Penn State Law Review

Volume 122 | Issue 3 Article 5

7-1-2018

Cyber Risks, Systemic Risks, and Cyber Insurance

James E. Scheuermann

Cyber Risks, Systemic Risks, and Cyber Insurance

James E. Scheuermann*

ABSTRACT

The literature on cyber insurance is replete with statements to the effect that "cyber risks are systemic risks." Through an analysis of the concept of systemic risk and the categorization of 19 principal types of cyber risk, this article discusses the extent to which this view is true and the practical implications, for risk managers and cyber insurance underwriters, of the conclusion that only some cyber risks are systemic.

In the cyber context, systemic risk may be most usefully characterized as the risk that arises out of a digital network (1) that consists of standardized or functionally homogeneous, interconnected, and interdependent nodes; (2) that permits cascading adverse events throughout the nodes; and (3) in which such adverse events occur at such a high rate of speed that they cannot be contained at all or not in a timely fashion. I distinguish four types of systemic risk that satisfy this definition, depending on whether the node that is attacked in a cyber incident is "critical" or "non-critical" and whether it is internal or external to an enterprise.

This article reveals that (1) some cyber risks are always or virtually always systemic, some are never systemic, and some may or may not be systemic depending on particular factual circumstances; (2) the cyber risks that are systemic represent additional risks for firms relative to a non-digitally networked world; (3) that for policyholders in particular,

* James E. Scheuermann is a partner in the Pittsburgh office of K&L Gates LLP, where he represents policyholders in insurance coverage matters. He received his J.D. from the University of Pittsburgh School of Law (1989) and his Ph.D. (philosophy) from the University of Chicago (1982). This article reflects the author's views on insurance issues, but does not necessarily reflect his views on the resolution of those issues. Moreover, this article does not necessarily reflect the views of any client of K&L Gates LLP or the firm itself. Mr. Scheuermann acknowledges the thoughtful comments and research assistance of Laura K. Veith, and the helpful comments of Carolyn M. Branthoover, John R. Hardin, and Jeffrey J. Meagher, all attorneys at K&L Gates.

the inquiry into whether a particular cyber risk is systemic practically translates to the questions of whether that risk can be identified, whether it is susceptible to management at all and, if so, in what fashion (through cyber insurance, technical means, or some other means); and (4) it is not possible to state as a general rule that cyber-systemic risks are either more or less manageable than those cyber risks that are not systemic. Broad pronouncements that "all cyber risks are systemic" do not advance sound cyber risk underwriting or cyber risk management. An understanding of the types of cyber risks faced by a firm and attention to particular factual circumstances are needed to effectively underwrite and manage cyber risks, whether they are systemic or not.

Table of Contents

I. INTRODUCTION

Are cyber risks systemic risks? This question is commonly answered affirmatively in the literature on cyber insurance. Lloyd's of London ("Lloyd's"), for example, states that a principal characteristic of cyber risk "is systemic exposure" because "[d]igital networks and shared technologies form connections that can be exploited by attackers to generate widespread impacts."[1] In analyzing the risk associated with a cyber attack on a major cloud service provider, Lloyd's and AIR

1. LLOYD'S, BUSINESS BLACKOUT: THE INSURANCE IMPLICATIONS OF A CYBER ATTACK ON THE U.S. POWER GRID 3 (2015), https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-lloyds-business-blackout-scenario.pdf.

Worldwide write that the "reliance on a relatively small number of [cloud service] companies has resulted in systemic risk for businesses using their services."[2] When the term "systemic" is not expressly used, close synonyms are often used to characterize cyber risk. In the insurance trade press, one insurer's cyber leader stated that cyber risk "stems from how everything is connected across the internet, which places everything at risk."[3] Similarly, we are told by two scholars of cyber insurance markets that "[d]ue to [the] significant homogeneity and presence of dependencies in computer systems[,] their failure is highly correlated. [The] [r]ecent spate of Internet worms like *MS-Blaster* and *Sasser* have [sic] highlighted this very threat."[4]

The purpose of this article is (1) to analyze whether all, some, or no cyber risks are systemic, (2) for those that are, to explore the extent and ways they are systemic, and (3) to offer some reflections on why the understanding of certain cyber risks as systemic is important, or not, for participants in insurance markets. I argue that (1) only certain cyber risks are systemic, (2) there are four different ways a risk can be systemic, (3) it is more productive for policyholders and underwriters to view cyber risks in the plural, with some being systemic and some not, and to manage those risks accordingly, and (4) it is not possible to state as a general rule that cyber-systemic risks are either more or less manageable than those cyber risks that are not systemic.

The conclusion that only some cyber risks are systemic may have an air of the obvious. To take an easy example, the use of a stand-alone computer presents certain cyber risks but no systemic risks, as we intuitively understand "cyber risks" and "systemic risks." Nonetheless, the issue whether all cyber risks are systemic risks is important in itself and is useful to better understand the varieties of cyber risks and for cyber risk management guided by that understanding. At a minimum, this article is intended to dispel some of the misperceptions arising out of loose and casual claims that all cyber risks are systemic. These misperceptions may lead either to the (incorrect) view that cyber risk

2. LLOYD'S & AIR WORLDWIDE, CLOUD DOWN, IMPACTS ON THE U.S. ECONOMY 5 (2018).

3. Laurie Kamaiko, *Emerging Cyber Risk: Can Insurers 'Hack' It?*, MONDAQ BUS. BRIEFING (Dec. 6, 2017), http://www.mondaq.com/unitedstates/x/653120/Security/Emerging+Cyber+Risk+Can+Insurers+Hack+ItEmerging+Cyber+Risk+Can+Insurers+Hack+It.

4. Rainier Böhme & Gauray Kataria, *On the Limits of Cyber-Insurance*, *in* TRUSTBUS 2006: TRUST AND PRIVACY IN DIGITAL BUSINESS 31, 33 (S. Fischer-Hübner et al. eds., 2006); *see also* MARSH, ADDRESSING CYBER RISK 5–7 (2017), https://www.treasury.gov/initiatives/fio/Documents/1-Cyber_Insurance_Market_MarshLLC.pdf (stating, in Marsh PowerPoint slides, that cyber risk is systemic risk because of "widespread vulnerability," "single points of failure," and "cascading consequences").

management is no different than managing "normal" (non-systemic) risks or to the (incorrect) view that it is an insurmountable challenge (as might be heard from a harried risk manager, "my firm is doomed if it suffers a cyber attack, so why bother with insurance?"). For risk managers, a better understanding of their firms' cyber exposures, including those that are systemic and those that are not, allows them to move beyond these reactions and to formulate more effective and economical corporate strategies to manage those exposures.

The plan of this article is as follows. In Part II, I analyze the concept of "systemic" risk and discuss how it differs from two types of non-systemic risk and risk aggregation. I further distinguish four ways in which a cyber risk can be systemic. In Part III, I critique the broad view that cyber risk is systemic risk. I do this principally by presenting a classification scheme for cyber risks and showing that many of those risks are not systemic or are systemic only in certain defined circumstances. In Part IV, I discuss the implications of my analysis of cyber risks and systemic risks, which I hope will be useful for both insurers and policyholders.

II. "CYBER RISK" AND "SYSTEMIC RISK"

It is useful initially to clarify the terms "cyber risk" and "systemic risk." There is no single, commonly accepted definition of either term, and they are often used loosely in relation to other insurance concepts. In this Part II, I offer a broad definition of "cyber risk" and then move quickly to an extended analysis of systemic risk. In Part III, I return to the concept of cyber risk, distinguish 19 categories of cyber risks, and discuss whether each of them is a systemic risk or not.

A. Definitions and Distinctions

We can define "cyber risk" broadly as the enterprise risk (1) arising out of the use, operation, or adoption of digital information technology (IT) or digital operational technology (OT) within an enterprise, or (2) arising out of the sending of electronic data to and receipt of electronic data from others within or outside of an enterprise.[5] This definition

5. This definition is taken from and modifies the definition found in MARSH & HM GOV'T, UK CYBER SECURITY: THE ROLE OF INSURANCE IN MANAGING AND MITIGATING THE RISK 8 (2015), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf (quoting ISACA, IT RISK FRAMEWORK 11 (2009), http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf). For an alternative, but consistent, definition of "cyber risk," see MARTIN ELING & WERNER SCHNELL, THE GENEVA ASS'N, TEN KEY QUESTIONS ON CYBER RISK AND CYBER RISK INSURANCE 12 (Fabian Sommerrock ed., 2016) ("Any risk emerging from the use of

allows a negative answer to our question (are cyber risks systemic risks?) simply as a semantic point. I discuss this further below[6] and merely note here that this implication of the definition is not problematic.

