Received: 5 December 2020 | Revised: 27 February 2021 | Accepted: 1 March 2021

DOI: 10.1111/rmir.12169

PERSPECTIVE

Risk Management and Insurance Review WILEY

Cyber risk management: History and future research directions

Martin Eling[1] | **Michael McShane**[2] | **Trung Nguyen**[3]

[1]Institute of Insurance Economics, University of St. Gallen, St. Gallen, Switzerland

[2]Strome College of Business, Old Dominion University, Norfolk, Virginia, USA

[3]College of Business, East Carolina University, Greenville, North Carolina, USA

Correspondence
Michael McShane, Strome College of Business, Old Dominion University, 2026 Constant Hall, Norfolk, VA 23529, USA.
Email: mmcshane@odu.edu

Abstract

Cybersecurity research started in the late 1960s and has continuously evolved under different names such as computer security and information security. This article briefly covers that history but will especially focus on the latest incarnation known as "cyber risk management," which includes both technical and economic/management dimensions. The main focus of the article is to review research on individual steps of the cyber risk management process and on the overall process to highlight gaps and determine research directions. Two main findings are that cyber risk is difficult to include in the overall enterprise risk management process and that a move toward cyber resilience is necessary to deal with such a complex risk. Both findings require a level of interdisciplinary collaboration that is currently lacking.

1 | INTRODUCTION

According to Hiscox (2020), the median cost of a cyberattack on a business increased from $10,000 in 2019 to $57,000 in 2020. The total cost to all firms in the Hiscox sample rose by 50% from 2019 to 2020 with opportunities for attackers increasing as more employees work at home due to the pandemic. "Fourth Industrial Revolution (4IR) technologies," such as artificial intelligence (AI), quantum computing, Internet of Things (IoT) devices, 5G networks, cloud technologies, and blockchain have the potential to drastically increase efficiency and boost economic growth, but also to increase cyber risk resulting in losses of up to US$6 trillion in

[Article updated March 18, 2021 after first online publication: With consent of all three authors, the author order has been adjusted.]

2021 (World Economic Forum, 2020).[1] Even though the firms surveyed by IBM Ponemon (2020) have increased cybersecurity spending, the average time to identify and contain a data breach has not improved over the last few years, which was 275 days in 2015 and 280 days in 2020. This information indicates that even with the increased focus and spending on cybersecurity, cyber risk does not seem to be decreasing for organizations.

This article provides a comprehensive literature review of cybersecurity from when computers were first connected in networks until the present. The early research is based on technical methods that appeared in academic information systems and related journals (Siponen & Willison, 2007). The first cyber-related article identified in an academic business journal appeared in a risk management and insurance (RMI) journal in 2003 (Hovav & D'Arcy, 2003) and with scant other research until Gatzlaff and McCullough (2010). Both articles can be classified as focusing on the risk assessment step of the risk management process, specifically estimating the impact of cyberattacks. The early cyber risk research in academic RMI journals was followed by a trickle, mainly related to cyber insurance (Biener et al., 2015), but took off with the publication of two special cyber issues (Boyer, 2020; Eling, 2018). With critical mass appearing to have been reached in RMI journals, now is time to take stock to address where cyber risk management research currently is and where we believe it should go.

This article is organized as follows. Sections 2 and 3 are both literature reviews. Section 2 presents an overview of cyber risk management by describing the historical origin and development of the topic. Section 3 organizes the literature by specific steps of the risk management process. Section 4 contains a discussion of future directions for cyber risk management research.

2 | CYBER RISK MANAGEMENT: ORIGINS AND HISTORICAL DEVELOPMENT

2.1 | Early days of computer networking and security

What became the internet, originally known as Advanced Research Projects Agency Network (ARPANET), was funded in 1969 by the US Department of Defense, and originally had four connected nodes in the network (Roberts, 1988). One of the earliest organizations to investigate networked computer crime was the Stanford Research Institute (SRI) beginning in the early 1970s with the first public report on the subject released in 1973 (Parker, 2007). The early ARPANET mainly consisted of government and university computers, which allowed easy communication and collaboration using email and news groups with no emphasis on network security (Orman, 2003). This early network included a small group of people who knew and trusted each other, and pranks were often played among the members with a collegial, not a malicious, intent. In the early 1970s, Bob Thomas created a precursor of the worm, which self-replicated across ARPANET and displayed a message ("I'm the creeper: catch me if you can") on other computers but caused no harm (Chen & Robert, 2004). However, the era of academic fun over the network soon evolved in a more serious direction.

[1]We note that the cyber loss numbers are only estimates. Anderson et al. (2013) discuss the methodological flaws of such estimates and suggest an improved alternative that in aggregate also yields a number in the hundreds of billions of US$. The authors, however, explicitly state that an aggregation is not meaningful.

A main effort in early computer security involved technical efforts in the development of encryption techniques to safeguard important information (Shankar, 1977). Even early in the days of networked computers, Madnick (1978) argued that computer security cannot be achieved by focusing only on technical measures, but an economic view involving management is also essential. In 1983, lack of security and concern about malicious activity prompted the Department of Defense to split off a separate secure network, MILnet, from ARPAnet, which continued to be a relatively open network preferred by university researchers (Broad, 1983). The first well-known malicious security incident occurred in 1986 when an international effort attempted to infiltrate computers and copy information, which was detected by Cliff Stoll (Fitzgerald, 1989). In 1988, the "Morris worm" was the first network security incident involving the automated spreading of a worm around the network that caused unwanted side effects (Orman, 2003). An estimated 10% of ARPANET-connected computers were infected and shut down, which slowed down the entire network of about 88,000 computers at the time and is considered the first Denial of Service (DoS) attack (Hoar, 2005). This prompted ARPA, which had become Defense Advanced Research Projects Agency, to establish the Computer Emergency Response Team Coordination Center. In 1989, ARPANET migrated way from being a government research project and became known as the "internet" (Lukasik, 2010).

2.2 | Evolution of cyber risk management

2.2.1 | Terminology

We use the expression "cyber risk management," however, various terms have been utilized since the beginning of the computer age, such as computer security (Madnick, 1978), information security (Blakley et al., 2001), cyber risk management (Siegel et al., 2002), information security risk management (Bojanc & Jerman-Blaič, 2008), and cybersecurity (Von Solms & Van Niekerk, 2013). This array of terminology has resulted in multiple papers attempting to reduce semantic confusion (Alshaikh et al., 2014; Craigen et al., 2014; Finne, 2000; Schatz, Bashroush & Wall, 2017; Stubley, 2013; Von Solms & Van Niekerk, 2013). The evolution and legacy of various terms related to cybersecurity continues to cause confusion and hinders an integrated response both to manage corporate cyber risk and engage in interdisciplinary research.[2]

Von Solms and Van Niekerk (2013) distinguish between information security and cybersecurity. Information security only applies to the protection of information assets whether or not the information assets are stored inside or outside cyberspace. Cybersecurity is related to both information and noninformation assets that are within cyberspace or can be affected via cyberspace. Examples of noninformation assets are humans who can be compromised and physical assets that can be damaged using cyberspace, for example, via IoT devices. We agree with this concept of cybersecurity but use the term "cyber risk management" to make clear that a risk management process is being used to manage cyber risk.

[2]Althonayan & Andronache (2018) map out the evolution of terminology from computer security to information security to cybersecurity along with a dozen more terms used since the 1960s.

2.2.2 | Risk-based approaches to managing cyber risk

Risk-based handling of information system and computer related security has been discussed in the literature for decades (Alavi & Weiss, 1985; Eloff et al., 1993; Rainer et al., 1991), however, this early work was fragmented. Blakley et al. (2001) state that information security neglects applying most aspects of the risk management process and is failing due to a focus mainly on technical risk mitigation treatments for reducing only likelihood but not the impact of security events. Siponen and Oinas-Kukkonen (2007) review information security research through the early 2000s and conclude that little interdisciplinary collaboration exists; the main focus has been on technical issues, which we classify under risk mitigation in the overall risk management process. Collier et al. (2013) argue that cybersecurity should move past a focus on "technical issues at component levels" toward systems analysis that integrates the physical, information, cognitive, and social domains.

