CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

OCTOBER 2018

Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance

Ariel E. Levite, Scott Kannry, and Wyatt Hoffman

Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance

Ariel E. Levite, Scott Kannry, and Wyatt Hoffman

For your convenience, this document contains hyperlinked source notes indicated by this teal colored text.

© 2018 Carnegie Endowment for International Peace. All rights reserved.

Carnegie does not take institutional positions on public policy issues; the views represented herein are the authors' own and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Carnegie Endowment for International Peace. Please direct inquiries to:

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: +1 202 483 7600
F: +1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

CONTENTS

Executive Summary

The private sector is struggling to contend with the growing scope, scale, and complexity of cyber risks to corporations' finances, reputation, and even property. These risks cut across multiple areas of business operations and permeate relationships with suppliers, customers, and third parties. Most governments are by now aware that cyber threats can severely damage and disrupt their economies and infrastructure, and many invest significant effort and resources to confront this danger. Yet virtually all face serious bandwidth limitations in addressing cyber threats to private entities. Concerns over potential escalation or blowback if they pursue or retaliate against foreign hackers, including potential states or proxies, further dampen governments' enthusiasm for defending the private sector. Furthermore, those governments that seek to address private sector cyber vulnerabilities face serious pushback against onerous regulations and reservations about creating a moral hazard if they assume responsibility for protecting the private sector. These reasons and others have made a governmental solution to this worsening private sector predicament unsatisfactory—a situation that is unlikely to fundamentally change for the foreseeable future.

Faced with this sobering reality, the more resourceful and sophisticated private sector entities are scaling up their own efforts to address cyber threats. In addition to a range of security measures, many have turned increasingly to the risk challenging mechanism offered by cyber insurance policies. Yet the cyber insurance coverage presently available provides only a limited, uncertain, and ad hoc solution. The insurance industry harbors far greater potential to address the cybersecurity challenge. Historically, insurance has played a crucial role in understanding, managing, and mitigating the risks arising from emerging domains of human activity, particularly in the context of evolving technologies. This holds true for cyberspace, where insurance has the potential to assume a more fundamental role in reshaping the risk landscape. While this potential has largely gone unexplored, its historical track record in other domains suggests that the insurance industry could perform six core cyber risk mitigation functions: (1) engineering risks, (2) channeling corporate risk, (3) managing systemic risks, (4) harnessing collective security insights, (5) shaping broader risk trends, and (6) harmonizing risk-related standards and practices internationally.

The current state of cyber insurance remains far from the ideal role envisioned here. This paper analyzes the range of barriers that stand in the way of a properly functioning cyber insurance market—including practical, technical, operational, and strategic challenges, within and outside the insurance industry—and explores a series of individual and complementary efforts by the insurance industry, governments, vendors of information and communications technologies (ICTs), and other key stakeholders in the private sector toward realizing the full potential of insurance to reshape the risk environment. Cyber insurance will ultimately be indispensable in a broader solution to the

escalating cyber risk challenge. Harnessing its full potential will be imperative not only for managing corporate cyber risks, but for preventing potential systemic cyber incidents of growing concern for governments and the private sector alike.

Unlocking the Potential of Cyber Insurance: Complementary Efforts by Governments and the Insurance Industry	
Actions by the Insurance Industry:	**Actions by Governments:**
Adjust recruitment and training to enhance cyber expertise and expand collaboration with cyber risk and threat intelligence professionals	Relax barriers to cyber risk information sharing among insurers
Develop specialized modalities for dialogue with clients on cyber vulnerability and resilience	Expand dialogues on cyber risks and resiliency measures with private sector entities, especially insurers
Simplify procedures and enhance dialogue with policyholders on transparency of contracts, claims, and payments	Standardize reporting requirements for publicly traded companies on cyber risk management practices, resilience measures, and breaches
Promote and apply standardized, innovative tools and metrics for assessing cyber vulnerability, security and resilience, and organizational maturity linked to underwriting diverse cyber coverages	Broaden efforts, including through procurement processes, to encourage private sector development of standardized (and ideally internationally harmonized) criteria for certifying cybersecurity maturity of products and services
Enhance information exchange and sharing of best practices to inform assessment and underwriting internationally	Introduce governmental backstops for catastrophic cyber risk, conditional upon certain underwriting requirements
Promote cyber resilience measures to prevent cascading and aggregation risks due to widespread reliance on common platforms and service providers	Cautiously explore cyber liability provisions as incentives for vendors to enhance their efforts to mitigate and channel their cyber risk exposure
Partner with key vendors of ICT/industrial control systems and cloud services to enhance their cyber integrity throughout product life cycles	

Introduction

As human activity continues to migrate to cyberspace, many services and functions that are vital to individuals, organizations, institutions, and society as a whole have become much more dependent on the cyber world.[1] One aspect of this trend is the way in which the global economy increasingly relies upon the internet to propel economic growth.[2] As enterprises tie more equities to intangible assets such as intellectual property and data, factors that affect these resources have greater influence, and increasingly control, over physical assets and operations. Moreover, such factors have growing cognitive effects on how people think and interact within society. The meteoric rise in the number, type, and uses of connected devices—from smartphones to home appliances to automobiles—as well as the rapid growth in the role that artificial intelligence plays in facilitating autonomous behavior, are indicators of this functional and structural shift from physical space to the logical and cognitive layers of cyberspace.

Unsurprisingly, this transition has both positively and negatively affected human interactions. Among the negative effects are efforts by individuals, private entities, and even governments to exploit these trends to promote their ideological, political, strategic, and economic interests within and through cyberspace. Some of the most worrisome manifestations of these actions include cyber crime, cyber espionage, and cyberwarfare. In 2017, for instance, cyber attacks cost financial institutions alone over $18 billion.[3] But cyber risks are not confined to malicious activity, as flaws in product development or accidental misuse create equally worrisome vulnerabilities. Consequently, individuals and corporations currently face acute cyber risks to their data (confidentiality, availability, and integrity), operations, and provided and consumed services.

Cyber risks increasingly have a bearing on corporate performance, well-being, and in extreme cases even survival. A nascent market for cyber insurance has already emerged alongside other mechanisms for mitigating and channeling these risks. While the appeal of insurance to address this challenge is growing, efforts to unlock its potential thus far have generally been rather narrowly focused on its traditional role in engineering and channeling risk. Recent studies by the Organization for Economic Cooperation and Development (OECD) and the Geneva Association have detailed the current state of cyber insurance, barriers to its maturation, and potential policy solutions.[4] The present study concurs with many of their sound observations and important recommendations. However, it aims more ambitiously to broaden the aperture through which cyber insurance is viewed as an essential element of an approach to confront the global cybersecurity challenge.

Governments and the private sector must collaborate to realize the considerable potential inherent in the insurance industry to not only diminish private sector cyber risks but also prevent systemic cyber

incidents of growing concern to both. Unlocking this potential begins with an understanding of the scope of the cyber risk challenge and the dynamics shaping it.

The Cyber Risk Environment

In the U.S. market alone, the total number of cyber insurance claims came close to doubling between 2016 and 2017, from 5,955 to 9,017.[5] Although this indicator only partly illustrates the present magnitude of cyber threats, it nonetheless suggests the pace at which this problem is growing. Yet for a number of profound reasons, governments and corporations have found it difficult to satisfactorily address and respond to cyber threats:

- *Commercial incentives.* As companies introduce and expand the use of connectivity features such as remote access to data, processes, services, and products, these more numerous points of contact create more cyber attack vectors. Vendors of information and communications technology (ICT) products and services have similar economic incentives to roll out new technological features quickly, and this speed comes at the expense of cybersecurity. These incentives also account for at least some procrastination—up to and including outright renunciation of responsibility—in addressing cybersecurity vulnerabilities, especially in older (and therefore less economically viable) products. This problem is especially acute among smaller and less-sophisticated players, which are common in the Internet of Things sphere. Although individual and corporate activity benefit economically from their greater dependence on ICTs and industrial control systems (ICS), they face growing exposure to cyber risks to their integrity and reliability. The consequences of cyber events also have expanded, with one particularly visible example being the effect of computer glitches on the grounding of airline operations.[6]
- *Technical limitations*. Due to the sheer complexity of ICTs, testing and verifying the integrity and security of cyber systems is inherently challenging. As these systems have grown in complexity and have become subject to more frequent modification, preventing weaknesses from creeping into ICTs has become exceedingly difficult.
- *The appeal for intelligence, military, and law enforcement operations*. The volume and quality of human activity in cyberspace has attracted significant government attention. As more government entities worldwide enter the field or expand their existing footprint, they may be tempted to seize or hold onto existing vulnerabilities and even create new ones. They may also deploy more sophisticated tools for harnessing these vulnerabilities, rather than striving to eliminate them.