The term "systemic risk," when used in the literature on risk or insurance generally and cyber insurance in particular, has no one commonly accepted meaning. This literature, and the literature on systemic risk in other markets (for example, banking and financial markets), does contain certain commonly accepted elements such that, for our purposes, we can define "systemic risk" broadly as the risk that arises out of a network, and particularly of a digital network:

- that consists of standardized or functionally homogeneous nodes (computers, servers, and the like) that are interconnected and interdependent in salient respects,
- that permits cascading adverse events throughout all or many of the nodes in the network (sometimes referred to as "contagion" or "chain reactions"),
- and in which such adverse events occur at such a high rate of speed that they often cannot be contained at all or at least not in a timely fashion.[7]

These features combine such that a risk to one node in the network creates causally interdependent risks to all or some of the other nodes in the network, which is what is often called "systemic risk." The causal sequence is commonly discussed as taking either of two forms: (1) emanating from a single node to other nodes in chain-linked, falling dominos, or hub and spokes fashion, or (2) spreading from one or many nodes to other nodes in a random, probabilistic sequence, as when one or multiple pin balls hit many bumpers in no discernible pattern or when touching a spider web at a point sends ripples randomly through the web.[8] In a nutshell, systemic risk is risk arising out of two necessary

information and communications technology (ICT) that compromises the confidentiality, availability, or integrity of data or services. The impairment of operational technology (OT) eventually leads to business disruption, (critical) infrastructure break down, and physical damage to humans and property.").

6. *See infra* Section III.A.

7. *See infra* notes 8–9, 13–19 and accompanying text.

8. *See* Dirk Helbing, *Globally Networked Risks and How to Respond*, 497 NATURE 51, 54 fig.3 (2013); Olivier De Bandt & Philipp Hartmann, *Systemic Risk: A Survey* 10 (European Cent. Bank, Working Paper No. 35, 2000), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=258430. Causal sequences in complex systems reportedly involve feedback loops, simultaneous adverse effects, and other forms of random or nonsequential causation. *See, e.g.*, IAN BARTLE & MARC LAPERROUZA, ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE, SYSTEMIC RISK IN NETWORK INDUSTRIES: IS THERE A GOVERNANCE GAP? 4–6 (2009), https://infoscience.epfl.ch/record/142565/files/Bartle%20Laperrouza%20ECPR%20Sept09%20systemic%20risk.pdf; WORLD

features of a network, *viz.*, actual or functional standardization of component parts (including conduct) and interconnected and interdependent components (including actors).[9]

For "systemic risk" to be a useful term in the understanding and managing of cyber risk, it must refer to risk that is generated by or arises out of the use, operation, or adoption of a digital network and otherwise would not exist at all. If it could exist independently of such conduct, then it adds nothing to the discussion to call it "systemic." We should just refer to it as "risk," as we do with every other type of "normal" (non-systemic) risk.

Risks arising out of digital networks can be reduced or magnified by (1) actions taken by the actors in the network, (2) participants (digital nodes and actors) leaving or joining the network, and (3) the nature of the components in the network. Consider, as an example, a worldwide encryption-malware attack similar to the May 2017 WannaCry cyber attack.[10] First, if everyone except one user had patched their vulnerable operating system (OS) as soon as a patch was made available, before the attack took place, then the attack could not have spread worldwide and may never have been launched or found a target.[11] Second, if 100,000,000 vulnerable computers joined (or left) the network just before the attack, the attack surface for cyber criminals and nation-states would have been accordingly increased (or decreased) (as well as corresponding disruption and losses). Third, if the vulnerability that allowed the attack to happen persists, this increases the cyber risk of many other computers in the network relative to what this risk would be

---

ECON. FORUM, PERSPECTIVES ON A HYPERCONNECTED WORLD: INSIGHTS FROM THE SCIENCE OF COMPLEXITY 4 (2013), http://www3.weforum.org/docs/WEF_GAC_PerspectivesHyperconnectedWorld_ExecutiveSummary_2013.pdf; Helbing, *supra*, at 54, 56; De Bandt & Hartmann, *supra*, at 10–11. While this statement of the two types of causal sequence oversimplifies the causal complexities, it is sufficient for our present purposes, since those complexities—while they may be of interest in predicting how or how quickly cascading adverse effects may propagate through a network in any particular situation—do not alter the analysis of the question whether cyber risks are systemic risks.

9. For an application of these features in insurance and financial networks, see Daniel Schwarcz & Steven L. Schwarcz, *Regulating Systemic Risk in Insurance*, 81 U. CHI. L. REV. 1569, 1572–75, 1580–81, 1594–1605 (2014).

10. *See* Alex Hern & Samuel Gibbs, *What Is WannaCry Ransomware and Why Is It Attacking Global Computers?*, GUARDIAN (May 12, 2017, 12:16 PM), https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20 (explaining that the WannaCry ransomware attack used a software vulnerability in order to infect systems).

11. Dell Cameron, *Today's Massive Ransomware Attack Was Mostly Preventable; Here's How to Avoid It*, GIZMODO (May 13, 2017, 11:00 AM), https://www.gizmodo.com.au/2017/05/todays-massive-ransomware-attack-was-mostly-preventable-heres-how-to-avoid-it/; Hern & Gibbs, *supra* note 10 (discussing the software developer's patch that "ensur[ed] that the vulnerability couldn't be used to spread the malware").

if each of those devices had better OS security, which could be accomplished by fixing that vulnerability or by using an OS that does not have such a flaw.[12]

Sometimes "systemic risk" is used to refer to the risk of an entire network or system failing. Thus, for example, "systemic risk" has been defined as "the risk or probability of breakdowns in an entire system, as opposed to breakdowns in individual parts or components, and is evidenced by comovements (correlation) among all or most parts."[13] I do not find this "entire system failure" view of systemic risk particularly useful for present purposes because it is seldom the sense in which the term is used in the insurance literature and it fails to capture types of cyber risks that do not involve a complete system (network) failure, but that prima facie are systemic.

In discussions of systemic risk, authors tend to emphasize one or more of the features we have identified. One author has defined "systemic risk" as:

> the risk of having not just statistically independent failures, but interdependent, so-called 'cascading' failures in a network of *N* interconnected system components. That is, systemic risks result from connections between risks ("networked risks"). In such cases, a localized initial failure ("perturbation") could have disastrous effects and cause, in principle, unbounded damage as *N* goes to infinity. For example, a large-scale power blackout can hit millions of people. . . . The potential damage here is largely determined by the size *N* of the networked system.[14]

This definition is useful in that it contains most of the features we have identified above, and does so without committing one to a limited view of systemic risks as those that necessarily threaten an entire network. As a further example, in stressing the statistically dependent nature of systemic cyber risks and their origins in digital networks, two scholars stress the standardized or homogeneous nature of networks that create systemic risk.[15] They write that cyber risk is a systemic risk because:

---

12. *Cf., e.g.*, MARSH & HM GOV'T, *supra* note 5, at 9 ("[W]e can anticipate more frequent, larger, and even systemic attacks as an increasing number of devices go online."); Helbing, *supra* note 8, at 53 (stating that "common drivers of systemic instabilities" include "increasing system sizes" and "denser networks"); *id.* at 57 box 4 (noting the impact of decisions by individuals on "socially interactive systems").

13. BARTLE & LAPERROUZA, *supra* note 8, at 2 (quoting George S. Kaufman & Kenneth E. Scott, *What Is Systemic Risk, and Do Bank Regulators Retard or Contribute to It?*, 7 INDEP. REV. 371, 371 (2003)).

14. Helbing, *supra* note 8, at 51 box 1.

15. *See* Böhme & Kataria, *supra* note 4, at 32.