A cyber risk management process applies both risk mitigation and risk transfer techniques to reduce residual risk to acceptable levels (Gordon et al., 2003; Marotta & McShane, 2018; Siegel et al., 2002). Siegel et al. (2002) and Gordon et al. (2003) propose a cyber risk management framework that goes beyond technical risk mitigation to add risk transfer. During the risk management process, interaction exists between risk mitigation and the purchase of insurance, that is, insurance purchasers typically pay lower premiums by investing more in risk mitigation. Given the negative externality known from other real life situations, Öğüt et al. (2011) show that this desired interaction in a "cybersecurity risk management" process breaks down under these conditions resulting in firms investing less than socially optimal in risk mitigation and insurance. Even after decades of calls for computer security to move beyond just technical measures (Madnick, 1978), the technical side still dominates the management aspect and lacks an economic view of information security (Alshaikh et al., 2014; Cannoy et al., 2006; Ganin et al., 2020; Siponen & Willison, 2007; Zeller & Scherer, 2020).

3 | LITERATURE REVIEW: BY STEPS OF THE RISK MANAGEMENT PROCESS

We follow the basic risk management process (Elliott, 2019), but with a focus on managing cyber risks and specifically on steps 2 to 4, which is the heart of the risk management process:

1. Environmental scanning
2. Risk identification
3. Risk analysis
4. Risk treatment
   - Risk avoidance
   - Risk mitigation
   - Risk transfer
   - Risk retention
   - Risk exploitation
5. Risk monitoring and process review

We do not cover the first and last part of the process (environmental scanning and risk monitoring), which are too broad for the scope of this article. Environmental scanning is related to the incorporation of the risk management process into overall corporate governance,

such as an evaluation of whether the risk management process is aligned with the organization's risk appetite and achievement of objectives (Elliott, 2019). Risk monitoring and process review are related to parts of the process that are typically outside the work of risk managers, such as evaluating the effectiveness of the risk management process by the internal audit function and reporting to the board of directors and top management on changes that need to be made to the process (Elliott, 2019). Discussions of future cyber risk and corporate governance research are covered in a separate enterprise risk management (ERM) section (Section 4.2). We also note that risk exploitation is a relatively new ERM concept with no research about whether it is a risk treatment that can apply to cyber risk and is discussed in a later ERM section as well. Table 1 and Figure 1 provide an overview of the most important papers and results for this section.

3.1 | Cyber risk identification

This section summarizes, in chronological order, the discussions surrounding cybersecurity issues in the early days and how cyber risk was eventually identified as one of the major risk categories facing organizations. The scholarly contributions classified as cyber risk identification research originated mostly from the IT discipline. The majority of these studies were conceived during the 1970s to early 2000s period following the development of computer security but before developments, such as the IoT, which dramatically increase the number of potential cyberattack surfaces.

As noted in Parker (1972), computer and/or data security has long been considered critical to businesses. However, the topic had not been given adequate attention from academics and practitioners until a malicious security breach in 1986 was detected (Fitzgerald, 1989). A survey by Hoffer and Straub (1989) in 1986 indicates that only about 60% of organizations were practicing any type of computer security. Moreover, almost half the entities surveyed spent nine hours or less a week on such a critical function (Straub & Hoffer, 1987). In addition, surveys of managers conducted in the early 1980s show that data security is not even in the top 10 of critical concerns (e.g., Ball & Harris, 1982; Brancheau & Wetherbe, 1987; Straub, 1990). Collectively, these survey results imply that in the early 1980s, managers lacked the awareness to identify cyber risk.

Prompted by the 1988 Morris worm, McAfee and Haynes (1989) is the first academic work we found to formally identify worm attacks as a realistic risk factor that can threaten the operations of businesses worldwide. Their pioneering study also encourages further research efforts devoted to this promising topic. Straub (1990), among others, adopts a more universal definition of information security issues, so called computer abuse. The term "computer abuse" is formally defined as "the unauthorized and deliberate misuse of assets of the local organizational information system by individuals, including violations against hardware, programs, data, and computer service" (Straub, 1990, p. 257). Other studies also acknowledge that data security breaches can be identified as either accidental or intentional and can arise because of both external and internal unauthorized actions (e.g., Loch et al., 1992; Rainer et al., 1991). A typical example of an accidental external information security issue is loss of data due to natural disasters such as earthquakes or hurricanes. Service interruption due to sudden death of key personnel responsible for the IT function has also been identified as a potential threat for businesses. In addition, Loch et al. (1992) highlight the imminent threat of computer viruses, which were still relatively new in the late 1980s. Fried (1994) identifies other areas that are vulnerable to cybersecurity breaches including document imaging systems, mini-supercomputers, neural network systems, wide area network (WAN) radio communications, wireless local area networks, videoconferencing, smart cards, and so forth.

TABLE 1 Summary of the most important papers at each stage of the risk management process

Research areas and papers	Main point(s)
Panel A: Cyber risk management terminology	
Madnick (1978) Sample period: N/A	Coins the term "computer security" to characterize/describe issues associated with this field of study.
Von Solms and Van Niekerk (2013) Sample period: N/A	Describe the term "cybersecurity" (or "cyber risk management" in this literature review) as the protection of both information and noninformation assets that are within cyberspace or can be affected via cyberspace.
Althonayan and Andronache (2018) Sample period: N/A	Map the evolution of terminology from computer security to information security to cybersecurity.
Panel B: Cyber risk identification	
Hoffer and Straub (1989) Sample period: 1986	Find that only 60% of organizations practice any type of computer security in the 1980s.
McAfee and Haynes (1989) Sample period: N/A	Formally realize the threats of worm attacks (e.g., the Morris worm).
Howard and Longstaff (1998) Sample period: N/A	Propose a universal framework designed to improve consistency and integrity in identifying and cataloging computer security risks.
Marotta and McShane (2018) Sample period: N/A	Promote the honeypot concept that encourages the use of decoy systems to actively attract cyber attackers for the sole purpose of identifying new types of attacks before they become widespread.
Panel C: Cyber risk analysis	
Hovav & D'Arcy (2003) Sample period: 1998–2002	Document insignificant negative shareholder reactions to cyber-related incidents.
Cavusoglu et al. (2004) Sample period: 1996–2001	Find significant negative shareholder reactions to cyber-related incidents.
Gerber and Von Solms (2005) Sample period: N/A	Promote a holistic approach that includes the risk assessments of both physical and intangible (i.e., information) assets.
Maillart and Sornette (2010) Sample period: 2000–2008	Provide evidence of an organization size effect: as organization size grows, the largest possible amount of information stolen increases even faster
Janakiraman et al. (2018) Sample period: N/A (7 months)	Find a decrease of consumer spending at the attacked retailer after the data breach announcement.
Kamiya et al. (2020) Sample period: 2005–2017	Conduct a comprehensive study that systematically evaluates both the likelihood and severity of data breaches as well as identifying the corresponding determinants.
Panel D: Cyber risk treatment – avoidance	
Falco et al. (2019) Sample period: N/A	Describe designing and using inherently secure systems as a type of risk avoidance.