- *The lure for criminals, terrorists, hacktivists, and other potentially malicious users.* All of these groups can and have used cyberspace to promote their diverse aims. The present payoff matrix of such actions—with high potential yield and low odds of getting caught and paying a serious penalty for cyber actions—increases its appeal.
- *The broad dissemination of highly potent cyber attack tools.* These tools include those that have been leaked or stolen from leading nations' cyber weapon arsenals, as well as those that have been reverse-engineered by other entities.
- *The growing potential for systemic and cascading impacts of cyber incidents.* This is driven by multiple, intertwined trends: widespread reliance upon a limited number of common hardware and software platforms and services; market consolidation in key areas of the ICT sector; the creation of single points of failure for entire industries; complex, globalized supply chains; and the ever-expanding interconnectedness of systems and networks, among others. At the same time as the scope and scale of connected devices has rapidly grown with the Internet of Things, these connections have penetrated deeper into the physical world, including in the manufacturing sector, industrial operations, and key industries such as aerospace. Taken together, these trends generate new possibilities for cyber attacks to evolve and propagate widely and unpredictably throughout the ecosystem and cause broader ripple effects.[7] In recent years, this phenomenon has appeared repeatedly, as in the rapid spread, globally, of recent attacks presumably conducted against Ukrainian assets.[8]
- *Leveraging machine learning.* Looking ahead, the role that machine learning may play in the cybersecurity domain could not only help defenders but also benefit attackers, improving the sophistication (for example, tailoring) and efficiency of their actions.

In spite of these concerns, the current cybersecurity picture is not entirely bleak. In recent years, multiple governments have acknowledged the growing cyber threats and attendant risks to their private sectors. This awareness has yielded government policies, regulation, and legislation—as well as the creation of dedicated institutions and other initiatives—to protect their national cyberspace, their citizens, and their economies from exploitation by malicious cyber actors. Numerous and diverse government and corporate efforts are under way to try to ease this predicament. Some have attempted to track down and prosecute cyber criminals; others have created structures to foil and respond to especially egregious attacks; still others have promoted better cybersecurity practices across the entire ecosystem. Some of the more sophisticated players in the corporate world have established or expanded their own cyber threat intelligence operations and cybersecurity practices applied to their own networks, products, and services and have extended these throughout their supply chain and to customers. Some of these efforts have shown real promise for limiting or at least channeling cyber risks. For example, many larger players in the ICT/ICS space have been developing

more sophisticated standards and practices to enhance the security and reliability (as well as the performance) of cyber products.[9] The importance of and benefits from these efforts should be neither discounted nor discouraged.

On balance, though, the dynamics and incentive structure that have shaped the evolution of cyberspace do not leave much room for optimism that the cyber risk situation will fundamentally change for the better anytime soon. This sobering assessment reflects an awareness of the motivations that drive human and state action, as well as the unending competition between attackers and defenders. It also stems from a significant trait in human nature, because failure is inevitable in systems (especially complex ones) designed by humans. Recent trends in cyber attacks suggest that this point is not lost on aggressors, who correspondingly have chosen to direct their efforts at human attack surfaces. These circumstances create cyber vulnerabilities that could be exploitable for adversarial actions and are far more challenging to neutralize.

The Government Predicament

Strategic, political, and structural reasons hamper governments' capacity and will to diminish the scope and severity of cyber attacks against the private sector, let alone to disincentivize attackers:

- *Bandwidth limitations*. Governments are naturally predisposed to first address cybersecurity risks to their own networks and services, and then tackle such threats to critical infrastructure and other forms of potentially systemic and catastrophic risks. The remaining threats to corporations, civil society, and individuals are a much lower priority.
- *Moral hazard*. For cultural, ideological, political, and economic reasons, governments vary in their willingness and capacity to assume financial and other risks to the private sector. Even those that do contemplate offering some form of insurance of last resort have limited willingness to underwrite private sector risks. At least some of these governments are concerned that by assuming significant responsibility to address private sector cyber risks, they would encourage undue complacency among these entities, thereby enabling them to avoid taking necessary precautions, building resiliency, and protecting their own equities. This philosophy holds true for virtually all threats to property; cyber threats are no exception.
- *Strategic ambivalence and priorities*. Because of the inherent trade-off, tension, and synergy between offensive and defensive considerations, some forms of government behavior in cyberspace accentuate rather than ease the private sector's cybersecurity predicament. Sophisticated cyber tools have been developed and employed for intelligence, warfare, and

even law enforcement purposes, with more nations engaging in this activity. Moreover, all cyber players struggle to find the right balance between cybersecurity requirements on the one hand and offensive applications on the other. In cyberspace, even more so than in other areas, important defensive missions often must be conducted in tandem with or as a follow-on to offensive operations.

- *Deliberative restraint.* Aggressive government action against foreign nations engaging in cyber espionage and warfare is fraught with risks and challenges. Thus, even the most sophisticated and powerful governments often back away from taking on some of the more aggressive forms of state-sponsored or -conducted cyber behavior. The difficulty in reaching an adequate and publicly usable level of certainty in attribution, concern about the legitimacy of the response against forms of behavior in which they also engage, anxiety about the utility of available options for response, and fear of (and vulnerability to) retaliation or other forms of blowback all seem to inhibit government responses to cyber attacks in general and those directed against the private sector in particular. Moreover, contentious domestic political implications often surround any potential assertive response to such attacks. These concerns also dampen government enthusiasm for owning the private sector's cybersecurity risks more broadly.
- *Shortcomings of international collaboration*. As cyberspace becomes more international and interdependent, international collaboration is indispensable when fighting cyber crime and aggression. But in cyberspace, far more than in the physical world, sovereignty is often blurred or contested. Formidable political and legal obstacles make it difficult to reach a consensus on what constitutes unacceptable behavior in cyberspace and which responses are legitimate to sovereignty infringement and other forms of offensive cyber conduct. Unilateral responses to unacceptable cyber behavior also face painful dilemmas, serious risks, and daunting trade-offs. The inconclusive debate over the private sector's active defenses in cyberspace illustrates the gravity of the challenge to forming the necessary level of international collaboration through interstate agreements.[10]
- *Private sector pushback*. Corporations resist intrusive government regulation and other forms of interventions in their internal affairs, including their cyber risk management practices. Some of the pushback comes from the private sector's traditional concerns about government regulation, such as implementation costs and burdens, exposure to liability associated with compliance, and the risks involved in reporting cybersecurity practices (and breaches) to governments and the public. A further source of pushback comes from corporate reluctance to meet the competing demands of different governments in whose territory they are operating, or even from competing regulatory demands made by the same government.

All of these considerations ultimately lead to the conclusion that governments cannot be realistically expected to own, let alone fix, the private sector's entire cyber threat problem. This situation calls for action in two complementary directions. One is to define space for a public-private partnership in managing cyber risks. The other is to reflect on the role of private sector entities and mechanisms in managing their own cyber risks. The focus here is primarily on the latter.