> [I]nsurance relies on the principle of independent risks while standardized system environments by themselves create a global monolithic risk manifested in virtually every standardized system. Unlike in [the] physical world, where risks are geographically dispersed, in [the] information world, network exploits, worms and viruses span all boundaries. All systems that run standardized software and processes are vulnerable, because bugs in them, once discovered, are common knowledge and can be exploited anywhere.[16]

Other discussions of systemic risk emphasize "cascading" adverse consequences arising out of one or more causal events that affect or are within a network. For example, one author writes: "Other work has studied the error and attack tolerance of networks and cascade effects in networks, where local failures of nodes or links may trigger overloads and consequential failures of other nodes or links. Moreover, abrupt systemic failures may result from interdependencies between networks or other mechanisms."[17] The "other mechanism" that is interdependent with a network may itself be another network.[18] From the World Economic Forum we learn: "When a risk cascades through a complex system, the

16. *Id.* I offer this statement here only as an example of an emphasis on standardization in networked systems as a condition of systemic risk. It is, at a minimum, overly broad and reasonably may be characterized as hyperbolic. To consider just two counter-examples, the WannaCry ransomware attack of May 2017 did not infect the computers of those users of the vulnerable OSes who had used the patch made available months earlier or who used a different OS without the vulnerability. *See supra* notes 10–11 and accompanying text. The cyber attack on the electric grid of Ukraine in 2015 apparently was confined to that country. *See* WORLD ENERGY COUNCIL, WORLD ENERGY PERSPECTIVES: THE ROAD TO RESILIENCE 19 (2016), http://www.worldenergy.org/wp-content/uploads/2016/09/20160926_Resilience_Cyber_Full_Report_WEB-1.pdf. Neither cyber risk could reasonably be characterized as "a global monolithic risk."

17. Helbing, *supra* note 8, at 52; *see also id.* at 53. An example of a systemic failure whose initial cause originated outside of the network is the August 2003 failure of the sequential shutdowns of generating units in the electric grid in the northeast United States and Canada, which affected over 55 million people and 500 electrical generating units, and was the result, in part, of trees contacting high voltage lines. PETER SOMMER & IAN BROWN, REDUCING SYSTEMIC CYBERSECURITY RISK 43 (2011), https://www.oecd.org/gov/risk/46889922.pdf.

18. Consider, for example, a cyber extortion attack that locks up the computers of a bank that plays a critical role in the daily processing of wholesale and retail payments. If that attack spreads to the computers of some of the other banks that form part of the digital payments network, that would be an example of the cyber network acting as an "other mechanism" that may cause systemic failure in the payments processing network. The inability of the attacked banks to process wholesale or retail payments may have cascading effects for many other banks whose computers are *not* subject to the same cyber event, but which are part of the payments processing network of the banks that have been attacked. *See* De Bandt & Hartmann, *supra* note 8, at 13–14. The financial community has begun to address this possible scenario, including how it may lead to a run on the banks. Telis Demos, *Banks Build Line of Defense for Doomsday Cyberattack*, WALL ST. J. (Dec. 3, 2017), https://www.wsj.com/articles/banks-build-line-of-defense-for-doomsday-cyberattack-1512302401.

danger is not of incremental damage but of 'runaway collapse'—or, alternatively, a transition to a new, suboptimal status quo that becomes difficult to escape."[19]

Finally, stressing the rapidity with which systemic risks are realized, Lloyd's writes, "[i]n the event of sustained downtime of a top cloud service provider, simultaneous damage for all of its clients and dependents could lead to catastrophic financial losses."[20]

Systemic risks are distinct from two types of non-systemic risks. One type of non-systemic risk is the familiar individualized risk that is characterized by a cause that has only one insurance-relevant effect (a one-car accident or single building burning) or only relatively few other risks that are not generated by the interconnections and standardization characterizing a network (a three car accident). A second type of non-systemic risk is that in which a cause has multiple highly correlated effects because they are in proximity to each other in some salient manner, but, again, the risks are not a creation of the interconnections or standardization that characterize a network. In the case of natural catastrophes, such as hurricanes or earthquakes, or in a non-natural event such as a massive terrorist attack, the salient proximity is spatial or geographical. While this second type of non-systemic risk shares with systemic risks the feature of highly correlated effects, it is distinct because the effects are not the result of network properties but rather are independent of each other, for example, as when all of the roofs on the houses in a town (installed by many different roofers) are ripped off by the same hurricane, or when many buildings were damaged and many persons were killed in New York City by the 9/11 terrorist attacks. By way of contrast, if the same hurricane that destroyed the roofs also caused a failure of an electric generating plant, then the cascading effects of that failure throughout the electric grid would be the realization of systemic risk.

It is also instructive to distinguish systemic risk from what is often called risk aggregation or aggregation risk. Commentary on cyber insurance sometimes suggests that aggregated risk is the same as or closely connected with systemic risk. We read, for example, that "[u]nlike traditional property insurance where aggregation is monitored by physical locations, cyber insurance aggregation can span connected systems that extend beyond physical geographies. While a large systemic

19. WORLD ECON. FORUM, THE GLOBAL RISKS REPORT 2018, at 16 (2018); *see also* De Bandt & Hartmann, *supra* note 8, at 8 ("At the heart of the concept [of systemic risk] is the notion of 'contagion' . . . .").

20. LLOYD'S & AIR WORLDWIDE, *supra* note 2, at 5; *see also* BARTLE & LAPERROUZA, *supra* note 8, at 6–9; Helbing, *supra* note 8, at 53.

risk has not yet materialized, it does not mean the risk is not present."[21] Similarly, when companies rely on each other for data for their manufacturing or operations, this creates a "digital supply chain." Lloyd's tells us that:

> [T]his supply chain of digital interdependencies is now widely recognised as a significant source of risk aggregation by insurers. If a cyber attack occurs on a critical node of the cyber supply chain, such as a major cloud vendor, the attack could cause systemic business interruption to all associated businesses that rely on the vendor's services and systems to operate.[22]

Contrary to such suggestions, while systemic risk often is associated with aggregated risk, the two concepts are distinct. Aggregated risk (or risk aggregation) refers to the over-concentration or heavy concentration of insured loss exposure, where multiple losses impact one or many lines of insurance beyond the actuarial projections on which the insurance was underwritten.[23] The term is often used in connection with non-systemic risks such as natural catastrophes and terrorist attacks, and in those contexts the "over-concentration of loss exposure" usually refers to a particular geographic location where the risk is likely to occur or has occurred, for example, an area with a high risk of hurricanes or earthquakes.[24] In the case of cyber risks, geographic location is not a necessary condition of risk aggregation. A single cyber attack can spread globally and thereby create aggregation risk. For cyber risk, sources of risk arising out of standardization and interconnection play the role that spatial proximity plays in risk aggregation arising in connection with large-scale natural catastrophes. These sources of risk may be critical nodes ("bottlenecks") in the cyber network, such as a cloud service provider,[25] or widespread software vulnerabilities.[26] A cyber attack on a cloud service provider that lasts for days or weeks may have cascading global effects and theoretically could result in some insurers not being able to pay claims due to risk aggregation.[27]

Aggregated risk is highly correlated risk, and in that respect is similar to systemic risk. But not all aggregated risk is systemic risk,

21. Ashwin Kashyap & Julia Chu, *The Art of Measuring Cyber Aggregation Risk*, SYMANTEC (Dec. 15, 2016), https://www.symantec.com/connect/blogs/art-measuring-cyber-aggregation-risk.

22. LLOYD'S & AIR WORLDWIDE, *supra* note 2, at 43.

23. *See* RICHARD V. ERICSON & AARON DOYLE, UNCERTAIN BUSINESS: RISK, INSURANCE, AND THE LIMITS OF KNOWLEDGE 222–26 (2004).

24. *See id.*

25. *See infra* Section II.B.

26. *See* LLOYD'S & AIR WORLDWIDE, *supra* note 2, at 5.

27. *See* MARSH & HM GOV'T, *supra* note 5, at 23.

because the former need not arise from network properties while the latter does. Conversely, while some systemic risk may be aggregated risk—as in the example of the cloud service provider—not all systemic risk is aggregated risk. For example, a ransomware attack that spreads to computers in many nations may have limited adverse effects and those effects may have been uninsured or within the underwriting parameters of the cyber insurance policies implicated.

Finally, the issue of aggregated risk is primarily, or at least initially, an issue for cyber risk insurers rather than policyholders. That is, it is an issue of an insurer's calculating its financial exposure to any particular large-scale cyber incident across its insured policyholders or its lines of insurance, especially in the face of a dearth of meaningful data to inform the underwriting processes.[28] It typically is an issue for a policyholder only if the realization of aggregated risk renders an insurer unable to pay the policyholder's claim.[29] In contrast, systemic cyber risk is equally a challenge for insureds and insurers, because that risk arises out of a mode of doing business (through vulnerable networks) independent of either party's assessment of that risk. In principle, insurers can control or at least manage aggregation risk in the underwriting process with respect to multiple insureds or lines of insurance. Aggregation risk is a function of risks assumed by an insurer through underwriting, through acting as an insurer. Systemic risk is created by largely functionally homogeneous networks prior to and independent of any insurance transaction or conduct such as the transfer and pooling of risks or actuarial analyses of risk.