TABLE 1 (Continued)

Research areas and papers	Main point(s)
Panel E: Cyber risk treatment – mitigation	
Falco et al. (2019)	Use Parkerian hexad to identify opportunities to reduce risk.
Sample period: N/A	
Gordon and Loeb (2002)	Propose optimal amount of information security investments (should not exceed 1/e of the value at risk).
Sample period: N/A	
Anderson and Moore (2006)	Describe impact of network externalities (people who connect insecure devices to the internet do not bear the full consequences of their actions).
Sample period: N/A	
Panel F: Cyber risk treatment - transfer	
Gordon et al. (2003)	Develop a framework for cyber risk management including insurance.
Sample period: N/A	
Böhme and Kataria (2006)	Propose models and measures for correlation in cyber insurance.
Sample period: 2003 - 2005	
Böhme and Schwartz (2010)	Describe unifying framework for modeling cyber insurance.
Sample period: N/A	
Mukhopadhyay et al. (2013)	Discuss design of cyber insurance products.
Sample period: N/A	
Biener et al. (2015)	Describe insurability of cyber risk (difficulties related to interrelated losses, lack of data, and information asymmetries).
Sample period: 1971–2009	
Eling and Wirfs (2019)	Distinguish between "cyber risks of daily life" (insurable) and "extreme cyber risks" (not insurable).
Sample period: 1995–2014	
Panel G: Cyber risk treatment - retention	
Garg (2020)	Finds that breached firms hold more cash than non-breached firms.
Sample period: 2005–2018	

Toward the late 1990s, scholars from IT and other related disciplines eventually became aware of the lack of consistency and integrity in cataloging computer security risks and realized the need for a universal framework. Howard and Longstaff (1998) later consolidated relevant discussions of information security incidents in a comprehensive manner and proposed a common language to be used in the field. This common language project carefully analyzes, organizes, classifies and identifies incidents and attacks that should be considered cyber threats, which we find largely consistent with the risk identification step (assets, vulnerabilities, and threats) of the traditional risk management process. In this framework, the identifiable assets include but are not limited to account, component, computer, data, internetwork, network, and process. See Figure 2, which is based on Howard and Longstaff (1998, p. 16):

One way to classify and identify cyberattacks is whether they affect the "confidentiality, availability or integrity of information or information systems" (Biener et al.,

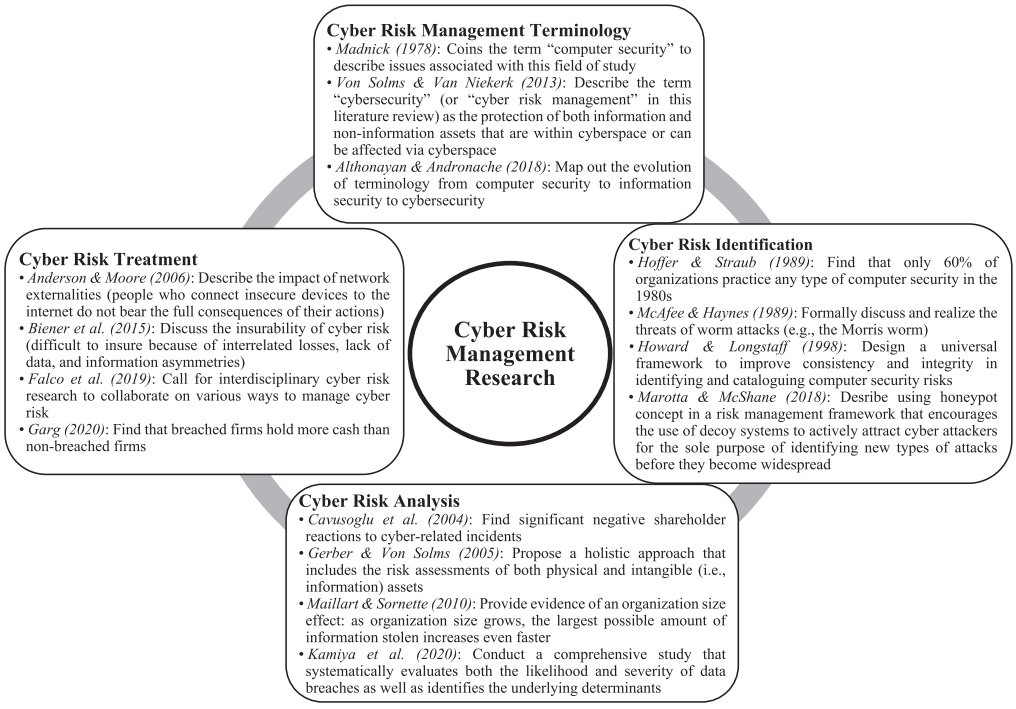

FIGURE 1 Highlights of cyber risk management research since the 1960s

2015). For example, data breach mainly affects confidentiality, denial of service and ransomware attacks involve availability of information, and website defacement reduces integrity, whereas phishing attacks might affect both confidentiality and integrity (McShane & Nguyen, 2020). Generally, an item is considered an identifiable asset when there are significantly negative consequences if the breached data are made publicly available, falsified, or no longer accessible. In addition, according to Howard and Longstaff (1998), cyber risk vulnerability can occur in the three primary areas of design, implementation, and configuration. Some noteworthy examples of identifiable threats are denial of service, corruption of information, and theft of resources. Howard and Longstaff (1998) framework of cyber risk identification receives further corroboration from other studies such as Bandyopadhyay et al. (1999).

Transitioning to the 21st century, various conceptual models are proposed to help identify cyber risk more efficiently (e.g., Chittester & Haimes, 2004; Hurst et al., 2014; Marotta & McShane, 2018). Chittester and Haimes (2004) propose the use of hierarchical holographic modeling and control objectives for information and related technology to identify potential risks to the supervisory control and data acquisition systems. Furthermore, Hurst et al. (2014) recommend the application of behavioral observation and big data analysis techniques to detect anomalies that are likely to pose as threats to the IT infrastructure. In a continuously changing race with attackers always a step ahead of defenders, scholars recently call for a more proactive risk identification approach. For example, Marotta and McShane (2018) review the honeypot concept of actively attracting cyber attackers with decoy systems for the sole the purpose of understanding and identifying new types of attacks before they become widespread.

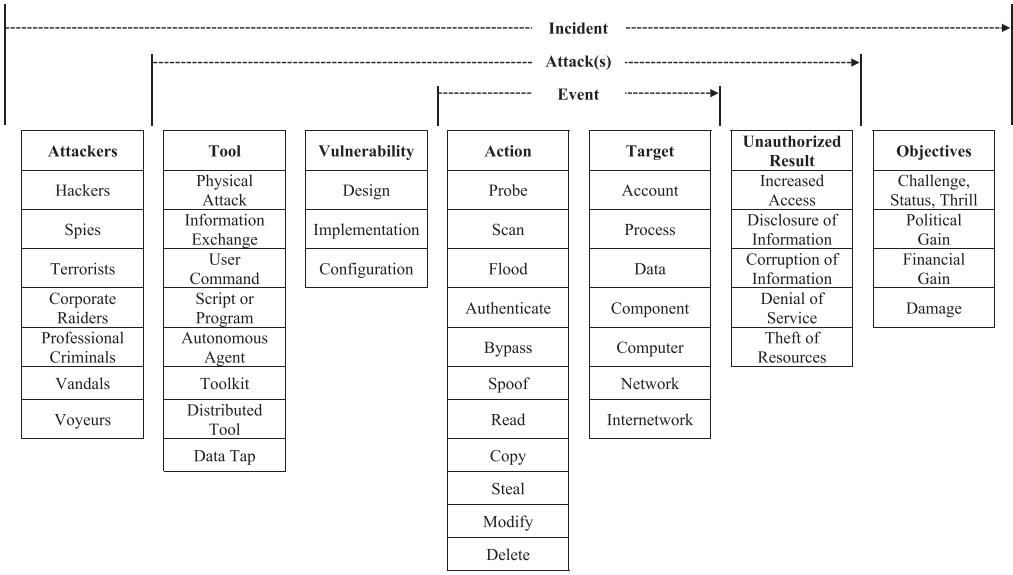

FIGURE 2 Computer and network incident taxonomy from Howard and Longstaff (1998, p. 16)

3.2 | Cyber risk analysis

Over the past five decades, scholars have gradually acknowledged cyberattacks as a major threat for businesses, and further investigated the likelihood and potential financial and other impacts of cyberattacks on firms. In terms of geographical distribution, the examinations were mostly conducted in the United States.

Gerber and Von Solms (2001) describe the difficulty of the traditional risk analysis methods to keep up with the evolution over three eras ("Computer-Centric, the IT-Centric, and Information-Centric eras") and propose an approach more suited to the Information-Centric era that includes the protection of the confidentiality, integrity and availability of information. Information is an intangible asset that is difficult to value (Burch et al., 1979) and to handle by traditional risk analysis (Frosdick, 1997). Gerber and Von Solms (2005) propose holistic risk assessment that includes both physical and intangible assets.