The Private Sector Predicament

To seriously weigh the potential role that the private sector entities and mechanisms can play in protecting their own cyber equities, it is necessary to understand the cyber-related challenges that the private sector faces in its daily operations:

- *The magnitude and complexity of cybersecurity risks*. Cyber risks cut across most business areas and activities and directly or indirectly affect virtually all performance and liabilities, and consequently present new liabilities and risks. Thus, effective cyber risk management presents conceptual, organizational, operational, technological, financial, and management challenges. Companies must assess and map their cyber risks, keep these assessments up to date, and figure out and execute comprehensive strategies to deal with them in house. Even if a company hires a cybersecurity vendor or works with a cybersecurity partner to solve these problems, it is no small challenge to determine which outside firms are best suited to address its cybersecurity requirements.
- *Cybersecurity investments draw on precious corporate resources.* Investments in cybersecurity come straight off the bottom line, and yet may still provide insufficient immunity against the gravest cyber risks. This problem is further compounded by the tension between investing in cybersecurity technology and operations, or in cyber resilience and risk-channeling measures. Because of the novelty of the entire field and the immaturity of those measures, most corporations have invested in cybersecurity technology and operations at the expense of developing a more comprehensive, long-term approach.
- *The limitations of passive defenses.* Passive defenses alone are insufficient to contend with increasingly sophisticated cyber attacks. Even when successful, their utility over time remains highly uncertain. And even when most successful, passive defenses fail to truly penalize cyber predators, and effectively encourage further attempts to breach corporate networks, products, and services.
- *Legal limitations and prohibitions on active cyber defenses.* In many jurisdictions, some of the more active cybersecurity measures remain ideologically and legally contentious or are outright prohibited in the private sector. Even where these measures may halt or impose

costs upon cyber attackers and help law enforcement agencies pursue them—thereby raising barriers for entry and diminishing criminal appetites for such activities—the private sector can only go so far in its efforts.[11] Moreover, most corporations are not presently able to offset the potential liabilities associated with deploying active defense measures.

- *Insufficient ability to channel cyber risk exposure to insurance carriers*. Even though the insurance industry traditionally plays a critical role in risk channeling, at present the private sector is not fully capable of taking advantage of cyber risk insurance. (This concern will be studied in greater depth in the coming sections.)
- *Hindrances caused by commercial competition and government regulations.* Regulations on cross-border data flows and antitrust measures are a particular concern for collaborative private sector efforts, especially in the context of an uneven international regulatory environment. Adding to these concerns are political and national security considerations and commercial competition. Moreover, there is natural anxiety over the potential risks created by sharing intimate data about security practices. These factors not only hinder but often outright prevent critical efforts to pool resources, share best practices, and otherwise deal collectively and comprehensively with evolving national and international cyber threats.
- *Brittle public tolerance for cybersecurity breaches*. Although the public reaction to reports of cybersecurity breaches remains inconsistent and uncertain, people are more aware of the risk and expect that corporations will do more to defend themselves against such risks and disclose any failures that occur. Market forces are already responding to such revelations, and corporations face potentially aggressive litigation if they fail to prepare for such scenarios.

The private sector predicament associated with cyber risks has generated two dramatic developments in risk management practices. One is to assign a greater share of business activity to the cloud, an approach that appears to channel much of the responsibility for protecting private companies' data to a handful of large, sophisticated cloud service providers. The other is to turn to the insurance industry to perform its traditional role in risk channeling. Because this paper will focus on cyber risk insurance, this discussion will be confined to just one general remark about cloud service providers.[12] The cloud is rapidly emerging as an important commercial service and cybersecurity solution, leveraging the sophistication and economies of scale of its service providers. Governments and some of the world's largest companies have now joined small and medium-sized enterprises in outsourcing the storage and processing of their data to cloud service providers. This trend has many benefits, but it also makes cloud service providers an increasingly lucrative target for hackers. For the time being, it is vital to remain vigilant about the effects that would ensue should cloud service providers suffer from major cyber incidents, which may rise to a systemic level considering the small number of major cloud service providers and the concentration of data and other equities in their systems. As a

result, even the viability of the cloud solution may hinge on comprehensive cyber risk insurance packages including expanded coverage beyond just business interruption. This kind of package, combining cloud services with insurance coverage, has already begun to emerge and may in the future become an integral component of the cloud services model.[13]

In short, there are few readily available fixes to the private sector's predicament, and none without pitfalls. Corporations need to redress the underlying sources of cyber risk, in particular the interaction of structural and behavioral factors that contribute to its dramatic expansion. The following section, therefore, is an effort to understand how insurance may contribute to cyber risk mitigation and management, to analyze why this potential has not yet been realized, and to explore what can be done to start unlocking this potential.

The Role of the Cyber Insurance Industry

As the reasonable and unsurprising calls for the insurance industry to be more closely involved in cyber risk management have grown, recent trends in this respect have been positive. The increasing rates for cyber insurance premiums, for instance, appear to indicate that more companies have been adopting cyber insurance products.[14] It is clear that cyber insurance can play an essential role in addressing the immediate situation that corporations face, but this hardly exhausts its potential to shape the broader cybersecurity equation. Insurance offers a uniquely promising contribution to resolving the private sector predicament. The industry's ability to motivate behavior can begin to reshape the commercial incentive structure, and systematic efforts to do so may help reverse some of the deeper technical trends that make risk management so difficult.

The unique capacities of the insurance industry; its demonstrated ability to engineer and address complex risks; and the novel, multi-dimensional, (primarily) privately owned, and transnational nature of cyberspace all suggest that insurance is especially well suited to perform a pivotal role in stabilizing the domain. Its role can be evaluated through six core functions of insurance:

1. *Engineering risk.* By accumulating data from experience and analysis of effective risk management practices, insurers can develop greater insight into the factors shaping the cyber risk environment.
2. *Channeling corporate risk.* Underwriters, as per usual insurance standards, would take on the core function of assuming corporate cyber risks.
3. *Managing systemic risks*. The process of identifying potential aggregation risks could not only avert exposure to catastrophic losses but also provide an invaluable service to governments

trying to anticipate and address possible systemic cyber attacks. The ability to identify and help prevent cascading effects or single points of failure may diminish the prospects for severe economic or national security impacts; in turn, this may reduce the potential for an international crisis or conflict stemming from a cyber attack.

4. *Harnessing collective insights to improve security.* The interrelated, interdependent nature of cyberspace is both a tremendous challenge and an opportunity. On the one hand, malicious capabilities rapidly diffuse and have ripple effects across the ecosystem. A new exploit or technique typically will spread quickly and be used by a vast range of actors, forcing defenses to constantly adapt to globally dispersed threats.[15] On the other hand, mechanisms to effectively leverage insights across the ecosystem can support common solutions. The insurance industry can be a central repository for granular data relevant to security across the private sector and can provide the analytical capabilities to extract deeper insights from this data beyond adapting defenses to immediate threats.
5. *Shaping broader trends in the risk landscape*. In an environment where commercial decisions significantly affect risk exposure, insurers supply financial incentives to change private sector behavior. These changes could have major long-term effects on the opportunities for and cost-benefit analysis of malicious activity. For instance, insurers could dissuade policyholders from behaviors that dramatically expand attack surfaces, such as the unnecessary use of remote-control capabilities for critical infrastructure components, or conversely encourage implementation of expedient cybersecurity practices (even when they carry residual contagion risk) by extending liability coverage to those that apply them.
6. *Internationally harmonizing standards and practices*. The lack of common standards or norms in such a transnational and interdependent domain exacerbates the cybersecurity challenge and creates a fragmented environment suitable to malicious activity. The difficulty of striking interstate agreements in this space impedes progress toward harmonizing national approaches and addressing the gaps between them. Unlike national regulation, the insurance industry's influence extends across state boundaries. Insurance can thus act as a global proxy regulator capable of promoting mutually beneficial practices and standards internationally, as it historically has done in other domains.

The insurance industry's primary role is to understand and manage risk. When it performs this role well it could have a profound systemic impact. Lloyds of London, for example, was formed to tackle maritime risk in the early decades of global seafaring and trade; by studying navigational routes, ship construction methodologies, and pirate attack patterns, the firm was able to partner with industry to make maritime risk manageable. In the early 1900s, insurers deployed similar methodologies to drastically reduce the incidence of boiler explosions and subsequent property damage and death. Today, product liability insurers help drive manufacturing and safety standards, environmental

insurers help foster brownfield redevelopment, and property insurers collaborate with policyholder clients to achieve a status often referred to as a "highly protected risk," which affords broader coverage at more economical premiums than would otherwise be achievable.