---

28. The insurance literature is replete with references to inadequate data on cyber risks due to the chronic underreporting of cyber incidents (as to their number, type, and severity), the unpredictability of the timing and happening of cyber incidents, and the number of cyber attacks (since they are caused by human actors with various motivations and means). That lack of data, however, is not unique to cyber risks that are systemic, but is common to all types of cyber risks. *See, e.g.*, DEP'T OF HOMELAND SEC., INSURANCE FOR CYBER-RELATED CRITICAL INFRASTRUCTURE LOSS: KEY ISSUES 1–2 (2014), https://www.dhs.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf (noting that the first-party cyber insurance market is nascent due to a "lack of actuarial data; aggregation concerns; and the unknowable nature of all potential cyber threat vectors"); ELING & SCHNELL, *supra* note 5, at 10 ("Data on cyber risk are scarce, *e.g.*, because the victims are reluctant to report such events."); LLOYD'S, *supra* note 1, at 26 (noting that one of the challenges in properly assessing cyber risk is "[i]nsufficient or poor quality loss information—available historical data does not reflect the current environment or evolving threat landscape" and also noting the "[u]ncertain value of loss information" that insurers now possess). Some authors believe that systemic risks are inherently not susceptible to being analyzed on the basis of past data as are "normalized," non-systemic risks. *See, e.g.*, WORLD ECON. FORUM, *supra* note 19, at 55 ("Systemic effects generally cannot be extrapolated from past data, but require different techniques to engage with the uncertainty of multiple futures.").

29. *See* MARSH & HM GOV'T, *supra* note 5, at 6.

As an example of cyber risk aggregation, a cyber attack on a major cloud service provider could have harmful effects on many policyholders in many industries, including financial services, software and tech services, hospitality, retail, and healthcare.[30] In addition, aggregated risk may be reflected in the insured losses, including third-party liability claims, covered under multiple lines of insurance, including cyber, property, directors and officers, technology errors and omissions, general liability, workers compensation, political risk, sabotage and terrorism, medical malpractice, and healthcare professional.[31] Risk aggregation is particularly problematic for insurers when they have not underwritten and priced cyber risk into noncyber policies, such that a massive cyber attack leaves them financially vulnerable or unable to meet their coverage obligations.

B. Further Distinctions: The Lloyd's Hypothetical Attack on Electric Generation Plants

To further clarify the concept of systemic risk, it is useful to consider the hypothetical cyber attack that Lloyd's holds out as an example of systemic cyber risk. In its study, entitled *Business Blackout*,[32] Lloyd's considers the effects of a hypothetical cyber attack on components of the United States electric grid. In the Lloyd's scenario, an unnamed group uses a piece of malware to infect the computers in the control rooms of 100 electric generation plants. *Each control room is infected independently of the others*. Because of protective relays, the malware does not spread beyond the control rooms at 57 percent of the sites. Ultimately, when the attack command is given, the malware is used to disrupt and destroy over 70 generators "*by exploiting the systemic importance of control rooms, with each control room typically managing several generators*."[33] This attack has widespread effects throughout the electric grid, and causes a massive electrical outage and substantial economic losses in the northeastern United States.[34] Lloyd's uses this hypothetical to illustrate that cyber risks are characterized by "systemic exposure": "Digital networks and shared technologies form connections that can be exploited by attackers to generate widespread impacts."[35] Is

30. *See* LLOYD'S, COUNTING THE COST: CYBER EXPOSURE DECODED 29 (2017), https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2017/cyence/emerging-risk-report-2017—-counting-the-cost.pdf.

31. *See id.* at 31.

32. *See* LLOYD'S, *supra* note 1.

33. *Id.* at 11 (emphasis added).

34. *See id.* at 9–13.

35. *Id.* at 3; *see also id.* at 25 ("[Cyber] risk itself is not constrained by the conventional boundaries of geography, jurisdiction or physical laws. The scalability of

Lloyd's characterization of its hypothetical as an example of systemic risk correct? Is it useful in understanding cyber risks and managing them?

The Lloyd's study is correct that the cyber risk *internal to each firm is* systemic. The computers in each control room control several generators and the adverse effects cascade from those computers to the networked generators at each site. That, however, does not make the focus of the hypothetical—multiple independent infections and separate external attacks—a *cyber* risk that is systemic outside of each firm or from one firm to another. Nothing in the hypothetical's contemplated chain of adverse cyber effects is a function of networked connections between control rooms at different sites—such connections are not part of the hypothetical. There are no cascading adverse *cyber* effects from one control room to another. There are cascading *network* effects throughout the electrical grid and beyond. Those, however, are not cyber (digital, computer) networks. The cascading effects in those other networks reflect the shocks from the cyber networks acting as external causes of those adverse effects, or, in other words, they are systemic effects spreading through different networks. To sharpen the point, if the attackers infected only one control room's computers and that disrupted or destroyed the generators at that one site, and thereby caused a massive failure of the electrical grid, no one would think of that as an example of systemic *cyber* risk outside of that one site. Even if the attackers independently attacked one site a week until all the control room computers in the hypothetical were infected, that still would not make the cyber risk systemic outside of each site. The fact that they were all attacked at once does not change that conclusion.

There are two ways to view the Lloyd's hypothetical. First, Lloyd's has used the term "systemic risk" too loosely and in fact has painted a picture of non-systemic digital risk analogous to an earthquake or hurricane. The "digital hurricane" hypothesized—in which each control room is attacked independently of other control rooms by a malevolent actor and there are no cascading effects from one control room's computers to another's—is not a picture of systemic risk. There are no cascading effects from one control room's computers (a node) to another's, even if the damage from this "digital hurricane" is widespread and highly correlated, just as the many houses independently "attacked" and damaged by a natural hurricane do not constitute systemic risk.

Alternatively, we may view the Lloyd's hypothetical as an example of one form of systemic risk, namely, "vertical-internal" systemic risk. It

---

cyber attacks—the potential for systemic events that could simultaneously impact large numbers of companies—is a major concern [for cyber insurers.]").

is "vertical" systemic risk because the attack was made on a critical node in the network (control room computer(s)) from which the cascading effects flow (downward) to other digital nodes (the generators) dependent upon or controlled by that critical node.[36] It is "internal" because the critical node is internal to the enterprise. In contrast, an example of a "vertical-external" systemic risk would be a cyber attack on a major cloud service provider, leading to an outage of that provider. A vertical-external attack is likely to have cascading adverse effects (downward) for all of a provider's customers because the provider is a bottleneck for customers who cannot do business without it (just as the computers in the Lloyd's hypothetical are bottlenecks for the generators they control). The cloud provider is a critical point of the Internet infrastructure for those customers who use it. This attack is "external" because the critical node, the cloud service provider, is external to any firm that is an adversely affected customer. Similarly, the distributed denial of service attack on Dyn, Inc., a domain name system service provider, in October 2016, was an actual vertical-external attack on a critical node in the Internet on which numerous large businesses (including Twitter, CNN, and Reddit) depended to direct consumers to their websites.[37] A successful attack on one of the critical technical protocols on which the Internet depends, such as the Border Gateway Protocol (which determines routing between Internet service providers) or Internet exchange points (the nodes that connect different computer networks throughout the Internet), would be other examples of the vertical-external systemic risk.[38]

This sort of vertical-internal or vertical-external systemic failure is to be distinguished from one in which the target of the attack is not a critical piece of Internet infrastructure but nonetheless is a conduit for the spread of malware, a virus, a worm, or the like to any other node in the network. We can call this "horizontal" systemic risk. The WannaCry ransomware attack reflects this horizontal-external systematicity because

36. *See* SOMMER & BROWN, *supra* note 17, at 42 ("Some network designs may be vulnerable to a large-scale cascade triggered by the disabling of a single key node . . . ." (citation omitted)). Any vertical systemic risk can also be viewed on a hub and spokes model, where the critical node is the hub and the adverse effects cascade through the spokes to each node dependent upon or controlled by the hub. Note that if a rim or wheel connects the nodes at the end of the spokes, then the cascading effects between those nodes would represent horizontal systemic effects.