First, we review the literature on the potential determinants of the probability of experiencing a cyber-related event. In general, researchers report that firms with certain characteristics are more likely to experience a cyberattack, despite mixed evidence due to different time periods and sample construction criteria. Among the studies examined, firm size is typically found to be positively related to likelihood of being a target of a cyberattack. An exception is Lending et al. (2018) who focus on multiple types of cybersecurity breaches including incidents caused by both internal and external parties over the 2004–2012 period, and document instead that the probability of being breached is greater for smaller companies. According to Lending et al. (2018), a possible explanation is that larger firms may have better information security infrastructure that discourages cybercriminals from perpetrating the attacks.

There is also some inconsistency with regard to the effect of corporate governance. As reported in Lending et al. (2018), firms with better corporate governance practices (e.g., smaller board size with more financial expertise) are less likely to experience a breach. Furthermore, corporate social responsibility helps reduce the likelihood of having a cybersecurity breach, since activist hackers

may have the incentive to target socially irresponsible firms as an act of punishment for the mismanagement of environmental or product safety issues. However, in a recent comprehensive study on external data breaches over the 2005–2017 period, Kamiya et al. (2020) find no evidence that firm-level corporate governance measures such as board size, chair-CEO duality, and the percentage of outside directors can explain the chance of having a data breach caused by outside parties. In terms of financial strength, according to Kamiya et al. (2020), being a financially healthy company increases the probability of experiencing cyberattacks. In contrast, Higgs et al. (2016) examine multiple types of data breaches over the 2005–2014 period and find empirical evidence that firms with greater financial leverage are more likely to report cybersecurity breaches as these firms may have insufficient resources to invest in cybersecurity systems, which makes them more vulnerable to cyberattacks. Likewise, Boasiako and Keefe (2020) study cyber-related incidents during the 2005–2018 period and report that cybersecurity breaches are more likely to occur at financially constrained firms compared to financially healthy firms.

With respect to other firm characteristics, the literature (e.g., Boasiako & Keefe, 2020; Ettredge et al., 2018; Higgs et al., 2016; Kamiya et al., 2020) has indicated that the likelihood of being a target of successful cyberattacks is positively associated with firm age, firm value, profitability, capital expenditures, acquisitions, R&D spending, intangible assets, and growth opportunities. In addition, firms with trade secrets or inexperienced technology committees and firms without a risk management committee are more likely to be attacked. Examining a comprehensive global data set of cybersecurity breaches with actual incurred costs over the 1995–2014 period, Eling and Wirfs (2019) highlight that human behavior, in line with the IT literature, is one of the main drivers of cyber risk. At the industry-level, previous work has documented that firms operating in retail and high-tech industries or in more competitive industries tend to have higher probability of experiencing or reporting data breaches (Amir et al., 2018; Ettredge et al., 2018; Kamiya et al., 2020). In a related research stream, scholars also propose different statistical models to analyze and estimate the probability of cybersecurity breaches. For instance, Shetty et al. (2018) apply Bayesian belief networks and develop the Cyber Risk Scoring and Mitigation tool to assess cyberattack probabilities based on continuously updated software vulnerabilities and assets at risk. Recently, Insua et al. (2019) propose the use of adversarial risk analysis combined with optimization and develop a comprehensive framework to enhance the prediction of cybersecurity threats. Similarly, Sentuna et al. (2020) incorporate machine learning techniques to improve the accuracy of the estimated cyberattack probabilities.

Moving from probability to impact, McAfee and Haynes (1989) is the first academic work to analyze the potential effect of information security breaches. They investigate the impact of the 1988 Morris worm and estimate the overall costs were about $98 million in 1988 dollars. Initiated by Bharadwaj and Keil (2001) and Ettredge and Richardson (2002), a significant body of literature examines the effect of cybersecurity breaches on shareholder value as measured by short-term shareholder reactions. Based on event study methodology, shareholder reactions are typically estimated as the cumulative abnormal returns (CAR) over certain event windows. Intuitively, a cyberattack is considered an adverse event for the targeted firm due to its expected incurred costs, thus such an event should elicit negative shareholder reactions. Nevertheless, the reported empirical evidence is inconclusive.

Some event studies document significant negative shareholder reactions to cyber-related incidents (e.g., Bose & Leung, 2014; Cavusoglu et al., 2004; Gatzlaff & McCullough, 2010; Higgs et al., 2016; Modi et al., 2015; Yayla & Hu, 2011), whereas others find insignificant evidence (e.g., Amir et al., 2018; Das et al., 2012; Hovav & D'Arcy, 2003; McShane & Nguyen, 2020). In addition, there is inconsistency with respect to the reported average market value loss (if any). The literature suggests

that the observed mixed findings may be explained by firm- and attack-related characteristics as well as types of data affected. For example, Malhotra and Kubowicz Malhotra (2011) report that shareholder reactions are less negative for smaller firms, and Yayla and Hu (2011) find that DOS attacks arouse more negative market reactions than data breaches. There is also empirical evidence that shareholder value losses caused by DOS attacks are more severe than those caused by website defacement (Garg et al., 2003). Similarly, Kamiya et al. (2020) document significant shareholder wealth losses for affected firms only if the attacks lead to the loss of personal financial information. Other studies propose and document that the adverse impact of cyberattacks appears to fluctuate over time. In particular, Gatzlaff and McCullough (2010) find that more recent cyber-related incidents result in more negative shareholder reactions than attacks in an earlier period. In contrast, analyzing a comprehensive sample of cyberattacks over the 2007–2016 period, McShane and Nguyen (2020) report that the impact of cyberattacks on short-term shareholder reactions over time follows a U-shape curve. Possible explanations for the observed pattern include increased cybersecurity investments and cyber insurance usage, and/or investors becoming accustomed to the frequent occurrence of these cyber-related events.

Compared with the substantial number of studies examining the impact of cybersecurity breaches on shareholder value in the short-run, less attention has been devoted to their effect on firm long-term performance (Kamiya et al., 2020; Ko & Dorantes, 2006; Lending et al., 2018; McShane & Nguyen, 2020; Morse et al., 2011). In general, there is some agreement among the mentioned papers that cyberattacks incur additional costs for targeted firms, which lowers their long-term performance on average. Using quarterly accounting performance, Ko and Dorantes (2006) find that breached firms' return on assets decreases in the third quarter following the attack. In addition, the accounting performance measures of breached firms are found to be significantly lower than those of non-breached firms. Consistently, Lending et al. (2018) document an average long-term value loss of −3.5% as measured by 1-year buy-and-hold abnormal stock returns.

Researchers have recently looked at other aspects of a firm that can be adversely affected by cybersecurity breaches. Specifically, Iyer et al. (2020) find delayed negative reactions to cyberattacks in the bond markets, which roughly translates to $3.8 million losses in value per bond over a period of 1 month. Makridis and Dean (2018) provide empirical evidence that firm productivity is negatively associated with the number of records breached by a cyberattack. Regarding manager replacement, Lending et al. (2018) report that firms are more likely to appoint a new chief executive officer (CEO) and a new chief technology officer (CTO) after a data breach incident, whereas Kamiya et al. (2020) document insignificant evidence of CEO turnover in the targeted firms after a cyberattack. In addition, there is evidence that breached firms invest more in risk management and reduce risk-taking incentives of the management team (Kamiya et al., 2020).

