.

Such a program would include the following components:

1. **Private Reinsurance Pool:** Authorization for the government to enter into an agreement with a private reinsurance pool to support cyber coverage above a certain threshold. The agreement would establish a threshold of losses stemming from a cyber incident, which insurers and the reinsurance pool would be responsible for paying. Should losses from a systemic cyber incident exceed the threshold, the government would cover some or all of the remaining claims.
2. **Incident Certification:** Prior to the coverage of losses by the government, a designated senior government official would certify that the systemic cyber incidents resulted in catastrophic losses to the insurance industry and are eligible for coverage under the legislation.
3. **Mandatory Coverage:** A requirement that all primary insurers offer coverage to commercial clients for losses caused by cyber incidents that does not differ materially from the terms, amounts and other coverage limitations applicable to losses arising from non-cyber events. No one would be required to purchase cyber insurance.
4. **Multi-line Coverage:** The reinsurance pool should consider the lines of business that are critical to the ongoing functioning of the U.S. economy. This includes worker's compensation, property, general liability, aviation, marine, medical malpractice, cyber and other lines of insurance. The federally backstopped reinsurance would ensure that insurers had sufficient capacity to continue offering coverage to the market and prevent material economic disruption following a systemic cyber incident.
5. **Loss Prevention:** Risk-reduction provisions—such as economic incentives for consumers, corporate customers and product/service providers to invest in cybersecurity—would also be specified in the legislation.

Handout / Getty Images

DATE:	EVENT:
July 2010	**Stuxnet**
DAMAGE: **Unknown**	The Stuxnet worm took advantage of several zero-day vulnerabilities, including a vulnerability in Siemens industrial control systems, to grant itself privileges to manipulate computer-controlled industrial processes. The worm was used to destroy centrifuges in an Iranian uranium enrichment facility.

6 Conclusion

Cyber insurance is an important tool to help reduce and protect against systemic cyber risks and potential catastrophic losses.

As the possibility of systemic cyber risk grows, the insurance industry must continue to assess how to respond to potential disruptions and financial damage. This report outlines two major ideas that could help them do so.

First, for cyber risks to have catastrophic impact at the level of systemic risk, they must be amplified by a high level of **criticality**, **interconnectedness** and **homogeneity** as well as a lack of **resilience**. These, in concert with an incident that is **infectious**, **destructive** and **sophisticated**, can cause the impacts of an event or series of events to bleed over into different sectors. Interconnectedness is especially noteworthy as it can amplify cascading effects across a sector or function, such as an attack on the SWIFT system that affects the global economy, or a common vulnerability in Linux or Windows that is present across the Internet.

Second, the insurance industry has a dual position in the face of systemic cyber risk. It has the potential to be significantly damaged from such systemic cyber risk—an event with large contagion factors that hits the entire insurance market at once could trigger the systemic risk discussed in this report. For years, experts have discussed the possibility of a major, catastrophic cyber event that would have unprecedented impacts. The evolution in cyber weapons and the way attacks are carried out requires evolution in approaches to mitigate these threats. Recommendation 4 in this report—creating a government backstop for systemic cyber incidents—aims to address this potential damage to the insurance market. In particular, it has emerged from the understanding that the impacts of future cyber attacks cannot be predicted. Even as cyber risk modeling continues to improve, the constant evolution of these threats, as well as emerging risk, leave a degree of uncertainty that will persist in evaluations of systemic cyber risk.

Conversely, the insurance industry also has the ability to help address the underlying factors that contribute to systemic cyber risk. Through strong underwriting and risk modeling, insurance companies have the potential to not only shield themselves from the type of catastrophic event

mentioned above, but also drive down their customers' exposure. To this end, the insurance industry has an interest in ensuring the cyber insurance market develops in a healthy, sound way that is based on accurate risk assessment and improved modeling. The recommendations provided in this report are designed to ultimately foster a healthy, resilient cyber insurance market.