37. *See* Mark Camillo, *Cyber Risk and the Changing Role of Insurance*, 2 J. CYBER POL'Y 53, 56 (2017); Nicky Woolf, *DDoS Attack that Disrupted Internet Was Largest of Its Kind in History, Experts Say*, GUARDIAN, (Oct. 26, 2016, 4:42 PM), www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

38. *See* ELING & SCHNELL, *supra* note 5, at 27; SOMMER & BROWN, *supra* note 17, at 5; *see also* LLOYD'S & AIR WORLDWIDE, *supra* note 2, at 46–47 (providing additional examples of the vertical-external systemic risk).

the many points of attack were not critical (bottleneck) nodes in the Internet infrastructure. A cyber attack on a major cloud service provider also will be a horizontal-external attack to the extent that the disruption of digital supply chains spreads from customers of the cloud provider to their vendors or customers, even when those vendors or customers are not customers of the cloud provider. The causal sequence, then, is vertical when it proceeds from a single critical node in the network (the cloud provider) to each of its customers, and horizontal when it proceeds from all or some of the customers to their customers, vendors, and so on.[39]

In the Lloyd's hypothetical, the cyber risk arises from the standardized digital systems employed by all of the control rooms, which allows the same malware to infect each of them. That, however, is not a horizontal systemic risk because the malware and adverse effects do not spread from one control room to another. If every bank in the United States left its front door and vault open every night, criminals could exploit that standard practice, but a theft from one bank would not necessarily (or even probably) have cascading effects on other banks; if thieves attacked other banks, they would do so independently of any network interconnections with the first bank. Similarly, if every builder in a hurricane-prone area used the same shoddy roofing practices, that would not count as systemic risk. If the computers in each plant's control room were interconnected with the computers at other plants' control rooms, (1) thereby spreading the malware from one to the other or (2) such that an activation of the malware in one of the computers caused adverse (cascading) effects in the computers at other sites, then the risk would be horizontally systemic. This would be the case because the adverse effects would be the result of digital network effects throughout the network and that do not begin with a single critical node that controls the flow of data to or from other nodes (presumably, any one of the control rooms was as good a target as any other). We will return to these distinctions between vertical and horizontal and internal and external systemic risk below,[40] and consider their implications for policyholders and insurers there.

The Lloyd's blackout hypothetical is also illustrative of a second important analytic point, namely, that whether any given risk is a systemic risk depends in part on how one defines the system or network.

39. The terms "vertical" and "horizontal" are not intended to suggest that causality in networks is neatly sequential, chain-linked, or "falling dominos" causality. *See supra* note 8 and accompanying text. The terms "vertical" and "horizontal" are principally intended to distinguish causal sequences through a critical node (bottleneck) from those that do not involve a critical node, respectively.

40. *See infra* Part IV.

In the blackout hypothetical, "the protective relays [that] make the attack non-viable at 57 [percent] of [the] control rooms"[41] effectively take those control rooms' computers out of the relevant network. While many firms worldwide were adversely affected by WannaCry, the affected firms were only those that used certain older OS's and had not implemented the security patch that previously was made available.[42] Those firms utilizing a later version of an OS, a different manufacturer's OS, or which had patched their vulnerable OS were not subject to the cascading network effects of WannaCry.[43] For purposes of assessing their risk from WannaCry, these firms were not part of the relevant network, even though they were full participants in the cyber network we call the Internet or worldwide web. In contrast, in the cloud provider example, the salient network is defined as the provider and its customers (and perhaps also those digitally upstream and downstream from the customers). The only way for *a customer* of the cloud provider to avoid the network effects of the attack on the provider would be to use a different cloud provider or to not use cloud services at all. If the attack were to disable the provider's provision of services, there would be no way to remain in that network and not suffer the effects of that attack.

Generic and loose views of a digital network, the system (for example, all digital devices in the Internet or a local area network (LAN)), may tend to exaggerate systemic risk. We see this reflected in some of the quotations at the beginning of this article.[44] Similarly, very narrow definitions—for example, all users of operating system *A*, who have encrypted their critical data, have appropriate firewalls, and have cybersecurity measures, *X*, *Y*, and *Z*—may underestimate systemic risk.

Of more immediate practical import, one of the technical risk management challenges illustrated by these examples is for firms to retain the standardization and interconnections that allow them to be fully functional participants in digital networks, while at the same time differentiating their software, hardware, and users in ways that minimize network (systemic) risks (for example, through patches, firewalls, encryption, anti-virus software, employee training, and so on). As a general rule, less differentiation increases system standardization, interconnectedness, and systemic risk, while greater differentiation decreases standardization, interconnectedness, and systemic risk (which at the theoretical end point would result in no system at all).

41. LLOYD'S, *supra* note 1, at 11.
42. *See* Cameron, *supra* note 11; Hern & Gibbs, *supra* note 10.
43. *See* Cameron, *supra* note 11; Hern & Gibbs, *supra* note 10.
44. *See supra* Part I; *supra* notes 1, 3 and accompanying text.

This extended analysis of the concept of systemic risk has been necessary because if this concept is not clearly distinguished from related concepts, then it is difficult, if not impossible, to undertake useful and productive underwriting or management of such risk. One author, for example, quotes and adopts the Financial Stability Board's definition of "systemic risk" as "the risk of disruption to the flow of financial services that is (i) caused by an impairment of all or parts of the financial system; and (ii) has the potential to have serious negative consequences for the real economy."[45] The author then notes the "challenges" in determining whether cyber crime in securities markets is systemic and the lack of "recognized thresholds and benchmarks for determining the line between systemic and non-systemic cyber-crime."[46] These "challenges" and lack of "thresholds and benchmarks" should come as no surprise given the definition of "systemic risk" the author and the Financial Stability Board adopt. Their definition does not distinguish the risks that arise from the standardization and interconnectedness of the components of a network from those that do not, and further does not demarcate systemic risk as risk relating to cascading adverse network effects (or "contagion"). The quoted definition, with a few minor changes, is as readily applicable to a hurricane or earthquake, as discussed above. These are highly correlated, but not systemic, risks. Consensus on "thresholds and benchmarks" will follow from consensus on what constitutes systemic risk and how it is distinguished from "normal," non-systemic risks.

III. THE VARIETIES OF CYBER RISKS

The preceding analysis of the concept of systemic risk takes us part of the way to a complete answer to our question whether cyber risks are systemic risks. The remaining ground is covered by analyzing the concept of cyber risk, considering the principal kinds of cyber risks, and asking which of those risks are systemic, if any.

A. The Merely Semantic Answer to Our Question

In Section II.A, I defined "cyber risk" broadly as the enterprise risk (1) arising out of the use, operation, or adoption of digital IT or digital OT within an enterprise or (2) arising out of the sending of electronic data to and receipt of electronic data from others within or outside of an enterprise. This definition allows us to answer our question, by fiat, in

45. Rohini Tendulkar, *Cyber-crime, Securities Markets & Systemic Risk* 23 n.112 (IOSCO Research Dep't & World Fed'n of Exchanges, Staff Working Paper 2/2013, 2013) (emphasis omitted), https://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf.

46. *Id.* at 22–23.

the negative.[47] I note this only as an analytic point before moving to the more substantive and practically important analysis of our question.

If systemic risk is risk that arises out of a network, as I have argued, then our broad definition of "cyber risk" allows us to answer our question in the negative, since there are uses of digital IT and OT that are unconnected to a network, and more specifically to the Internet. Obviously, the use of a stand-alone computer presents certain cyber risks (software glitches, data theft or corruption) that are not systemic. Similarly, the use of computers that are part of a LAN that is not connected to the Internet creates systemic risk only within that network and little to no Internet-related systemic risk. Until a nation-state or cyber criminal figures out how to penetrate an air-gapped LAN, or unless an Internet-related risk is introduced manually (through the insertion of an infected thumb-drive, for example), external-Internet-related systemic risks will not exist for a LAN.[48]

With that understanding, we now proceed to the more interesting and practically important question: which cyber risks related to networked computers are systemic risks?

B. The Classification of Cyber Risks

We can employ two criteria to classify the principal types of cyber risks: (1) the source of the risk, whether it is internal or external to the firm, and (2) the state of mind, if any, associated with the risk, whether it was maliciously caused or not. These criteria are merely the skeleton of a useful classification scheme for the principal types of cyber risks. They do not determine the number or types of cyber risk in any concrete fashion; for that we must turn to historical or probable cyber events. Further, I intentionally limit the classification of cyber risks on these criteria to the types of risks faced by enterprises (including not-for-profit entities). I do not capture cyber risks faced by natural persons, such as cyber bullying or revenge porn.

47. Note also that a narrower definition of "cyber risk"—one that makes it synonymous with the systemic risks arising out of the use of digital networks—would, of course, lead to an affirmative answer to our question, again by fiat.

48. *See* SOMMER & BROWN, *supra* note 17, at 6.