Focusing on the consumer side of the impact, Maillart and Sornette (2010) analyse a comprehensive data set of personal information theft and find evidence of an organization size effect, specifically that as organization size grows, the largest possible amount of information stolen increases even faster. Mikhed and Vogan (2018) investigate a 2012 case where bank lending information was stolen from the South Carolina Department of Revenue and observe that affected bank customers tend to take necessary and immediate actions such as acquiring fraud protection services and freezing credit files after the breaches is reported. However, on average, they do not switch lenders or open new credit cards at a higher rate than unaffected individuals in the control groups. Interestingly, this finding implies that the involved financial institutions in the breach are not negatively affected in terms of profitability because they were not the direct targets of the attack. Studies from other disciplines, such as marketing and decision science, also investigate the negative

effect of cybersecurity breaches on consumer trust and consumer spending (Bansal & Zahedi, 2015; Janakiraman et al., 2018). Using proprietary data from a multichannel retailer, Janakiraman et al. (2018) document a decrease in consumer spending after the data breach announcement. Furthermore, the authors find empirical evidence of consumer migration from the breached to the nonbreached channels of the retailer. Other investigated aspects of breached firms include earnings management and real earnings manipulation (Xu et al., 2019), cash holdings (Boasiako & Keefe, 2020; Garg, 2020; He et al., 2020), abnormal bid-ask spread and trading volume turnover (Rosati et al., 2017), audit fees (Yen et al., 2018), and investment activities and external financing (Boasiako & Keefe, 2020; He et al., 2020).

According to Romanosky (2016), although the number of cyberattacks and cyber-related litigation has increased substantially over the years, the average incurred actual costs are less than $200,000 which is much smaller than the commonly cited losses of millions of dollars. Romanosky and Goldman (2017) identify the growing disconnect that prevents the successful adoption of the term "collateral damage"—the incidental losses of civilian lives or objects—in the cyber domain of US military warfare, which is also pertinent to businesses. Furthermore, they discuss the two unique challenges in evaluating collateral damage in cyber-related incidents. In particular, the pervasiveness of unknown interdependencies and the ambiguity in determining the relevant potential harms make it difficult to generate reliable estimates of collateral damage. Based on the traditional framework, they propose a modified version of the collateral damage estimation methodology that is more suitable for the cyber domain.

To conclude this section of cyber risk analysis research, several papers document spillover effects of cybersecurity breaches (e.g., Cavusoglu et al., 2004; Garg, 2020; Kamiya et al., 2020). In other words, the impact of cyberattacks can spread from the targets to other related firms in the same industry or geographical region. For example, Cavusoglu et al. (2004) find that security developers also benefit from the reported cybersecurity incidents in terms of market value appreciation. In addition, Garg (2020) shows that not only attacked firms but also their suppliers as well as their peers in the same industry or geographical region increase their level of cash holdings after the reported cyber-related incidents.

3.3 | Cyber risk treatment

The estimated likelihood and potential impact are used to determine the appropriate treatment, which includes avoidance, mitigation to reduce likelihood and/or potential impact, transfer, and retention. Treatments can interact and multiple treatments can be applied for a risk as follows:

a. Avoid the risk if possible and it makes economic sense.
b. Implement risk mitigation measures to reduce the risk as long as it is economically meaningful.
c. For residual risk remaining, select the optimal mix of risk transfer versus risk retention until the residual risk is acceptable.

3.3.1 | Avoidance

We do not dwell on this risk treatment, which is not realistic in an era so dependent on information technology and not a rational option for organizations in a digital world. However,

appropriate design of hardware and software that connects to the internet might be considered a type of avoidance. For example, IoT devices are typically designed to get out the door rapidly as minimum viable products in an entrepreneurial race to be first with little consideration for security. Requiring adequate security for any device that connects to the internet could be considered a type of risk avoidance (Falco et al., 2019), however, it can be argued this can also be a type of risk mitigation.

3.3.2 | Mitigation

Cyber security researchers typically use the Parkerian hexad to identify opportunities to mitigate risk (Falco et al., 2019), which consists of the six main elements of information security (confidentiality, possession or control, integrity, authenticity, availability, and utility). Reviews of technical mitigation treatments in information security (IS) include Siponen and Oinas-Kukkonen (2007) who categorize the literature into four security issues ("access to information systems, secure communication, security management, and development of secure information systems") and related techniques (password and biometrical authentication; cryptographic techniques; key management, virtual private networks, and programming language security).

Beyond this study on the technical aspects of risk mitigation, a prominent contribution in the context of the economics of information security investment is the Gordon and Loeb (2002) model. Their model proposes that information security investments should be calibrated by the 1/e rule, that is, the optimal amount of information security investments should not exceed 1/e of the value at risk. Another important paper on risk mitigation and the incentives for cyber risk management is Anderson and Moore (2006) who apply economic theories to practical information security problems. One important aspect is the misaligned incentives in the design and deployment of computer systems, especially the impact of network externalities: people who connect insecure devices to the internet do not bear the full consequences of their actions. This means that investments in risk mitigation and prevention also have spillover effects on other parties in a network. In this context, the authors also mention the difficulty in measuring information security risks and identification of liability as other challenges.

3.3.3 | Transfer

When it comes to risk transfer, the discussion on the use of insurance as an instrument for cyber risk management began in the early 2000s, both in academia and in the industry where a small niche market was developing for new policies covering risks from the internet. The first scholars looking at the intersection between cybersecurity and insurance came from the field of information security and the first contributions are published in information security journals such as Communications of the ACM and in the proceedings of the Workshop on the Economics of Information Security (WEIS) conferences.

One of the most cited papers from that time is Gordon et al. (2003) who discuss insurance within a framework for cyber risk management. The authors analyze the limitations of current cyber risk management and evaluate the challenges in implementing cyber insurance. The three most critical challenges are the lack of data for pricing, adverse selection, and moral hazard. One important trade-off in this discussion is between the amount of money that should be spent on cybersecurity and the amount of money used to buy cyber insurance, a discussion

which is also closely related to the above referenced paper on optimal information security investments (Gordon & Loeb, 2002).

One of the core problems when insuring cyber risk is the potential accumulation risk, meaning that all insured units might be affected by the same cyber loss event. One prominent example in this context is the Wannacry virus that affected IT systems worldwide. In their early contribution long before Wannacry, Böhme and Kataria (2006) analyze models and measures for correlation in cyber insurance and highlight that among the different cyber risk classes influencing failure of information systems, not all exhibit similar correlation properties. They introduce a twin-tier approach with a first tier being the correlation of cyber risks within a firm (e.g., correlated failure of multiple systems on its internal network). The second tier refers to the correlation at a global level meaning correlation across independent firms in an insurer's portfolio. Local cyber loss events such as an insider attack (high internal, low global correlation) are easier to insure than global loss events because the necessary premium for global loss events would be extremely high due to the lack of diversification opportunities.

Building upon these results, Böhme and Schwartz (2010) develop a unifying framework for modeling cyber insurance that classifies all market models of cyber insurance known up to that time. The framework highlights the distinct properties of cyber risk (interdependent security, correlated risk, and information asymmetries) and the informal arguments in favor of cyber insurance as a tool to align incentives for better network security. Given their analytical results questioning the viability of a market for cyber insurance, they also highlight parameters that should be endogenized in future models to improve the understanding of insurability of cyber risks. These are for instance the network topology, the information structure, and the organizational environment.

Mukhopadhyay et al. (2013) consider the concrete design of cyber insurance products. They use a Copula-aided Bayesian Belief networks model to assess cyber risk and collective risk theory to compute premium for cyber insurance products. To effectively design products, they also propose a utility-based preferential pricing model that takes risk profiles and wealth of the prospective insured firm into account before proposing the premium.

On the empirical side, research was for many years limited by the lack of useful data sets. This changed to some extent in the mid-2000s with many US jurisdictions implementing mandatory reporting requirements for data breaches and the development of respective data sets. Maillart and Sornette (2010) use such a data set to study the two fundamental properties for premium calculation, meaning the frequency and severity of data breaches. Their analysis reveals the existence of two distinct phases for the breach frequency over time: an explosive growth up to about July 2006 and a stable rate thereafter. The breach size follows a heavy-tailed power-law distribution, which remained stable over time and does not depend on the organization's type (business, education, government, and medical) and size. Edwards et al. (2016), Wheatley et al. (2016), and Eling and Loperfido (2017) extend Maillart and Sornette (2010) by enlarging the data set and applying an extended analytical approach. One drawback of data breach information is that only the number of breached data is reported with very little actual loss information in monetary values, which limits its use for premium calculation.