In the absence of government regulations for cybersecurity (particularly in the U.S.), cyber insurance has emerged as an authority to promote and enforce certain cybersecurity standards. Using existing cybersecurity standards in underwriting processes (as elaborated in Recommendation 1) can contribute to the solidification of these standards and promote better cyber hygiene in insureds and even for their customers. While this can raise the overall level of cybersecurity and reduce risk, the government's role in setting and enforcing cybersecurity standards should not be overlooked. Government standards bodies are seen as legitimate actors in this space, and if they are able to develop risk-informed cybersecurity standards, insurance companies can play a role in promoting and implementing these standards. Allowing insurance companies to become de facto regulators as the sole authority setting minimum acceptable cybersecurity standards—which would ultimately be governed by the market—is not a permanent solution to the continuing challenge of improving general cybersecurity and cyber resilience across all sectors.

The complex nature of cyber systems and continuing innovation and evolution in technology ensure permanent uncertainty in estimating cyber risk. However, the framework outlined in this report serves to provide insight into the factors and actions that can increase—or mitigate—such risk. Cyber insurance is an important tool to help reduce and protect against systemic cyber risks and potential catastrophic losses. In an environment characterized by increasing cyber threats and a growing reliance on technology and global interconnectedness, a better understanding of systemic cyber risks, bolstered by a healthy, risk-informed cyber insurance market, is critical to creating capacity and resilience.

Board of Directors

LEADERSHIP

Ross Perot, Jr. (U.S.)
Chairman
EastWest Institute
Chairman
Hillwood Development Co. LLC

R. William Ide III (U.S.)
Counsel and Secretary
Chair of the Executive Committee
EastWest Institute
Partner
Akerman LLP

Amb. Cameron Munter (U.S.)
CEO and President
EastWest Institute

CO-FOUNDERS

John Edwin Mroz† (U.S.)
Former President and CEO
EastWest Institute

Ira D. Wallach† (U.S.)
Former Chairman
Central National-Gottesman Inc.

MEMBERS

Haifa Al Kaylani (Lebanon/Jordan/U.K.)
Founder and Chairman
Arab International Women's Forum

Peter A. Altabef (U.S.)
Chairman and CEO
Unisys Corporation

Tewodros Ashenafi (Ethiopia)
Chairman and CEO
Southwest Energy (HK) Ltd.

Mark Joseph Bild (U.S.)
Managing Partner
BAI Corporation

Mary McInnis Boies (U.S.)
Counsel
Boies, Schiller & Flexner LLP

Sir Peter Bonfield (U.K.)
Chairman
NXP Semiconductors

Matt Bross (U.S.)
Chairman and CEO
Compass-EOS

Robert N. Campbell III (U.S.)
Founder and CEO
Campbell Global Services LLC

Maria Livanos Cattaui (Switzerland)
Former Secretary-General
International Chamber of Commerce

Michael Chertoff (U.S.)
Executive Chairman and Co-Founder
The Chertoff Group
Former Secretary of the U.S. Department of Homeland Security

David Cohen (Israel)
Chairman
F&C REIT Property Management

Roger Cohen (U.S.)
Op-Ed Columnist
The New York Times

Joel H. Cowan (U.S.)
Professor
Georgia Institute of Technology

Addison Fischer (U.S.)
Chairman and Co-Founder
Planet Heritage Foundation

Olivia Fischer (U.S.)
Philanthropist
Planet Heritage Foundation

Hon. Steven S. Honigman (U.S.)
Founding Member
Quieter Oceans LLC

Dr. Hu Yuandong (China)
Chief Representative
UNIDO ITPO-China

John Hurley (U.S.)
Managing Partner
Cavalry Asset Management

Ralph Isham (U.S.)
Managing Director
GH Venture Partners LLC

Anurag Jain (U.S.)
Chairman
Access Healthcare

Gen. (ret.) James L. Jones (U.S.)
Former U.S. National Security Advisor
Former Supreme Allied Commander Europe
Former Commandant of the Marine Corps

George Kadifa (U.S.)
Managing Director
Sumeru Equity Partners

Zuhal Kurt (Turkey)
Chairman of the Board
Kurt Group

Gen. (ret.) T. Michael Moseley (U.S.)
President and CEO
Moseley and Associates, LLC
Former Chief of Staff
United States Air Force