Cyber Risk Classification Matrix for Enterprises[49]

	Internal	External
Malicious	1. Unauthorized system access by rogue internal actors (employees, independent contractors) to: (a) steal, destroy, encrypt, or alter the firm's data (personally identifiable information (PII), personal health information (PHI), and confidential business information (CBI)), software, or hardware; (b) introduce malicious code to manipulate or control the firm's IT or OT; (c) introduce malicious code to the systems of a third party; (d) create false transactions; (e) fraudulently transfer funds; (f) engage in illegal acts (e.g., insider trading, collusion with competitors, or industrial/commercial espionage); (g) engage in cyber extortion; and	4. Unauthorized system access by rogue external actors (nation-states, criminals, hacktivists, or individuals) to: (a) steal, destroy, encrypt, or alter data (PII, PHI, CBI), software, or hardware; (b) introduce malware to manipulate or control the firm's IT or OT; (c) create false transactions; (d) fraudulently transfer funds; (e) engage in cyber extortion; (f) engage in industrial/ commercial espionage; and (g) mount a denial of service attack 5. Accessing, stealing, and publishing data that inadvertently has been made accessible as a result of: (a) the misconfiguration of a system such that confidential data is

49. Portions of this matrix are taken from MARSH, UK CYBER RISK SURVEY REPORT: 2016, at 12 (2016), https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/UK%20Cyber%20Risk%20Survey%20Report%202016.pdf. I have substantially modified the matrix found in the Marsh report to achieve greater analytic clarity and comprehensiveness. For an alternative matrix, see MARSH & HM GOV'T, *supra* note 5, at 8.

	(h) create defamatory media content or content that infringes a third party's intellectual property rights 2.(a)–(h) Authorized access by rogue internal actors who engage in unauthorized acts (as identified in 1(a)–(h) above) 3. The intentional unlawful collection or storage of data (e.g., biometric data, data on children)	accessible to third parties; or (b) the sending of confidential data unencrypted or posting it to an unsecured website 6. Attack on critical infrastructure on which the Internet and other digital networks depend, e.g., electricity and telecommunications networks and the critical components of the Internet itself (domain name servers, the Border Gateway Protocol)
Non-Malicious	7. Operational error of authorized personnel, including an employee unwittingly falling for a phishing scheme or business email compromise scheme 8. Software error that impacts the firm's IT or OT network 9. Security failure that allows the firm's system to introduce malicious code to a third party's system 10. Creation of digital media content that is (unintentionally) defamatory or that (unintentionally) infringes another's intellectual property rights	13. Lost or stolen computing device (phone, laptop) 14. Introduction of computer virus, malicious code by vendor, customer, business partner, or other third party 15. Vendor supplying component parts that are infected with virus, malware, etc. 16. Vendors, customers, or business partners unintentionally releasing the firm's confidential data in its control 17. Operational error of vendor, customer, or business partner that impacts the firm's IT or OT network

	11. System failure (due to failure of hardware components, the firm's electrical infrastructure, etc.) 12. The unintentional unlawful collection or storage of data	18. Software error of vendor, customer, or business partner that impacts the firm's IT or OT network 19. System failure (due to non-firm infrastructure failure, e.g., electrical, telecommunications, Internet outage, etc.)

This matrix could be expanded to create one or more additional subcategories of cyber risks. To consider just two examples, there are (1) risks whose sources are both internal and external to the enterprise, and (2) risks that are a combination of the risks identified here. As an example of the first, a phishing scheme works only if an internal actor clicks on a link or an attachment sent by a malicious actor, usually an external actor, and thereby provides the external actor with access to the firm's computer system. Similarly, a business email compromise scheme allows the fraudulent transfer of funds from an enterprise to a criminal's bank account only if an internal actor is duped by the phony email, again usually sent by an external actor that provides the fraudulent banking instructions. It is sufficient for present purposes to categorize these risks with respect to the actions of the last actor in the causal sequence (that is, categories 5(a), 5(b), 7, and 13). As an example of the second, a cyber attack may consist of multiple assaults, such as a Distributed Denial of Service (DDoS) attack with an insertion of malware and/or data theft,[50] while our matrix considers each risk as independent of every other. With the understanding that our matrix is not exhaustive of the types of cyber risks, it is adequate to allow us to assess the claim that all cyber risks are systemic.

C. Which Cyber Risks Are Systemic, and Not?

The examination of these 19 categories of cyber risks reveals that they either (1) are not systemic risks, (2) are always or nearly always systemic, (3) are systemic only in certain circumstances, or (4) can be systemic in different salient ways from a risk management perspective. I consider these possibilities in turn.

50. *See* LLOYD'S & AIR WORLDWIDE, *supra* note 2, at 6.

1. Cyber risks that are not systemic

A few of these cyber risks will never be systemic risks (either vertical or horizontal) or will be so only in the most unusual circumstances. Categories 1(h), 2(h), 3, 10, 12, and 13 are seldom, if ever, systemic risk. Category 13, by itself, is not a systemic risk, but subsequent conduct by the actor who has come into possession of the device may create systemic risk.

2. Cyber risks that are always or nearly always systemic

Failures of an enterprise's entire digital network as a result of internal or external events (categories 6, 11, and 19) would appear to be always or nearly always systemic risks. A successful attack on a critical node within the Internet infrastructure (category 6) would appear to lead to systemic losses in almost all circumstances. When a firm's system failure (categories 11 and 19) is due to a hardware glitch or failure, then the system failure may properly be viewed as a cyber-systemic risk, because the failure is a result of some component or feature of the system itself. When the system failure is the result of the failure of non-digital internal or external infrastructure (for example, a power surge or failure), the risk may be viewed as a cyber-systemic risk (because presumably the failure cascades throughout the digital network). However, it may be viewed as a business interruption or property risk because the failure is not primarily a consequence of the *cyber* or *digital* nature of the network, but rather simply reflects the fact that computers, like most other modern technologies outside of transportation, are powered by electricity.

3. Cyber risks that are systemic or not depending on the circumstances

The remaining categories will be systemic only in certain circumstances or, when they are systemic, they can be such in different ways. Consider each of the malicious-external risks, 4(a)–(g) in the matrix. Depending on the circumstances, each of these can be either non-systemic or systemic. A large retailer may have its credit card data copied and stolen by a cyber criminal, for example, and that attack may not have any cascading cyber effects internal to the firm or for any other external networked IT user. Similarly, a cyber extortion attack may be directed only to that same retailer, and so be internally systemic, but not spread horizontally to any external networked IT user (externally non-systemic). Or, like the WannaCry attack, the cyber attack on one firm may spread worldwide as a result of network effects and attack many other firms that were not its intended or primary target (horizontal-

externally systemic).[51] Similarly, the June 2017 NotPetya attack, which masqueraded as a cyber extortion attack, but appears to have had nonfinancial motivations, and spread worldwide causing billions of dollars of losses, was horizontally-externally systemic.[52] The Lloyd's hypothetical attack on U.S. electric generation plants falls within category 4(b), and is an example of a cyber risk that is not systemic in the horizontal-external sense, but is systemic internally to the firm, i.e., in the vertical-internal sense (even though it has an external source).

The malicious-internal risks (categories 1–3 in the matrix) also may or may not be systemic depending on the circumstances. An internal actor may steal data by copying it onto a thumb drive with no further network effects within or outside of the firm. That same actor, however, may introduce malware that spreads throughout the firm's computer network, and thus would be a systemic risk within the firm and possibly also to computers external to the firm.

Many, but not all, of the non-malicious cyber events also can be systemic risks or not, depending on circumstances. An error in the firm's accounting system software (category 8) may lead to errors in the accounts receivable data, for example, but have no further cyber network effects within the firm (or external to it), while an error in the firm's software controlling electric power generators or manufacturing equipment may. The former would not represent an internal systemic risk while the latter would.

---

51. The WannaCry ransomware attack affected more than 230,000 computer systems in 150 countries. *See* Ellen Nakashima & Philip Rucker, *U.S. Declares North Korea Carried Out Massive WannaCry Cyberattack*, WASH. POST (Dec. 19, 2017), https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html?utm_term=.4654e84e4887. Media and government reports have stated that WannaCry was an attack by North Korea directed to the government of the United Kingdom, and was intended to disrupt United Kingdom government operations; it masqueraded as a cyber extortion attack to hide its source and purpose. *See, e.g.*, Thomas P. Bossert, *It's Official: North Korea Is Behind WannaCry*, WALL ST. J. (Dec. 18, 2017, 7:15 PM), https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537; Nakashima & Rucker, *supra*.