The insurance industry's potential, as evidenced by these ongoing success stories, is grounded in its near real-time vantage point of risk insight. Every day, countless companies have their risks underwritten and receive payments for claims; behind the scenes, the insurance industry churns and analyzes data to understand which risk management practices are working and which are not. For the segments of risk where this potential has been realized, top insurers are considered risk engineering advisers that happen to provide insurance, rather than the other way around.

Most, if not all, of the insurance industry's potential with respect to cyber hinges on data—cybersecurity program data, loss exposure data, threat data, and the like. The best analogy for what the insurance industry needs from a cyber standpoint can be found in the property world. Take, for instance, a single building: underwriters want to understand how the building was constructed; what materials were used; how the building is continually maintained, upgraded, and guarded; what types of tangible property and human capital it contains; and, ultimately, what it all costs—which is what the insurance policy will pay for if the building is damaged or destroyed. The process to obtain the requisite data can be a deep dive, but collecting it is the norm in the property insurance world. The net benefit of that ongoing data collection effort is the risk engineering advice that the insurance industry continually provides to its property holders.

What Prevents Cyber Risk Insurance from Realizing Its Full Potential?

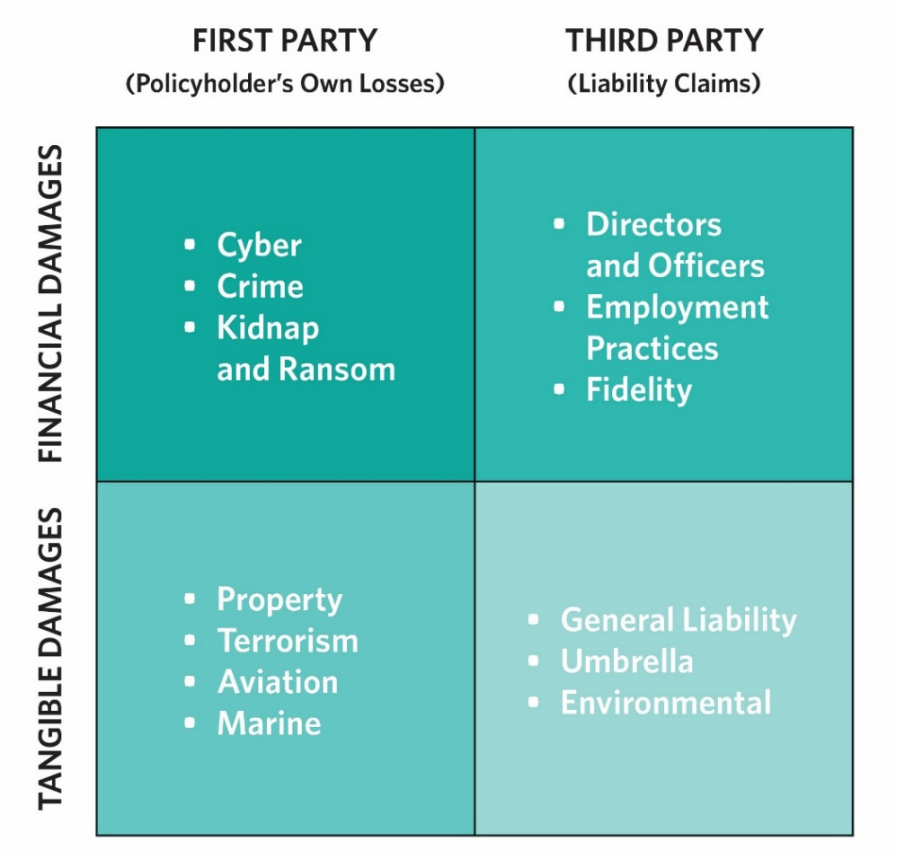
To understand why cyber risk insurance has fallen short of realizing its full potential, it is crucial to look at the current realities that characterize the insurance industry and the barriers these create to an ideal interaction between insurers and policyholders.

Product Evolutionary Realities

Years before the current privacy climate formed, the earliest cyber insurance policies were born in the property world. Cases such as *Ingram Micro v. American Home Assurance* led property insurers to refuse to provide coverage for intangible property such as "data," thereby creating a demand for policies that did cover such exposures.[16] But even though deep-dive risk engineering approaches are the norm for property insurance, most insurance companies built their cyber insurance operations

within financial/management insurance divisions, where clients prefer and brokers promote the ease of transaction and emphasis on efficiency. Instead of a collaboration in which insurers are expected and allowed to take a true deep dive into risk, they typically make underwriting determinations on only the minimal amount of information necessary to support coverage.

In the current and ever-evolving cyber risk climate, governments, corporations, and the insurance industry itself should all recognize that cyber threats present a peril that transcends most commercial insurance lines—meaning that cyber predicated losses are of the type relevant to many types of insurance coverages. As seen in the table, which categorizes types of insurance coverage according to whether they pertain to financial or tangible damage and whether they cover the policyholder's own losses or liability claims, there are at least nine types of insurance policies designed to cover the losses that a cyber peril can cause.



Although industry awareness of the nature of cyber threats and potential losses has been growing, the majority of insurers do not currently have the underwriting expertise or the data management systems to effectively treat cyber as a transcendent risk and gather the granular data needed to develop robust underwriting datasets. From an underwriting and data insight standpoint, much of

what is being observed or collected applies only to the specific exposures that are being underwritten. This challenge affects not only insurers but also reinsurers—the latter may be more detached from the underlying risks, but they are desperately seeking insights that could help them offer significant reinsurance capacity and further unlock the market.

Because cyber risks are transcendent risks, (presenting unprecedented potential for cross domain and cascading effects) there is no such thing as an "all-risk" cyber insurance policy that would cover the entire spectrum of potential loss. Such a policy, for example, might cover not only forensics expenses related to a breach of credit card information but also the associated insurance costs of a segment of natural gas pipeline that was exploded by a malicious command sent to the industrial control systems. To outsiders, this distinction might seem insignificant, but it exemplifies the challenge that insurers face in figuring out how cyber perils should be understood and underwritten—ultimately driven by the reality that in recent decades, the insurance industry has evolved by specializing into myriad risk segments.

Furthermore, the insurance industry has rarely, if ever, had to face a cyber-centric challenge before, at least as far as a risk that can change drastically in real time. Most risk classes remain relatively static, certainly in comparison to cyber risk. The constant evolution of technology and practices, the difficulties in anticipating vulnerabilities, and the ability of malicious actors to adjust their tactics and adapt to security measures all make cyber risk a constantly moving target for risk engineering.[17] As the aforementioned OECD study found, the unique characteristics of cyber risk call into question the ability to meet the general "principles of insurability"—in short, the need for risks to be random and independent in occurrence, quantifiable, and diversified across a community facing shared risks.[18] Further, two particularly disruptive trends mentioned previously—cloud services and the introduction of machine learning for both offensive and defensive measures—appear likely to make it even more difficult for insurers to get a handle on risk exposure. Consequently, the traditional method of basing coverage and rates on historically deep underwriting and loss data does not and will not hold for cyber risk. Insurers should understand that observing and sharing front-end best practices is the best way to start making cyber risk manageable.

Customer Behavior Realities

At the vast majority of enterprises, the chief information security officer (CISO) or chief security officer (CSO), or their functional equivalents, are responsible for cybersecurity programs. Even today, many CISOs/CSOs are skeptical of the insurance industry. They find it difficult to understand an entirely different discipline than their own technology-centric world, and sometimes

still believe that their company's decision to purchase an insurance policy is an indictment of their own efforts. Additionally, many CISOs/CSOs incorrectly believe that the cyber insurance underwriting process centers on collecting and pricing security vulnerabilities, which could invite attacks or liability suits or even provide insurers with grounds to deny coverage. The latter certainly is not true. Nor should the former be the case.