Biener et al. (2015) is one of the first empirical analysis papers using actual cyber loss data. While most previous studies were limited to conceptual frameworks, simulation studies, or the number of breached data, the authors generate a data set of 994 cyber loss events from the SAS operational risk database and analyze these with methods from actuarial science. Their findings emphasize the distinct characteristics of cyber risks compared with other operational risks and empirically illustrate highly interrelated losses, lack of data, and severe information

asymmetries. All these problems hinder the development of a sustainable cyber insurance market. Eling and Wirfs (2019) continue this study with a larger data set of 1574 events using the peaks-over-threshold method from extreme value theory. They identify "cyber risks of daily life" and "extreme cyber risks," the first one being easy to insure, but the latter one causing significant insurability concerns. They also confirm findings from the data breach literature that extreme value theory is needed to model cyber risk. Given all the insurability problems mentioned above, it remains unclear whether cyber risks are an insurable risk at a large scale, especially given the difficult diversification properties and the risk of change that renders past data less useful.

Romanosky et al. (2019) apply content analysis to examine actual cyber insurance policies filed with state insurance commissioners and report several major findings regarding how insurers price cyber risk in practice. First, a firm's asset or revenue base rate, rather than specific technology or governance controls, is the most common and important input used to compute insurance premiums. Some insurance companies utilize specific information gathered in the policy's security self-assessment forms whereas the majority opts for more generic risk categories. Although industry risk factors are usually included in the underwriting process, no justification or explanation for the weighting scheme is provided. In addition, insurers do not seem to follow the standard industry classification such as SIC or NAICs. Second, while some carriers use sophisticated algorithms, cyber insurance policies geared towards small businesses are much simpler. Premiums paid for insurance against first party (i.e., the targeted firm) losses are generally less expensive than those paid for insurance against third party (i.e., the targeted firm's customers) losses. This evidence implies that insurers expect costly legal actions from the involved third parties. Insurers reduce risk of the substantial uncertainty related to offering cyber insurance by including sublimits and exclusions, but this makes it difficult for policyholders to reasonably purchase the desired amount of cyber coverage. Finally, it is still unclear which level of sophistication of premium estimation is optimal for an insurance company, and which is most appropriate for evaluating the insured's risk. Wrede et al. (2020) investigate affirmative and silent cyber coverage in insurance policies and find that silent cyber represents a considerable risk for insurers. Looking at the characteristics of insurers that offer cyber insurance, Cole and Fier (2020) find that excess and surplus (E&S) lines insurers are much more likely to offer cyber coverage than admitted insurers.

3.3.4 | Retention

In the risk management process, after all the risk avoidance and mitigation has been implemented that is economically rational, the next consideration is to decide on the optimal mix of risk retention and risk transfer until the level of residual risk is acceptable. There is interaction between risk retention and transfer, meaning that risk transferred is not retained, and there is an inverse relation between amount of risk retained and the cost of insurance. Various methods can be used to retain risk, such planned funded retention (e.g., self-insurance and captives), planned unfunded retention (e.g., the choice of deductible used with insurance), and unplanned unfunded retention for risks that either were not identified or identified but cost more than forecast (Flitner, 2010; Miller & Griffy-Brown, 2018). Cyber risk retention does not appear to be a topic that has garnered much research attention, though evidence has been found that breached firms tend to have more cash holdings than non-breached firms (Garg, 2020).

4 | FUTURE RESEARCH: GAPS IN CYBER RISK RESEARCH

Based on the previous literature review, we identify gaps in cyber risk management research (see Table 2). This analysis is broken down into two main parts: potential research related to each step of the cyber risk management process followed by research directions for the overall process.

4.1 | Gaps in cyber research on specific steps of the cyber risk management process

4.1.1 | Gaps in cyber risk identification research

With respect to cyber risk identification, we urge research scholars in the business-related disciplines to explore other potential aspects that are vulnerable to cyberattacks given the continuous technological advancement in recent years. Anecdotal evidence suggests that future cybersecurity breaches will occur under three main themes: overreliance on fragile connectivity, loss of trust in the integrity of information due to falsified information spread by automated sources or bots, and eroded controls caused by the implementation of new regulations and technology (Information Security Forum, 2019). Among others, Belani (2020) lists several vulnerable areas including the cloud environment, deepfakes, smart contract hacking, social engineering attacks, AI fuzzing, AI-enhanced cyberattacks, and machine learning poisoning, which deserve more attention from both scholars and practitioners in the coming years.

More specifically, according to the Oracle and KPMG cloud thread report 2020 by Oracle.com (2020), cloud technology—one of the more recently identified assets—will continue to create new challenges for businesses in terms of cybersecurity. In many companies, the bulk of corporate data are in the cloud, which will make them attractive targets for malicious attacks. Regarding deepfakes, an AI-based technology, cybercriminals can create and scatter fake audios or videos online to impersonate important figures or spread distorted information. In response to these imminent threats, it may be a good time to re-conduct survey-based research like those studies in the 1980s to gain a general understanding of whether practitioners, especially top management teams, are fully prepared to prevent or handle the consequences caused by this new generation of cyberattacks. In addition, it is important to continue to engage in exploratory research on these issues to confirm and expand Howard and Longstaff (1998) cyber risk identification framework, which will help maintain consistency and integrity when scholars communicate about cybersecurity threats.

More research is needed to understand what malicious actors are considering with the goal of reducing their information advantage. Moving further in that direction, researchers can investigate whether to move beyond a cyber defense only posture to include cyber offense, which is promising concept but fraught with liability issues and other potential downsides, such as unintentional escalation, questionable legality, destabilization of cyberspace, and collateral damage resulting from misattribution of the perpetrator's identity (Lilli, 2021).

TABLE 2 Gaps in cyber risk research and future research directions

Cyber risk identification	**1.** Re-conducting survey-based research to gain a general understanding of whether practitioners, especially top management teams, are fully prepared to prevent or handle the consequences caused by the new generation of cyberattacks (deepfakes, smart contract hacking, machine learning poisoning, etc.). **2.** Engaging in exploratory research on these new types of attacks to confirm and expand the Howard and Longstaff (1998) cyber risk identification framework, which will help maintain consistency and integrity when scholars communicate about cybersecurity threats. **3.** Performing research to understand what malicious actors are considering with the goal of reducing their information advantage. Moving further in that direction, cyber offense, despite its potential downsides, is a promising topic.
Cyber risk analysis	**1.** Continuing to examine other determinants (e.g., managerial overconfidence) of cybersecurity breach likelihood beyond those already studied, as well as studying the relative probabilities of occurrence among different types of cybersecurity incidents. **2.** Developing models to estimate the probability of cyberattacks that can be used to decide on cyber risk treatments including both mitigation and transfer. **3.** Examining the potential impacts of cyberattacks on other aspects besides firm value (e.g., payout policies) as well as the interaction among market participants in the event of cyberattacks. **4.** Applying big data sets and/or machine learning techniques in cyber risk analysis. **5.** Conducting cyber risk analysis in other geographical regions and investigating the potential effects of cultural differences and legal origins on how market participants respond to cyberattacks. **6.** Cultivating common themes, objectives, and thematic areas for scenario analyses of potential frequency and severity of extreme cyber risks. **7.** Appling risk scores developed with Bayesian probabilities in option theoretic models to analyze and assess cyber risk. **8.** Analyzing cyber risk as operational risk within insurance companies and dependency with insurer's underwriting of cyber risk.
Cyber risk treatment	**1.** Continuing to engage in cyber risk treatment research as richer data sets containing actual loss information associated with cyberattacks become available. **2.** Performing behavioral economics studies to investigate the incentives of attackers and victims of cyber loss events. **3.** Pursuing additional analyses on the effectiveness of countermeasures, which helps determine the success of cyber risk management. **4.** Undertaking research that looks into the design and effectiveness of public and private information-sharing platforms to build more sophisticated risk models and advance the practice of cyber risk management. **5.** Studying the optimal regulation for the small and growing cyber insurance market as well as the evolution of cyber insurance when