52. The NotPetya malware attack (masquerading as a ransomware attack) was initially aimed at disrupting computers in Ukraine, and then spread to computers in Denmark, India, and the United States. *See* Jeremy Kirk, *Latest Ransomware Wave Never Intended to Make Money*, BANK INFO SECURITY (June 29, 2017), https://www.bankinfosecurity.com/latest-ransomware-wave-never-intended-to-make-money-a-10069; Sarah Marsh, *U.S. Joins UK in Blaming Russia for NotPetya Cyber-attack*, GUARDIAN (Feb. 15, 2018, 5:45 PM), https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine; Ellen Nakashima, *Russian Military Was Behind 'NotPetya' Cyber Attack in Ukraine, CIA Concludes*, WASH. POST (Jan. 12, 2018), https://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?utm_term=.aa4824497af1.

4. Cyber risks that are systemic in different ways

For those cyber risks identified in the matrix that in some circumstances are systemic, or that almost always are systemic, we can view the risk as being systemic along two axes—vertical-horizontal and internal-external. This results in four types of systemic risk: vertical-internal, vertical-external, horizontal-internal,[53] and horizontal-external. The question for underwriters and policyholders is whether the different ways in which a risk can be systemic presents a greater or lesser degree of risk. Saying that a particular cyber risk is a systemic risk, even when that is true, may be far less informative or useful from a risk management perspective than it initially appears until one knows the manner in which the risk is systemic.

One federal court has distinguished three types of "malicious cyber acts:" those acts in which (1) "a computer is the target of malicious activity," where presumably "a computer" means a computer's hardware or software, (2) a computer is an essential tool for the malicious activity, and (3) "the use of a computer is incidental to the malicious activity."[54] For example, a DDoS attack would fall into category (1), cyber fraud or theft of electronic data would fall into (2), and defamatory website content would fall into (3) because such content could be published in hard copy or in a newspaper.[55]

It is tempting to use this classification scheme to categorize cyber risks as systemic or not. The scheme has the allure of simplicity, but it has two flaws. First, it is not sufficiently comprehensive. It does not capture, for example, critical nodes in the Internet infrastructure, such as the Border Gateway Protocol (category 6 in the matrix). Further, there is no simple correlation between these three categories and systemic risk. Malicious acts falling into the court's first category—attacks in which the computer is the target of the activity—may or may not represent systemic risks, or may only represent one type of systemic risk. A DDoS attack on one company (category 4(g) in the matrix) may have no cascading cyber effects beyond that company, and so may be a form of vertical-external systemic risk, but not horizontal-external systemic risk. A rogue employee may inject malware into the firm's accounting software and there may be no adverse cascading effects from one

53. A horizontal-internal systemic risk is one in which the attack is made on a non-critical (not a bottleneck) network node (a computer or other digital technology) internal to the firm, and then spreads to other nodes within the firm. An internally generated malware infusion that spreads throughout the firm's computers is an example.

54. Am. Health, Inc. v. Chevere, No. 12-1678(PG), 2017 WL 6561156, at *2 (D.P.R. Dec. 22, 2017).

55. *See id.*

computer to another; each computer in the accounting department would be no more or less adversely affected than if it were the only computer using infected software. Perhaps the most that can be said with any level of confidence is that while not all of the cyber risks that fall into the court's first category are systemic, some cyber risks that are systemic will fall into this category.

In sum, the lesson to be drawn from the matrix presented above is that some types of cyber risks can be described as always or nearly always systemic (categories 6, 11, and 19), or not (categories 1(h), 2(h), 3, 10, 12, and 13) with a fairly high level of confidence. For the remaining types, we can conclude they are systemic or not only after an examination of the particularities of that risk in a given set of circumstances. The *American Health, Inc. v. Chevere*[56] court's three-part classification scheme does not alter that conclusion.

IV. INSURANCE AND RISK MANAGEMENT IMPLICATIONS

We can conclude from the foregoing discussion that not all cyber risks are systemic, but some undoubtedly always or nearly always are, and some are in the right circumstances. Upon reflection, the conclusion that not all cyber risks are systemic has an air of the obvious, and rightly so, because examples supporting this conclusion are readily found. The conclusion that while some cyber risks are always, or nearly always, systemic is also not surprising. The limited categories of such risks may be unexpected, however, especially in light of the broad pronouncements in the literature that cyber risks are systemic risks. The more nuanced conclusion that many, or most, categories of cyber risk are systemic only in certain circumstances is perhaps the most important result of the foregoing analysis, because it requires underwriters and risk managers to determine the particular cyber risks that a firm may face in order to assess and manage those risks cost-effectively. In light of these conclusions, it is useful to ask what practical implications they have for insurance underwriters and policyholders. My remarks here are, as they must be, preliminary and general, given the variety of systemic cyber risks different enterprises face.

The most important implication of the proposition that some cyber risks are systemic may be that these systemic risks are *additional* risks facing virtually all firms; these risks historically did not exist at all, and currently do not exist outside of the use and operation of networked digital systems. Fifty years ago, if a bad actor wanted to attack or destroy all of a firm's oil refineries or manufacturing plants, it would have had to

56. Am. Health, Inc. v. Chevere, No. 12-1678(PG), 2017 WL 6561156 (D.P.R. Dec. 22, 2017).

do so building by building, site by site. Now it can do so by an infusion of malware into the firm's critical OT, which then cascades to other nodes in the firm's OT network across many states or countries.[57] Similarly, while extortion and financial theft historically have been "one-off," "normalized" risks, cyber extortion and cyber financial theft are examples of what now may be systemic risks in some circumstances. In traditional risk-analytic terms, the existence of systemic cyber risks tends to increase the probability and severity of losses, all other variables held constant, relative to a non-cyber world. This is especially the case because cascading adverse effects can spread far beyond the initial target(s) of a cyber attack, as the WannaCry and NotPetya attacks demonstrate.[58] Insurers and policyholders are living in a different—systemically riskier—risk environment than they were before the widespread adoption of digital networks and the rise of bad actors willing and able to exploit them.

Whether a particular cyber risk is systemic or not reflects different concerns for insurers than for policyholders. For insurers, systemic risk involves aggregation risk, as discussed above,[59] and in the cyber context, a lack of the actuarial data that informs standard underwriting practices[60] and an ever-changing threat landscape. These challenges may have led some underwriters to reduce the cyber coverage available in the market (through greater use of self-insurance features of cyber policies or not

57. For example, in 2014, the "Energetic Bear" virus was discovered in over 1,000 energy firms in 84 countries. Nicole Perlroth, *Russian Hackers Targeting Oil and Gas Companies*, N.Y. TIMES (June 30, 2014), https://www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html?_r=0. This virus was used for industrial espionage and, because it infected industrial control systems in the affected facilities, it could have been used to damage those facilities, including wind turbines, strategic gas pipeline pressurization and transfer stations, LNG port facilities, and electric generation power plants. *See id.* It has been suggested that a nation-state "pre-positioned attack tools to disrupt national scale gas supplies." WILLIS TOWERS WATSON, ENERGY MARKET REVIEW 21 (2016), www.willis.com/naturalresources/pdf/EMR2016/WillisTowersWatsonEmR2016.pdf. In November 2016, hackers destroyed thousands of computers at six Saudi Arabian organizations, including those in the energy, manufacturing, and aviation industries. *See* Jose Pagliery, *Hackers Destroy Computers at Saudi Aviation Agency*, CNNMONEY (Dec. 2, 2016, 5:53 AM), http://money.cnn.com/2016/12/01/technology/saudi-arabia-hack-shamoon/; *see also* Sewell Chan, *Cyberattacks Strike Saudi Arabia, Harming Aviation Agency*, N.Y. TIMES (Dec. 1, 2016), https://www.nytimes.com/2016/12/01/world/middleeast/saudi-arabia-shamoon-attack.html?_r=0. The attack was aimed at "stealing data and planting viruses." Chan, *supra*; *see also* Pagliery, *supra*. The attack also wiped the computers involved so they were unable to reboot. *See* Chan, *supra*; Pagliery, *supra*. This attack was similar to a 2012 attack on Saudi Aramco, the world's largest oil company, which destroyed 35,000 computers. *See* Pagliery, *supra*.

58. *See supra* notes 51–52 and accompanying text.

59. *See supra* Section II.A.

60. *See supra* note 28.

issuing such policies at all) or to charge higher premiums for the policies issued.