Typically, risk managers, or sometimes procurement departments—much different segments of the organization than the area controlled by the CISO/CSO—handle insurance purchasing. Beyond the practical reality that insurance policies do not translate well to security technology, both disciplines have different decision considerations, budgetary realities, and lines of authority. This reality makes risk management–security leader collaboration difficult to achieve.

Insurance Market Realities

Competition is a good thing, but on occasion it can have adverse consequences, and the cyber insurance marketplace is a good example. At least seventy-five and perhaps more than one hundred insurers offer some form of cyber insurance, meaning that competition is strong and intense. Over the past few years, this competitive dynamic has resulted in many insurers believing that the best way to win and maintain business is to make the underwriting process as easy as possible—or in certain cases, nonexistent—hoping over the long term that all that will be needed is to build up a sufficient premium bank (also known as "cash flow underwriting"). This dynamic is exacerbated by the various insurance brokerage firms that are keen to transact as much business as possible to drive revenue, and thus are complacent participants.

From a talent standpoint, insurance professionals in the property world often have legitimate engineering credentials and experience, whereas many cyber underwriters are barely into their professional careers. Security credentials would be preferred, but the universal competition for security talent means that most potential cybersecurity professionals seldom consider the insurance industry as a career path. It would not be uncommon for a seasoned CISO/CSO to face questions from a novice underwriter with little to no information security experience during a cyber underwriting interview.

Risk Aggregation

These factors, combined with the previously mentioned challenges, drive another critical reality: insurers and reinsurers are struggling to comprehend cyber-related aggregation risk arising from the interconnection of platforms and shared service providers, including in the cloud.[19]

As discussed above, a number of accelerating trends contribute to the increasing potential for systemic and cascading impacts from cyber incidents. This makes it difficult for insurers to assess how cyber risks across different policyholders may correlate—creating the potential for aggregation risk. For example, if a broad swath of manufacturing firms relies upon a single "industrial Internet of Things" platform for their operations, a cyber attack compromising that platform could disrupt manufacturing across an entire industry. An insurer underwriting multiple such firms would face potentially massive losses from just one cyber incident. The problem gets even worse when considering how malicious actors might leverage different kinds of systemic impacts in combination.

Anticipating where and how such aggregation risks might emerge can be extremely difficult in part because they can arise from a range of sources: Reliance upon a single platform or service, common hardware or software products, common nodes in globalized supply chains, and interconnections throughout the ecosystem that allow cyber attacks to propagate, among others. This unpredictability compounds the already arduous task facing insurers attempting to assess any single policyholder's exposure.

This concern over aggregation risk has in itself been a major driver behind the hesitancy of reinsurers to provide substantial reinsurance capacity for cyber—a hesitancy that inhibits the overall insurance market because primary insurers will constrain what they can offer without reinsurance support.[20]

This is a problem that can be solved by data and risk insight—the common thread running through all of the aforementioned challenges. The cloud underwriting predicament explains the challenge well. Insurers and the reinsurers behind them must be able to underwrite a cloud provider itself and all of the customers of that cloud service, including the underlying risk of those customers' reliance upon that cloud service provider, in order to put together an accurate picture of the overall risk. The insurance industry is arguably undertaking such an endeavor on a daily basis, but these challenges create a reality whereby coordination of all underwriting and data insight is impossible. Despite the fact that cloud providers' own survival is contingent on top-notch security, which should make it a better risk class, the potential systemic and aggregation risk associated with cloud services continues to be a daunting challenge for the insurance industry.

How Can the Cyber Risk Insurance Industry Unlock Its True Potential?

What would it look like for the insurance industry to operate at full potential regarding cyber risks? It may be easiest to answer that question by explaining an ideal ongoing insurance coverage relationship, whereby a policyholder maintains coverage with an insurer or syndicate of insurers over time. In that context, any time coverage is underwritten (whether initially or for a renewal), the policyholder's risk management practices would be evaluated against the insurer's own underwriting model. This model would be updated in real time based on the insurer's observations both in continuously underwriting a portfolio of similar risks and conducting postoperative analyses when claims are paid. The ideal underwriting model, therefore, is a dynamic database of risk management best practices and failure points.

In this ideal state, the underwriting process is not unilateral; rather, it is a dialogue between the policyholder and insurer along two specific lines: (1) "Here's what we've observed about your risk management practices and how they rate relative to your peers"; and (2) "Here's the current set of best practices from that peer group—you should consider doing these things because the evidence suggests that such approaches are beneficial, and avoid or stop doing these other things because they have resulted in losses and paid claims." However, this ideal state also goes further. It involves financial and coverage incentives that vary based on industry insights. Certain best practices might come with premium reductions if they are adopted, or additional premium charges if they are not adopted. If a policyholder is advised to avoid or abandon certain risk management practices or technologies, insurers could then stipulate increased premium charges or policy exclusions to negate coverage if a loss or claim results from those practices or technologies that the policyholder was asked to avoid. By the time the next policy renewal comes around—typical commercial insurance policies are purchased every year—the process will repeat, with up-to-date information and a refreshed set of suggestions. This approach may combine well with the pre- and post-event services offered by various insurers.

Property, maritime, and some other classes of risk largely operate in this fashion, where information exchange is the most valuable component of the transaction. Admittedly, most if not all classes of risk where this potential has been achieved have a much less dynamic risk environment than cyber. Perhaps the ideal state for cyber insurance involves a frequent cadence of revisions, where interim underwriting check-ins happen every three months with a deeper dive annually. The key question, then, is how to unlock this potential for cyber and achieve a symbiotic relationship between insurers and policyholders? To address this question, the following points suggest a few practical solutions, mostly centered on trust and transparency, to drive more substantial information and data sharing.

- *Cyber talent procurement and cross-training.* Given the intense competition for cybersecurity talent, it is unsurprising that the insurance industry lags other industries with respect to attracting and retaining skilled cybersecurity expertise. Unfortunately, this can cause an imbalance in expertise, whereby newly minted generalist underwriters are expected to facilitate an underwriting dialogue with seasoned cybersecurity professionals. Brokers and insurers should loosen the purse strings when it comes to compensation and incentives for appropriate cybersecurity expertise. This becomes especially important as advances in cyber threats, including autonomous attack and defensive capabilities, make it far more challenging to understand the risk from an underwriting standpoint. Given the cross-product nature of cyber risk, moreover, both brokers and insurers should invest in cyber risk awareness training for all product disciplines.
- *Specialization of insurance underwriting and deeper collaboration with cyber security service providers.* Partnerships with cybersecurity researchers and managed security service providers can fill some of the gaps in the insurance industry's expertise and capacities. These can integrate specific services such as security audits, vulnerability assessments, and penetration testing into the underwriting process. Third-party expert assessments of a policyholder's assets would give insurers greater insight and understanding of risk exposure. More important, these practices would directly raise the baseline level of security by identifying flaws and motivating efforts to mitigate them by making coverage conditional upon their being addressed.
- *Claims transparency.* Insurers should strive to be as transparent as possible with respect to cyber claims received, cyber claims paid, and the reasons for claim denials, without compromising client-specific or confidential information. This suggestion speaks to product efficacy and intends not only to separate those insurers that are truly attempting to understand the risk and develop responsible coverage from those that simply are trying to book premium as easily as possible, but also to build confidence among the many security professionals who are skeptical of insurance products and the insurance industry.
- *Contract simplicity and understanding.* Insurers should strive to develop the simplest and most easily understood insurance contracts. Ideally, insurers will appropriately define a cyber event and specify the types of losses that the policy will cover, with only the most necessary exclusions. Further, given the abundance of misperceptions about the types of losses that cyber insurance policies cover, insurers should offer a coverage key similar to the four-quadrant taxonomy depicted earlier in this paper. This simple tool can provide a means for companies to easily understand the impact of a cyber event and how their cyber insurance policy or policies relate to the categories of impact. One of the biggest benefits of these clarified policies is that security leaders will be able to better grasp and feel confident in how

the policies work. Similar to claims transparency, stronger buy-in from security leaders is critical to unlock the potential of the insurance industry.