Karen Linehan Mroz (U.S.)
President
Roscommon Group Associates

F. Francis Najafi (U.S.)
CEO
Pivotal Group

Amb. Tsuneo Nishida (Japan)
Professor
The Institute for Peace Science at Hiroshima University
Former Permanent Representative of Japan to the United Nations

Admiral (ret.) William A. Owens (U.S.)
Chairman
Red Bison Advisory Group LLC

Dr. William J. Parker III (U.S.)
President and CEO
National Defense University Foundation

Sarah Perot (U.S.)
Director and Co-Chair for Development
Dallas Center for Performing Arts

Kathryn Pilgrim (U.S.)
International Writer

Laurent M. Roux (U.S.)
Founder and President
Gallatin Wealth Management, LLC

Ikram ul-Majeed Sehgal (Pakistan)
Chairman
Security & Management Services Ltd.

Amb. Kanwal Sibal (India)
Former Foreign Secretary of India

Kevin Taweel (U.S.)
CEO
Asurion

Alexander Voloshin (Russia)
Chairman of the Board
JSC Freight One (PGK)
Non-Executive Director
Yandex Company

Adm. Patrick M. Walsh (U.S.)
Vice President
U.S. Navy and Marine Corps Services
Boeing Global Services

Amb. Zhou Wenzhong (China)
Secretary-General
Boao Forum for Asia

NON-BOARD COMMITTEE MEMBERS

Hilton Smith, Jr. (U.S.)
President and CEO
East Bay Co., LTD

CHAIRMEN EMERITI

Martti Ahtisaari (Finland)
2008 Nobel Peace Prize Laureate
Former President of Finland

Berthold Beitz† (Germany)
President
Alfried Krupp von Bohlen und Halbach-Stiftung

Ivan T. Berend (Hungary)
Professor
University of California, Los Angeles

Francis Finlay (U.K.)
Former Chairman
Clay Finlay LLC

Hans-Dietrich Genscher† (Germany)
Former Vice Chancellor and Minister of Foreign Affairs of Germany

Donald M. Kendall (U.S.)
Former Chairman and CEO
PepsiCo Inc.

Whitney MacMillan (U.S.)
Former Chairman and CEO
Cargill Inc.

Mark Maletz (U.S.)
Former Chairman, Executive Committee
EastWest Institute
Senior Fellow
Harvard Business School

George F. Russell, Jr. (U.S.)
Chairman Emeritus
Russell Investment Group
Founder
Russell 20-20

H.E. Dr. Armen Sarkissian (Armenia)
President of Armenia

DIRECTORS EMERITI

Jan Krzysztof Bielecki (Poland)
CEO
Bank Polska Kasa Opieki S.A.
Former Prime Minister of Poland

Emil Constantinescu (Romania)
President
Institute for Regional Cooperation and Conflict Prevention (INCOR)
Former President of Romania

William D. Dearstyne (U.S.)
Former Company Group Chairman
Johnson & Johnson

Stephen Heintz (U.S.)
President
Rockefeller Brothers Fund

Amb. Wolfgang Ischinger (Germany)
Chairman
Munich Security Conference

John W. Kluge† (U.S.)
Former Chairman of the Board
Metromedia International Group

Amb. Maria-Pia Kothbauer (Liechtenstein)
Ambassador of Liechtenstein to Austria, the OSCE and the United Nations in Vienna

William E. Murray† (U.S.)
Former Chairman
The Samuel Freeman Trust

John J. Roberts (U.S.)
Senior Advisor
American International Group (AIG)

Daniel Rose (U.S.)
Chairman
Rose Associates Inc.

Leo Schenker (U.S.)
Former Senior Executive Vice President
Central National-Gottesman Inc.