From the perspective of an insured, most generally, the issue whether cyber risk is systemic risk may be most practically meaningful as a surrogate for whether a risk is more or less identifiable or within its control, and hence, more or less subject to available risk management techniques. The critical issue for a customer-policyholder in the cloud vendor example may not be that the cloud vendor represents systemic risk, but rather that the average customer-policyholder cannot meaningfully control all or some of the risk that using a cloud provider represents, or meaningfully quantify that risk when determining its cyber policy's limits and sub-limits. Consider an electric generation company that has two critical suppliers who may be unable to perform a supply contract—a fuel supplier and a cloud vendor. Assume that the business interruption or other costs of the failure of either to perform for the same period of time are equal. From a risk management perspective, then, the systemic nature of the cloud vendor risk and the non-systemic nature of the fuel supplier risk may practically amount to the insured's greater ability to manage (control) the non-systemic risk relative to systemic risk. Cyber risks that are relatively less susceptible to being managed by technical or human resources generally will require management, when management is possible, through risk transfer mechanisms (in the form of insurance, indemnity clauses, or additional insured clauses in commercial contracts).

The distinctions I drew above[61] between the four kinds of systemic risks—vertical-internal, vertical-external, horizontal-external, and horizontal-internal—imply that a useful answer to our question "is cyber risk systemic risk?" is not a simple "yes" or "no," even for those cyber risks that are systemic. For those cyber risks, it may be more productive from the underwriting and policyholder risk-management perspective to ask "systemic in what way?" Formulating the systemic risk problem more precisely in terms of this question may be more likely to lead to better answers as to how to underwrite and manage any particular cyber risk. The owner of an electric power generating plant presumably has more control over vertical-internal systemic risk (by installing protective relays, as in the Lloyd's hypothetical) than over the vertical-external risk represented by a cyber attack on its cloud service provider. It may want to shape its cyber insurance coverage (especially the limits or sub-limits) to reflect that difference.

A word of caution is in order, however. It is tempting to say that internal systemic risks (whether vertical or horizontal), as a general rule

61. *See supra* Section II.B.

are more amenable than external systemic risks to cost-effective risk management. This proposition, however, is in need of testing against each firm's actual risks. In the WannaCry attack, for example, which was the realization of a horizontal-external systemic risk, employing technical measures (a software patch) might have been as easy and as cost-efficient as many human resource or technical risk-management techniques needed to minimize a firm's internal systemic risks. It appears that the only general "rule" one can articulate with respect to the management of systemic cyber risks turns on the issue of control—namely, to the extent that any type of cyber risk arises out of the conduct of employees or digital equipment over which the firm exercises effective control, or at least greater effective control than it exercises over actors and equipment external to the firm, generally the firm will be better situated to manage that risk than otherwise. That "rule," it must be acknowledged, runs the risk of stating the obvious.

To approach this matter of practical import a bit more systematically, we ask, what is the goal of cyber risk management for an enterprise? Pro-actively (*ex ante* a cyber incident), it is to minimize the probability of the happening of a cyber incident, and to minimize its severity if it does occur. Reactively (*ex post*), it is resiliency.[62] The reactive answer assumes that no firm is immune from a cyber attack, and that the only question is how best to survive one—how to minimize losses and damages and resume normal operations as promptly as practicable. Contrary to some suggestions,[63] there is nothing automatic or natural about risk minimization *ex ante* or resilience *ex post*.

For any identified cyber risk, there are only four ways to manage it: accept it, avoid it, mitigate it, or transfer it.[64] A firm can accept a cyber risk by doing nothing to avoid it (being passive) or by taking reasonable, cost-risk beneficial measures and realizing that some cyber risk is ineliminable (active avoidance). A firm can avoid a cyber risk in a variety of ways, such as by not entering a market, by not conducting

62. *See, e.g.*, COMM'N ON ENHANCING NAT'L CYBERSECURITY, REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY 2 (2016) https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf ("Resilience must be a core component of any cybersecurity strategy; today's dynamic cyber threat environment demands a risk management approach for responding to and recovering from an attack."); WORLD ENERGY COUNCIL, *supra* note 16, at 4 ("Greater resilience to cyber risk is critical to current and future energy security."); *see also* WORLD ECON. FORUM, *supra* note 19, at 54–55 (discussing three "new tools" for managing systemic risks, namely, structural resilience, integrative resilience, and transformative resilience).

63. *See* WORLD ECON. FORUM, *supra* note 19, at 54 ("Resilience is, in fact, a property of complex systems.").

64. *See* NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 5 (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

business in some fashion (for example, online sales), or by not contracting with certain vendors or customers (for example, vendors or customers with weak cybersecurity). A firm can mitigate its cyber risk—both before and after a cyber incident—through technical tools (for example, encryption of data, updating and patching of software), human resource tools (for example, training employees and limiting employee access to critical data and trade secrets to those with a need to know), and corporate governance tools (for example, a Board of Directors focused on cybersecurity and willing to make the necessary expenditures for it). Finally, the firm can transfer some of its cyber risk through its contractual arrangements (for example, cyber or traditional forms of insurance and other commercial contracts).

Note that the predicate for engaging in any of these forms of risk management is that the risk is identified. Knowing that a systemic cyber risk exists, and in what way it is systemic (vertical-internal, horizontal-internal, vertical-external, or horizontal-external), may be practically the most important and most difficult task for policyholders seeking to employ cost- and risk-effective strategies for managing those risks. The matrix above,[65] and the accompanying discussion of it, are intended to provide a starting point for policyholders to identify the types of systemic (and non-systemic) cyber risks that may be facing their firms. Of course, with new software and hardware vulnerabilities being discovered almost daily, and new cyber criminals and new attack methods constituting an ever-changing threat environment, how the categories in that matrix are populated will be dynamic and changing well into the foreseeable future, all of which makes risk identification challenging.

To return to the example of the risk of a cyber attack on a major cloud vendor, for any policyholder-firm that uses the cloud vendor, that risk is both a vertical-external systemic risk and also a horizontal-external systemic risk if that attack would disrupt the digital data supply chains between the policyholder and its customers or other vendors, as discussed above.[66] The policyholder can attempt to manage the vertical-external systemic risk by avoiding it (not doing business with this or any other cloud vendor) or transferring it (through contractual indemnification by the vendor or cyber insurance). But for the many policyholders who are customers, pre-incident mitigation (minimization) strategies may be nonexistent or ineffective for this vertical-external systemic risk and accepting the risk is possible, but not a meaningful form of risk management. The horizontal-external systemic risk from an

65. *See supra* Section III.B.
66. *See supra* Section II.B.

attack on the cloud vendor, even for a policyholder that does not use that vendor, arises from the disruption of digital data supply chains among the policyholder and all others who do use the attacked cloud vendor or who are exchanging data with other firms that do.[67] As to that horizontal-external systemic risk, many policyholders cannot practically avoid it, and so their risk management strategies effectively will be limited to mitigation and transference, and even some of these may have severe limitations. For example, for industries in which data in real-time is essential, certain mitigation strategies (for example, backing up data daily or hourly) will be useless. Risk transference through the contingent business interruption coverage of a cyber policy with a high limit, low retention, and short waiting period may be the only way to effectively manage this systemic risk.

V. CONCLUSION

Understanding cyber risk and how to manage it cost-effectively is not for the faint-hearted. "Cyber risk is systemic risk" may make a good lead in a glossy marketing brochure or in a trade publication article, but it does not advance our understanding of cyber risks (or systemic risks) or how to manage those risks. In an effort to advance such understanding, I have analyzed the concept of systemic risk applicable to digital networks and presented a classification scheme of the principal types of cyber risks. From these theoretical starting points, I attempted to demonstrate that (1) some cyber risks are always or virtually always systemic, some are never systemic, and some may or may not be systemic depending on particular factual circumstances; (2) the cyber risks that are systemic represent additional risks for firms relative to a non-digitally networked world; (3) for policyholders in particular, the inquiry into whether a particular cyber risk is systemic practically translates to the questions of whether that risk can be identified, whether it is susceptible to management at all and, if so, in what fashion (through cyber insurance, technical means, or some other means); and (4) perhaps most importantly, it is not possible to state as a general rule that cyber-systemic risks are either more or less manageable than those cyber risks that are not systemic. If these conclusions are sound, then understanding, identifying, and effectively managing cyber risks, whether systemic or

67. The quote from Lloyd's at the beginning of this article—"[R]eliance on a relatively small number of [cloud service] companies has resulted in systemic risks for businesses using those services[,]" LLOYD'S & AIR WORLDWIDE, *supra* note 2, at 5—fails to recognize the horizontal-external systemic risk even to those firms that do not use a cloud vendor's services.

not, will remain a challenge for underwriters and policyholders well into the foreseeable future.

***