- *Use of maturity-based underwriting methodologies*. Increasingly popular cyber risk management maturity models, such as the Cybersecurity Capability Maturity Model (C2M2) and the U.S. National Institute of Standards and Technology's Cyber Security Framework (NIST-CSF), can serve as core underwriting methodologies.[21] These methodologies take a different approach to cybersecurity than most of the traditional compliance/control frameworks, which, given their static nature, are really only a security baseline. Maturity models, by contrast, are designed to measure and support an organization's overall cyber risk management health and its interest in continual improvement—an approach that is much better suited to the dynamic nature of cyber risk.

Complementary Efforts by Governments and the Insurance Industry

The practical solutions offered above can begin to move the cyber insurance industry toward its ideal state. Yet sustained, coordinated action by both industry and governments, individually and together, is needed to help the insurance industry realize its full potential to shape the broader trajectory of the cyber risk landscape along the lines of the six core functions of insurance.

Given its significant role in the cyber domain, the private sector should be the focal point for efforts to reshape this risk landscape. Complementary efforts by governments and industry should therefore focus on reorienting the incentive structure shaping corporate behavior. This entails a holistic approach addressing both the factors shaping risk management practices and those shaping underlying risk exposure in the first place—decisions made across the full spectrum of business operations. In other words, the focus should not just be on ad hoc cybersecurity solutions but on ways to comprehensively address the factors that increase or mitigate cyber risk exposure, from the supply chain to the end of the product life cycle. The following section describes what such an approach might look like, including individual and collective actions in the context of a broad agenda for government, insurance industry, and broader private sector efforts.

Diminish the Appeal of Cyber Risk Exposure

Part of the problem is a lack of comprehension of how cyber risks cut across all aspects of business operations. Cyber risks are difficult to scrutinize, and the expertise and analytical potential of

insurance is needed to improve their clarity. Doing so would enable existing market forces to drive risk management to more effectively shape cybersecurity practices.

As the insurance industry matures in its role and ability to engineer cyber risk, it can discern from the data those practices that increase exposure or create aggregation risks. Insurers can directly disincentivize such practices, or incentivize mitigation measures, through the cost of premiums and policy exclusions. But a more robust assessment of cyber risk should also inform clients, consumers, shareholders, and potential investors in order to create additional market incentives. Informed by insurers, influential stakeholders (including major holding corporations and credit-rating agencies) could be nudged to factor cyber risk management more thoroughly into their assessments and determinations.

Clearly, governments can, by themselves, make progress toward this objective. They have a range of tools at their disposal to directly regulate or indirectly prompt cybersecurity and risk management practices in the private sector that would, in turn, empower insurers. For example, they could determine and clarify through regulation and legislation which active cyber defense practices (such as "hack backs") would be considered legitimate and which would be deemed unacceptable or even unlawful.[22] Most obviously, this includes mandated cybersecurity practices for governmental services, critical infrastructure, and other areas. Further efforts to develop and promulgate voluntary standards, benchmarks, and metrics for cyber risk management have already proven beneficial to the private sector.[23] Governments can also leverage their sheer weight in different sectors to generate market forces through their own acquisition processes and contractual relationships. These could include, for example, standards for cybersecurity practices, personnel training or certification, or cyber insurance coverage for procurement contracts.[24] The European Union Council is already developing a common framework for the certification of ICT products and services throughout the EU.[25] Such standards can, in turn, spread throughout the market to drive broader shifts in behavior. Likewise, the blacklisting by governments of products deemed compromised can have a powerful effect, dissuading others from buying them.

Of course, many such activities are already being undertaken by governments, though often in an ad hoc manner. Cooperation between governments and the insurance industry can more deliberately and effectively shape broader market incentives, such as through enhanced Securities and Exchange Commission (SEC) requirements for disclosure of material cyber risks to publicly traded corporations. This could improve transparency regarding cyber risk exposure and allow stakeholders to better differentiate among corporations based on their risk management practices. At a minimum, it would place pressure on companies to thoroughly assess cyber risk and pay attention to it at the highest levels of corporate leadership. Disclosures could include whether or not corporations have

cyber insurance coverage that adequately accounts for potential impacts across multiple areas of business, and could nudge them toward standalone coverage when appropriate. In turn, corporations may find it more palatable to signal effective cyber risk management by disclosing their insurance coverage than by disclosing sensitive information related to risk factors.

Collectively, these market pressures could help counterbalance the incentives that drive risk exposure. They could rectify the inattention to cyber risk, which itself happens in part because major cyber incidents to date appear to have had only modest, temporary impacts on businesses. Those responsible are rarely held accountable, and the damage to stock value is often fleeting.[26] Simply shedding light on the full extent and potential consequences of exposure to cyber risk would empower those with financial leverage to supply the motivation for risk management.

Even further, cyber insurance could play a role in making other mechanisms for motivating cybersecurity practices viable. This includes the potential for entities in roles that can critically impact wider risk exposure to face civil liability for failure to exercise reasonable diligence. Companies providing crucial ICT/ICS products and services or occupying central positions in the ecosystem, such as internet service providers, could bear some degree of liability if their products and services are egregiously insecure. The insurance industry can address legitimate concerns that liability would potentially stifle innovation. Insurers could partner with cybersecurity providers to help identify best practices in product and service development (for example, penetration testing and threat modeling) and cover liability if companies agree to follow these best practices.

Finally, collaboration will be essential to address potential systemic cyber risks. Insurers can help locate potential single points of failure and motivate steps to eliminate them and minimize the prospects for cascading effects from cyber incidents. For instance, the incorporation of diversity and redundancy into the design of products and services can improve the resilience of systems against widespread attacks.[27] Dynamic and adaptable defenses can likewise reduce the potential for systemic incidents. This is particularly relevant for cloud service providers, who are in a position both to harness the most powerful defensive measures—particularly through improvements in machine learning capabilities—and to undertake defense on behalf of less capable actors. Given their increasing criticality, including for many government functions, cloud services may eventually be deemed of systemic importance. Insurers can further identify when and where systemic risks might merit direct government intervention and determine other areas where governance mechanisms such as civil liability could be sufficient.

Increase the Viability of Cyber Risk Management

Improved assessment of and familiarity with cyber risk exposure, particularly among stakeholders that have direct financial levers to shape corporate behavior, should help differentiate corporations that have effective risk management from those that are overly complacent. Yet for market pressures to work, the visibility of corporations' exposure and risk management must correspond to practices that actually succeed in mitigating risk without exposing corporations to additional risks. Beyond simply identifying effective risk management practices, insurers can work with governments and cybersecurity providers to develop and promote cybersecurity innovations.

Governments and the insurance industry can foster efforts within the private sector and through public-private partnerships to build cybersecurity capacity, improve information sharing on threats and best practices, explore innovative technologies and approaches for more effective cyber defense, and develop common standards and metrics for cybersecurity. Government action to remove remaining barriers to collaboration (such as concerns regarding antitrust infringements) could generate momentum behind such efforts. More ambitious efforts might include national or international industry initiatives, which could help clarify baseline expectations for cybersecurity and create further incentives, such as reputational benefits. Insurers could provide critical support for these efforts by motivating policyholders to contract for cybersecurity services that meet formal or informal standards of professional practice, such as certification of operators and capabilities or membership in a corporate social responsibility initiative. The development of common standards and metrics would, in turn, provide the insurance industry with more effective benchmarks for cybersecurity practices. The cumulative impact would be to promote the professionalization of cybersecurity services—establishing indicators and baselines to help assess providers, reducing the likelihood that basic cybersecurity box-checking alone would create a false sense of security.