Mitchell I. Sonkin (U.S.)
Managing Director
MBIA Insurance Corporation

Thorvald Stoltenberg† (Norway)
Former Foreign Minister of Norway

Liener Temerlin (U.S.)
Chairman
Temerlin Consulting

John C. Whitehead† (U.S.)
Former Co-Chairman
Goldman Sachs
Former U.S. Deputy Secretary of State

† Deceased

Acknowledgments

This report was prepared by the EastWest Institute and authored by **Davis Hake**, **Andreas Kuehn**, **Abagail Lawson** and **Bruce McConnell**. The authors are extremely grateful for the advice provided by the experts listed below. Their inclusion here does not mean that they support or agree with any of the report's statements, proposals, recommendations or conclusions. In particular, the report greatly benefited from the expertise and experience of the leaders of the EWI Breakthrough Group on Systemic Risk and Cyber Insurance, who led working sessions and provided key inputs to the paper:

Erin English, Senior Security Strategist, Microsoft
Davis Hake, Co-Founder, Arceo.ai
Marsh & McLennan Companies: **Matthew P. McCabe**, Senior Vice President, Marsh; **Jeremy Platt**, Managing Director, Guy Carpenter; **John Plaisted**, Marsh Risk Consulting

The foundations of the paper were formed by a series of four workshops—in New York, Palo Alto, Washington, D.C. and Berkeley—convened by the EastWest Institute from October 2016 to January 2018. These workshops brought together over 75 experts from the insurance, reinsurance, technology, financial services and energy sectors, as well as government and academia to explore and increase the understanding of systemic cyber risk and cyber insurance.

The outcomes of the 2016 and 2018 workshops are available in summary form on EWI's website: https://www.eastwest.ngo/info/systemic-risk-and-cyber-insurance.

The following experts provided substantive commentary and advice during the development of the report:

Aaron Clark-Ginsberg, Associate Social/Behavioral Scientist, RAND Corporation
Athanasios Drougkas, NIS Expert, European Union Agency for Network and Information Security (ENISA)
Gregory Falco, Cybersecurity Postdoctoral Fellow, Center for International Security and Cooperation, Stanford University
Asaf Lubin, Cybersecurity Policy Postdoctoral Research Fellow, The Fletcher School of Law and Diplomacy, Tufts University
Thomas Maillart, Senior Lecturer, Information Science Institute, University of Geneva
Pythagoras Petratos, Researcher, Blavatnik School of Government, University of Oxford
Sasha Romanosky, Policy Researcher, RAND Corporation
Catherine Rudow, Vice President, Cyber Insurance, Nationwide
Camelia Simoiu, PhD Candidate, Computational Social Science, Stanford University
Russell Thomas, Principal Modeler Cyber Risk, RMS
Matthias Weber, former Chief Underwriting Officer, SwissRe
Gordon Woo, Catastrophist, RMS

The following EWI associates provided invaluable support and assistance for this report: **Michael Depp**, **Conrad Jarzebowski**, **Anneleen Roggeman**, **Alex Schulman** and **Dragan Stojanovski.**

The EastWest Institute works to reduce international conflict, addressing seemingly intractable problems that threaten world security and stability. We forge new connections and build trust among global leaders and influencers, help create practical new ideas, and take action through our network of global decision-makers. Independent and nonprofit since our founding in 1980, we have offices in New York, Brussels, Moscow and San Francisco.

EastWest Institute
10 Grand Central
155 E. 44th Street, Suite 1105
New York, NY 10017 U.S.A.
+1 (212) 824-4100

communications@eastwest.ngo
www.eastwest.ngo

DATE: **April 2014**	EVENT: **Heartbleed**
DAMAGE: **$500 million**	A vulnerability in the OpenSSL cryptographic software library that allowed the theft of sensitive information normally encrypted. Years later, hundreds of thousands of systems remain unpatched and vulnerable.

Jasmin Merdan / Getty Images

Global Cooperation in Cyberspace

SUPPORTERS:

Microsoft
Unisys
Marsh & McLennan
JPMorgan Chase
The Hague Centre for Strategic Studies
Huawei Technologies
NXP Semiconductors
Qihoo 360
CenturyLink

PARTNERS:

William and Flora Hewlett Foundation
IEEE Communications Society
Global Forum on Cyber Expertise
Munich Security Conference
M³AAWG
The Open Group
Fudan University
University of New South Wales
Center for Long-Term Cybersecurity, University of California, Berkeley

New York | Brussels | Moscow | San Francisco
www.eastwest.ngo | **t:** @EWInstitute | **f:** EastWestInstitute