(Continues)

	more admitted insurers enter the market and reduce domination by the excess and surplus (E&S) lines market. 6. Commencing further investigation on risk dwelling in insurance policies and how to reduce it and offer fuller cyber coverage with fewer sublimits and exclusions that policyholders desire. 7. Examining the possibilities of using alternative risk models such as cat bonds or other insurance linked securities (ILS) as an option for the cyber risk transfer.
Overall cyber risk management process	1. Integrating cyber risk into the overall ERM framework: a. Pursuing research on the inclusion of cyber risk considerations in board and top management decision making and overall corporate governance. b. Studying the differences in terminology and frameworks both within and across ERM and cybersecurity to reduce barriers and advance interdisciplinary cyber risk management research. c. Investigating the potential upsides of cyber risk and addressing the differences between ISO 31000 and NIST concerning the cyber risk definition. d. Expanding, in addition to technical cybersecurity solutions, work on socioeconomic risk factors, process, and people to provide reliable information to decision makers within enterprises. e. Examining the optimal mix among cyber risk transfer, risk mitigation, and risk retention to reach the desired level of residual risk. f. Focusing on the interaction between the various stages of the ERM process, including the correlation between cyber and other types of risks. g. Undertaking research to confirm if the findings of physical supply chain risk management research can be applied to the cyber supply chain risk. 2. Moving beyond cyber risk management to include cyber resilience: Conducting interdisciplinary studies on the potential relationship between cyber risk management and resilience, the latter of which is defined as the ability and capacity to withstand systemic discontinuities and adapt to new risk environments.

4.1.2 | Gaps in cyber risk analysis research

Based on our understanding of the cyber risk literature, we recommend the following avenues for future cyber risk analysis research. First, we encourage scholars to continue to examine other determinants of cybersecurity breach likelihood beyond those already studied. One possible direction is to investigate the effect of managerial overconfidence, especially of the chief information security officers (CISOs), on the likelihood of cyber-related incidents. Given the recent supply of available and relevant data, it is also possible to study the relative probabilities of occurrence among different types of cybersecurity incidents. Specifically, it is interesting to address the questions: What makes a certain type of cybersecurity breach more likely than another? Is it worthwhile to invest resources to handle a less popular category of cyberattacks or is it better to just ignore and assume the risk? More work also needs to be performed on developing models to estimate the probability of cyberattacks that can be used optimally to decide

on cyber risk treatments including both mitigation and transfer (e.g., Sentuna et al., 2020; Shetty et al., 2018).

Second, regarding the impacts of cyberattacks, there are still aspects other than firm value that require further investigation. For example, building on previous studies that examine the effect of cybersecurity breaches on cash holdings (Boasiako & Keefe, 2020; Garg, 2020; He et al., 2020), researchers can look at the possible channels firms can deploy to retain more cash, for instance, firm payout policies. Rationally speaking, breached firms are expected to implement more conservative payout policies compared with nonbreached firms. Another promising research stream is to evaluate the interaction among market participants in the event of cyberattacks (e.g., Lin et al., 2020; Wang et al., 2020). For example, Wang et al. (2020) find evidence that short sellers are able to anticipate and act before data breach events, and short-selling activities indeed improve market efficiency, both of which highlight their positive role in the capital markets.

Third, in the context of information security risk assessment, Jacobs et al. (2020) discuss the trade-off between coverage and efficiency regarding the formulation of a remediation strategy in safeguarding against cyber vulnerabilities. The greater number of vulnerabilities a remediation strategy can handle, the more resources it consumes, which in turn lowers the efficiency of the strategy, and vice versa. In addition, Jacobs et al. (2020) show that a full model that utilizes big data sets and machine learning techniques outperforms previously documented heuristic approaches in terms of coverage and efficiency. More research should continue in this direction of applying these types of techniques to cyber risk analysis.

Fourth, most of the empirical evidence regarding the impacts of cyberattacks has been documented in the United States, whereas similar research conducted in other geographical regions is scant. This should become feasible with the advent of new cyber regulatory regimes around the world, such as the General Data Protection Regulation (GDPR) in the European Union, which will increase cyber event data availability. Future studies can be conducted across countries to investigate the relative likelihood and impact of cyberattacks. Although technology advancement and cybersecurity issues are not bounded by country borders, cultural differences, and legal origins may dictate how market participants (both firms and investors) respond to cyberattacks (Hofstede, 2001; Porta et al., 1998). For example, scholars can examine the potential influences of the two well-known cultural dimensions, uncertainty avoidance and long-term orientation, on how equity investors react to cybersecurity breaches. There is also limited research regarding the impacts of cyberattacks on the performance of other entities such as private companies or nongovernmental organizations (NGOs) (Imboden et al., 2013; Murciano-Goroff, 2019).

Fifth, as an alternative to deal with the lack of data, a variety of scenarios have been proposed in the applied literature and in industry studies (see e.g., Kelly et al., 2016; Ruffle et al., 2014). These worst-case scenarios include various incidents that lead to a disruption of critical infrastructure and thus to economic losses. One often discussed aspect in this context is the monocultures in soft- and hardware markets that result in potential loss accumulation in the event of a cyber incident. The projected economic effects of various scenarios show extreme variation, ranging from 0.2% to 2% of GDP in the year of the event. However, as these studies lack common approaches, objectives, and thematic areas, the comparability of the scenarios and a comparative economic impact analysis is only possible to a limited extent. All this leaves managers and policymakers with a vague idea on potential frequency and severity of extreme cyber risks, resulting in ambiguous risk management strategies as well.

Sixth, another potentially valuable research direction is to apply risk scores developed using Bayesian probabilities (Shetty et al., 2018) in option theoretic models to analyze and assess cyber risk, as has been done for credit risk. These models could prove beneficial to both insurers and the insured.

Corporate insureds could allow trusted cybersecurity companies to monitor the insured's network and provide a regularly updated risk analysis and assessment that can be used by insurers to more accurately quantify cyber risk and provide fuller cyber insurance coverage desired by the insured.

Seventh, little research has been done on cyber risk as an operational risk for insurance companies and its link to underwriting. For insurance companies, underwriting cyber risks might become less attractive if they anticipate that there might be some correlation with the insurer's own operational risk. Eling and Schnell (2016, 2020) discuss the potential dependence of insurer cyber risk underwriting and the insurer's own cyber exposures and recommend considering both in insurance regulation. Cohen et al. (2019) show that cyber losses and noncyber operational risk losses share a similar fundamental risk profile, which suggests that previously developed operational risk modeling techniques can be potential candidates to assess the direct financial consequences of cyber risk.

4.1.3 | Gaps in cyber risk treatment research

Cyber risk management today mainly focuses on prevention, which is a type of risk mitigation, while risk transfer instruments, such as insurance, are still in their infancy. Many unresolved problems need to be covered by future research. A fundamental issue is the lack of data for cyber risk management. Although databases do exist, especially for data breaches, there is no widely accepted data set that is usable for risk management and pricing of cyber insurance products. While data breach data sets have the advantage of presenting a homogenous and complete view on data breaches, they provide very little actual loss information. On the other hand, the SAS operational risk data set and other recently available cyber loss data sets have the advantage of containing actual cyber loss information but are typically very heterogenous and might be subject to reporting biases that plague other empirical studies.

Another critical aspect for cyber risk data sets is the risk of change. It is far from clear whether historical information on cyber loss events helps us to predict events in the future. This is especially important for the man-made cyber risks where the loss generation process does not follow a physical law but is subject to human behavior. Research on behavioral economics might be useful to better understand the incentives of attackers and victims of cyber loss events. There are multiple different motivations—from cybercrime with a profit motive to cyber espionage to cyber war—that need to be better understood.

Not only is there a lack of data on the risks, but lack of analyses on the effectiveness of countermeasures makes determining the success of cyber risk management a black box to some extent. Since cyber risk is prone to the fast-changing technological environment, we must also be cautious when extrapolating results into the future. As society becomes more dependent on new technologies (e.g., AI) and as systems become more interconnected (e.g., via blockchain, cloud computing, and IoT), cyber threats will become ubiquitous.