Most importantly, for corporations to be able to effectively channel cyber risk to insurers, cyber risk itself has to be profitable for the insurance industry. This necessitates some degree of insulation from potentially catastrophic losses from cyber incidents. Here, governments can provide a backstop for insurers, as has been done for similarly intractable risks like terrorism. For instance, in the United States, the Terrorism Risk Insurance Act of 2002 (TRIA) provides compensation to insurers for losses from acts of terrorism that reach a certain threshold. Although TRIA was extended to cover losses from cyber terrorism for standalone cyber insurance policies, significant ambiguity remains as to the thresholds that trigger coverage.[28] Specific proposals have been made elsewhere for how to extend this backstop in the United States, and there are growing calls for similar programs in other countries.[29]

TRIA-like backstops could encourage innovation in coverage and increase insurers' willingness to expand coverage boundaries. Such backstops would need preconditions, such as requirements that participating insurers provide appropriate underwriting acumen. This condition could be fulfilled by using the aforementioned risk management maturity models, C2M2 and NIST-CSF, as core underwriting methodologies. Such programs would be designed to sunset after a specified time, or after insurers have built up reserve capital to sustain the offerings on their own.

Ensure the Integrity of the ICT/ICS Supply Chain

This paper has focused largely on how governments and insurance can shape the incentive structure for corporations to manage cyber risk. But such efforts can only go so far without addressing the essential role of intrinsic norms and standards for those companies occupying critical nodes of the ICT and ICS supply chains. Given the widespread reliance upon their products and services, a failure on the part of these companies to exercise due diligence in their development and management has significant potential to generate systemic cyber risks. These, in turn, contribute to potential aggregation risks that become an inescapable concern for insurers and, equally, reinsurers, placing a ceiling on their appetite for cyber risk. Thus, the very stability of the ecosystem to some extent hinges upon trust in these vendors and their products. ICT and ICS vendors must therefore bear some responsibility for ensuring the integrity of their products throughout their life cycles, commensurate with their role in shaping the broader risk landscape.

This obligation calls for commitments by vendors to undertake certain obligations regarding their products as well as specific measures and metrics to enhance broader confidence in such commitments. For instance, vendors can implement measures to verify chains of custody and ensure the traceability of components and products throughout the supply chain that allow discovered vulnerabilities to be tracked back to their point of origin.[30] Fully elaborating what such commitments would entail, how they could be verified, and how governments could complement and incentivize them are the subjects of an effort parallel to this study.[31] The point here is to emphasize the importance of these companies' stewardship of their products in the context of complementary efforts by governments and the insurance industry. Verifiable commitments and metrics to ensure the integrity of ICT/ICS products would thus go a long way to assuage concerns of insurers regarding their ability to adequately assess cyber risk exposure and anticipate aggregation risks. Further, deep collaboration between these vendors and insurers toward implementing such measures can give the latter concrete metrics for gauging risk exposure and mitigation. Nowhere is this more essential than with respect to cloud services, given the market concentration and dependence upon such services.

Conclusion: Toward a Partnership Among Governments, Insurance Industry, and Corporations

Cyber risk presents a multifaceted challenge demanding action by governments, corporations, and the insurance industry alike. Sporadic and ad hoc attempts to address the problem thus far have failed to keep pace with its growing scope and severity. Meanwhile, the predicament of the private sector appears likely to continue to deepen. This paper has explored the unique contribution that cyber insurance, alongside and synergistic with other mechanisms, can make to a broader, strategic approach to this problem. In its ideal state, the insurance industry can begin to reverse the underlying trends driving the cyber risk challenge.

At the root of this deteriorating landscape is a perverse incentive structure for many industries that fuels risk exposure. Companies' product and service development decisions can both positively and negatively shape the risk environment, not just for themselves but for others. Poorly designed or insecure features and connections, for instance, may expand the cyber attack surface in unpredictable ways. For example, if numerous utility companies were to collectively rely upon a single cloud-based platform for critical infrastructure operations, they may unwittingly create a single point of failure with potential broader consequences for public safety and national security. Yet decisions that are instrumental in shaping the risk environment often are driven by commercial imperatives that militate against a more cautious approach to features and innovations that may increase risk exposure.

The continuous expansion of the cyber attack surface and the high payoff of attacks contribute to the favorable calculus for malicious actors—including criminals, terrorists, and nation-state hackers—which also has broader implications for stability. Returning to the above example, if those utility companies have industrial control systems exposed through links to their business networks, the perceived threat from a foreign state's cyber espionage targeting those networks would be dramatically higher. Preventing such exposure and enhancing resilience would both reduce risk and limit the potential for an international crisis to which governments would have to react.

For these reasons, unlocking the full potential of the insurance industry is increasingly imperative not only for the private sector but also for governments struggling to assess when and where corporate cyber risks rise to the level of national concerns. At the same time, cyber risk needs to be a profitable endeavor for insurers, and this demands government action to both empower insurers and place an upper ceiling on the potential consequences of cyber risk. This mutual dependency necessitates a long-term, strategic approach toward progressively expanding the role of insurance.

Governments, corporations, and the insurance industry can begin to tackle individual slices of this broader agenda separately. The insurance industry can evolve to implement the practical steps discussed above, improve the dialogue between insurers, and policyholders and increase the comprehensiveness, depth, and transparency of the underwriting process. Governments, by themselves and in collaboration with others, can gradually to raise baseline cybersecurity expectations and requirements. For instance, they can set requirements in their own procurement and certification processes that would inspire broader, structural shifts in the market.

Other efforts require a degree of reciprocity among governments, insurers, and key industry stakeholders. Otherwise, disjointed attempts to nudge the private sector in one direction or the other could prove counterproductive. For instance, enhancing cyber risk disclosure requirements without a means to signal effective cyber risk management might inadvertently punish corporations for accurately conveying the extent of their risk exposure. Similarly, commitments by corporations to ensure the integrity of products and services should be met with governmental efforts to complement and reinforce these.

Finally, some of the most ambitious efforts require sustained collaboration and a careful balancing of public and private interests. This includes creating government backstops for catastrophic cyber risk, which should only be done in close partnership with industry to properly scope and condition such coverage. Likewise, options for liability for failure to exercise due diligence in the development or provision of products and services necessitate careful consideration by governments and industry stakeholders. The capacity and willingness of insurers to underwrite such risks and minimize the potential impacts of liability on innovation are essential to assess before such steps should be taken.

This policy agenda, therefore, calls for a sustained partnership among these stakeholders and platforms to harmonize their approaches. Disinterested parties such as those in the nonprofit sector can provide neutral platforms to resolve the potentially diverging interests of stakeholders and communities. This is particularly necessary for cases like cyber risk where business interests and broader law enforcement, economic, and national security imperatives may clash—and even more so when the key stakeholders are globally dispersed.

The Carnegie Endowment for International Peace has undertaken this facilitating role in several such cases. It has convened government and industry players to cooperate on similarly complex, multifaceted risks in the nuclear domain. It also is increasingly active in bridging gaps between governments and industry within areas of cyber policy, including issues such as government interventions in ICT supply chains, managing systemic risks in the financial sector, and private

sector active cyber defense. Naturally, other nongovernmental organizations can also perform such a role.

Ultimately, this partnership is needed to address the fundamental sources of cyber insecurity. Governments and the insurance industry could do more than simply prompt changes in risk management practices. They could engender a deeper shift in decisionmaking toward a more proactive, risk-centric framework. This shift, in turn, could avert risk aggregation, erode the advantages of attackers in cyberspace, and help alleviate the pressure upon governments to respond to escalating cyber attacks. As long as governments and private sector defenders fall short in addressing these underlying sources of cyber insecurity, they will be forced to contain and respond to the negative consequences of malicious activity.

Ariel (Eli) Levite is a senior fellow in the Cyber Policy Initiative and the Nuclear Policy Program at the Carnegie Endowment for International Peace.

Wyatt Hoffman is a senior research analyst with the Cyber Policy Initiative and the Nuclear Policy Program at the Carnegie Endowment for International Peace.

Scott Kannry is CEO of Axio, a cybersecurity optimization firm.

The authors would like to thank Edmund Douglas for his valuable insights and feedback during the writing of this paper.

Notes

[1] In one indication of this trend, global Internet traffic is projected to grow threefold over the next five years. See "The Zettabyte Era: Trends and Analysis," Cisco, June 7, 2017, www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index vni/vni-hyperconnectivity-wp.html.

[2] According to a March 2016 report by McKinsey Global Institute, data flows accounted for $2.8 trillion of global gross domestic product (GDP) in 2014; in particular, "cross-border data flows now generate more economic value than traditional flows of traded goods." See, James Manyika et al., *Digital Globalization: The New Era of Global Flows* (McKinsey Global Institute, March 2016), 2, www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx. A similar study by the International Chamber of Commerce (ICC) found that in many countries the internet and data flows account for around 15 to 20 percent of GDP growth. ICC Commission on Trade and Investment Policy and ICC Commission on the Digital Economy, *Trade in the Digital Economy: A Primer on Global Data Flows for Policymakers* (Paris: ICC, 2016), https://cdn.iccwbo.org/content/uploads/sites/3/2016/09/Trade-in-the-digital-economy-A-primer-on-global-data-flows-for-policymakers.pdf.

[3] Laura Noonan, "Goldman Sachs Enlists Staff for Cyber Security War Games," *Financial Times*, June 6, 2018, www.ft.com/content/e7084d62-6994-11e8-8cf3-0c230fa67aec.

[4] See OECD, *Enhancing the Role of Insurance in Cyber Risk Management* (Paris: OECD Publishing, 2017), http://www.oecd.org/publications/enhancing-the-role-of-insurance-in-cyber-risk-management-9789264282148-en.htm; and Michael Siegel, Nadya Bartol, Juan Jose Carrascosa Pulido, Stuart Madnick, Michael Coden, Mohammad Jalali, and Michael Bernaski, *Cyber Insurance as a Risk Mitigation Strategy* (The Geneva Association, 2018), https://www.genevaassociation.org/research-topics/cyber-and-innovation/cyber-insurance-risk-mitigation-strategy.

[5] "U.S. Cyber Market Grew 32% in 2017 But Most Small-Medium Firms Opted Out," *Insurance Journal*, May 21, 2018, www.insurancejournal.com/news/national/2018/05/21/489930.htm.

[6] Angus Whitley and Michael Sasso, "Delta's U.S. Grounding Lifted after Latest Computer Glitch," *Bloomberg*, January 29, 2017, www.bloomberg.com/news/articles/2017-01-30/faa-says-delta-halted-domestic-flights-after-automation-failure.

[7] Global Agenda Council on Risk and Resilience, "Understanding Systemic Cyber Risk," World Economic Forum, October 2016, http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf

[8] See Ellen Nakashima, "Russian Military Was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes," *Washington Post*, January 12, 2018, www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

[9] See, for instance, the initiative of the National Institute of Standards and Technology on Cyber Supply Chain Risk Management at https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management.

[10] See, for instance, "The Digital Vigilantes Who Hack Back," *New Yorker*, May 7, 2018, www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back.

[11] See Wyatt Hoffman and Ariel E. Levite, *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?* (Washington, DC: Carnegie Endowment for International Peace, 2017).

[12] We thank our colleague, Tim Maurer, for his input on this section.

[13] See, for instance, Kirk Koenigsbauer, "Office 365 news at WPC 2016," Microsoft, July 12, 2016. https://www.microsoft.com/en-us/microsoft-365/blog/2016/07/12/office-news-at-wpc-2016/

[14] A recent brief by the Geneva Association estimates that the overall size of the cyber insurance market in 2016 in terms of gross written premiums amounted to US$2.5–$3.5 billion, and notes that industry participants reckon that the market may grow to $10 billion by 2020 and to $20 billion by 2025. See Daniel Hofmann, "Contours of an Emerging Market for Cyber Risk Transfer," The Geneva Association, April 10, 2018, www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/research_brief_-_contours_of_an_emerging_market_for_cyber_risk_transfer.pdf.

[15] See Ben Buchanan, "The Life Cycles of Cyber Threats," *Survival* 58, no. 1 (2016): 39–58.

[16] "American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc. (April 19, 2000)," Internet Library of Law and Court Decisions, n.d., http://www.internetlibrary.com/cases/lib_case155.cfm.

[17] One example of how attackers adapt to surmount defenses is the evolution in ransomware tactics to target backup processes and tools. See Rod Mathews, "Ransomware Will Target Backups: 4 Ways to Protect Your Data," *Dark Reading*, October 4, 2017, www.darkreading.com/endpoint/ransomware-will-target-backups-4-ways-to-protect-your-data/a/d-id/1330029.

[18] OECD, *Enhancing the Role of Insurance in Cyber Risk Management* (Paris: OECD Publishing, 2017), http://www.oecd.org/publications/enhancing-the-role-of-insurance-in-cyber-risk-management-9789264282148-en.htm.

[19] For further discussion of aggregation risk, including with respect to cloud services in particular, see OECD, *Enhancing the Role of Insurance in Cyber Risk Management* (Paris: OECD Publishing, 2017), http://www.oecd.org/publications/enhancing-the-role-of-

insurance-in-cyber-risk-management-9789264282148-en.htm; and Michael Siegel, Nadya Bartol, Juan Jose Carrascosa Pulido, Stuart Madnick, Michael Coden, Mohammad Jalali, and Michael Bernaski, *Cyber Insurance as a Risk Mitigation Strategy* (The Geneva Association, 2018), https://www.genevaassociation.org/research-topics/cyber-and-innovation/cyber-insurance-risk-mitigation-strategy.

[20] OECD, *Enhancing the Role of Insurance in Cyber Risk Management* (Paris: OECD Publishing, 2017), http://www.oecd.org/publications/enhancing-the-role-of-insurance-in-cyber-risk-management-9789264282148-en.htm.

[21] U.S. Department of Energy, *Cybersecurity Capability Maturity Model (C2M2): Version 1.1* (2014), www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf; and National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1* (2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[22] https://carnegieendowment.org/2017/06/14/private-sector-cyber-defense-can-active-measures-help-stabilize-cyberspace-pub-71236

[23] The National Institute of Standards and Technology's Cybersecurity Framework is a particularly relevant example, see https://www.nist.gov/cyberframework.

[24] For an in-depth proposal of how cyber risk management could be incorporated in the Department of Defenses' acquisition processes and contractual relationships, see, Chris Nissen, John Gronager, Robert Metzger, and Harvey Rishikof, *Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War*. The MIRTRE Corporation, August 2018. https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-8AUG2018.pdf.

[25] "EU to create a common cybersecurity certification framework and beef up its agency – Council agrees its position." *Press Release*, European Council, June 8, 2018. https://www.consilium.europa.eu/en/press/press-releases/2018/06/08/eu-to-create-a-common-cybersecurity-certification-framework-and-beef-up-its-agency-council-agrees-its-position/.

[26] On the limited impacts of cyber incidents on stock prices, see Russell Lange and Eric W. Burger (2017). "Long-Term Market Implications of Data Breaches, Not," *Journal of Information Privacy and Security* 13, no. 4 (2017): 186–206.

[27] See, for instance, Deborah Bodeau and Richard Graubart, *Cyber Resiliency Design Principles: Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines.* The MITRE Corporation, January 2017. https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf.

[28] Kevin P. Kalinich, "US Treasury Makes Standalone Cyber Insurance Policies More Valuable," Aon, 2017, www.aon.com/attachments/risk-services/cyber/TRIA-2017Update.pdf.

[29] For a U.S.-based perspective, see Robert Knake, "Creating a Federally Sponsored Cyber Insurance Program," Council on Foreign Relations, November 2016, https://cfrd8-files.cfr.org/sites/default/files/pdf/2016/11/CyberBrief_Knake_Cyber-Insurance_OR.pdf. For an international perspective, see Oliver Ralph and Ralph Atkins, "Swiss Re Chief Urges Governments to Back Cyber Insurers," *Financial Times*, December 28, 2017, www.ft.com/content/0212ad0e-e72d-11e7-8b99-0191e45377ec.

[30] See, for instance, SAFECode's "Software Integrity Controls" https://www.safecode.org/publication/SAFECode_Software_Integrity_Controls0610.pdf

[31] See Ariel E. Levite, "Rebuilding Trust in the ICT/ICS Supply Chain: Government Restraint and Corporate Active Trust Building," Carnegie Endowment for International Peace, (forthcoming).

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: +1 202 483 7600

CarnegieEndowment.org