When it comes to improving the fundamental data problems, one important role is seen in public and private information-sharing platforms. While a lot of time and money has been invested in setting up such platforms, we are not aware of any research looking into the design and effectiveness of such platforms. Governmental and private initiatives directed at enhancing the availability and quality of cyber risk data will be crucial to build more sophisticated risk models, making such research very important to advance the practice of cyber risk management.

Focusing on insurance, the regulation of cyber risk insurance is another open field for researchers. It is obvious that cyber risks differ from other risks. As cyber insurance portfolios

grow, one might investigate whether new regulatory models might be needed for cyber risks. This is a double-edged sword because too many regulations might dampen the cyber insurance market and hinder innovation. However, we know that standard regulatory models do not adequately reflect the potential heavy tails and accumulation risks of cyber risks. Research on the optimal regulation for the small and growing cyber insurance market is thus needed. In a related area, more work needs to focus on the evolution of cyber insurance as more admitted insurers enter the market and reduce domination by the E&S lines market. Further investigation on risk dwelling in insurance policies and how to reduce it and offer fuller cyber coverage with fewer sublimits and exclusions desired by policyholders is also warranted.

Another recent development that is largely unexplored is the extent to which alternative risk models such as cat bonds or other insurance linked securities (ILS) are an option for the cyber risk transfer. Drawing from the experience with natural catastrophe risks, some industry experts consider other low frequency and high severity risks, such as extreme cyber risks, as a suitable target for ILS. The rising awareness of cyber threats is stimulating immense interest in finding alternative solutions for the insurability of those risks. Some instruments already exist: Credit Suisse has issued a 223 million (USD) Operational Risk Cat Bond that includes cyber risk (Artemis, 2018). However, given the distinct characteristics of extreme cyber risks (such as heavy tails, nonlinear dependence, model and parameter uncertainty, and high costs due to asymmetric information), it remains unclear in how far alternative risk transfer will work on a broader scale for these risks.

4.2 | Gaps in the overall cyber risk management process

The previous section proposed research for individual steps of the cyber risk management process whereas this section covers gaps in the overall process with a look at ERM and a discussion of cyber resilience.

4.2.1 | Integration of cyber risk into the overall ERM framework

The integration of cybersecurity programs and ERM is difficult in organizations (Stine et al., 2020) with cybersecurity often dwelling in a functional silo (Falco et al., 2019). According to ERM theory, all risks should be managed together in a portfolio (Bromiley et al., 2015; McShane et al., 2011; McShane, 2018). Cyber is a complex, hard-to-define risk that crosses organizational and research boundaries. Corporate risk management and academic research face difficulties in crossing these boundaries, which is essential for cyber risk management to be effective (Falco et al., 2019). Bharathy and McShane (2014) argue that system methods are required to deal with such risks and provide an example of implementing ERM using a system dynamics approach.

Althonayan and Andronache (2019) document a misalignment between cybersecurity management and ERM citing cyber risk being siloed resulting in unsuccessful cyber risk management, which is a serious risk governance failure. Even though cyber risk has been promoted as a risk that should be considered by boards of directors and be an important focus for corporate governance (Weill & Ross, 2004), many boards are still not equipped to make decisions related to cyber risk, which remains stuck in lower levels of many organizations (Valentine, 2016). Recognizing this shortfall, the US Securities and Exchange Commission

(SEC) since 2018 requires companies traded on US public stock exchanges to report cyber risk related information in shareholder reports (Poyraz et al., 2020). A major ERM tenet is the integration of risk management into corporate governance, which means the incorporation of risk into decision making in carrying out the corporate strategy to achieve objectives (McShane, 2018). We recommend more research on the inclusion of cyber risk considerations in board and top management decision making and overall corporate governance.

Terminology is another barrier to integrating cyber risk into an ERM framework on a couple of different levels. Collaboration across academic and industry disciplines is required to manage cyber risk with Ramirez and Choucri (2016), Shameli-Sendi et al. (2016), and Falco et al. (2019) arguing that cooperation is hindered by lack of standard cyber risk management terminology. Within enterprises, this often results in the CISO and chief risk officer (CRO) not speaking the same language causing difficulty to integrate cyber risk into ERM risk portfolios (Doherty & Watson, 2017). An implication of this difficulty is that managers are not being provided information about potential cyber losses in terms useful to make effective risk management decisions (Doe, 2019). Compounding the terminology difficulties, multiple standards/frameworks have been developed and promoted for both ERM and cybersecurity, such as COSO ERM and ISO 31000 for ERM and the ISO/IEC 27000 and NIST CSF for cybersecurity (McShane, 2018; Roy, 2020). Paananen et al. (2020) survey the literature on information security plans (ISPs) and find lack of agreement on the definition of ISP and how to develop ISPs. They document a lack of connection between the technical aspect of ISPs and management implications. At the practical level, this could result in the difficulty of cyber risk management collaboration between CISOs and CROs. Research to better understand the differences in terminology and frameworks both within and across ERM and cybersecurity could be aimed at reducing barriers to essential interdisciplinary cyber risk management research.

Another terminology issue related to the various ERM and cybersecurity frameworks is the concept of risk exploitation as a potential risk treatment. This is the ERM concept that risk represents not only a downside to be managed but can be also an opportunity to be exploited to increase firm value (McShane, 2018; Nair et al., 2014). ISO 31000 is a general risk management standard with a definition of risk that implies risk can have both a downside and an upside whereas NIST defines cyber risk as having only potential adverse effects (Aven, 2011; Linkov and Kott (2019)[3]. Future work can look deeper to understand if cyber risk only has negative effects or can have a potential upside also.

To incorporate cyber risk into an ERM process, data is required to sufficiently quantify risks. Quantification allows investment decisions to be prioritized to achieve a main goal of ERM: manage identified risks to be within acceptable levels to increase the likelihood that an enterprise will achieve its objectives. Achieving this is especially complex for potential cyber risks as described previously. Work on the economics of cybersecurity investment has been an important topic in the information technology Shameli-Sendi literature and took off with the publication of Gordon and Loeb (2002). However, the struggle to provide reliable information to decision makers within enterprises is still an issue (Schatz & Bashroush, 2017). Research has mainly focused on investment in technical cybersecurity solutions that in a risk management process would be considered risk mitigation, which is a type of risk treatment. While most research has focused on the technical side of cybersecurity, expanding work on socioeconomic

[3]ISO 31000 risk management standard definition of risk: "effect of uncertainty on objectives." NIST Cybersecurity Framework (CSF) definition of risk: "a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization."

risk factors, process, and people would be beneficial. Ashby et al. (2018) find that the typical ERM approach of estimating likelihood and consequence is not effective for emerging risks, such as cyber threats. They propose that ERM needs to deal with such risks by "reducing uncertainty through knowledge acquisition" from a diverse group of stakeholders with a wide array of expertise.

A previous section discusses work on treatment using risk transfer, but in the overall risk management process, risk mitigation and risk transfer can interact, which has rarely been studied in the context of cyber risk management research. The cost of risk transfer should typically decrease if spending on cyber risk mitigation increases (Henrie, 2013; Mazzoccoli & Naldi, 2020; Young et al., 2016). Correlation also exists between risk retention and risk transfer because in general there is an inverse relation between the amount of risk transferred and risk retained. More work on the optimal mix of cyber risk transfer and risk retention to reach the desired level of residual risk could be beneficial.

More research needs to be done on the interaction of not only various risk treatments, such as risk mitigation and transfer, but between the various stages of the ERM process including the correlation between cyber and other types of risks. For example, a correlation between cyber and pandemic risks is suspected (Lallie et al., 2020). As discussed previously, risk analysis is an important step of the risk management process. There has been substantial work on determining the impact of cyberattacks on stock prices as described by McShane and Nguyen (2020) and Poyraz et al. (2020) but not on the interaction of the risk analysis step with other parts of the ERM process. An interesting avenue for physical supply chain risk management researchers is to investigate if their work can be applied to the cyber supply chain risk, meaning the cyber risk that organizations face from their suppliers and vendors and termed interdependent security by Böhme and Schwartz (2010).

4.2.2 | Move beyond cyber risk management to include cyber resilience

A literature review by Scala et al. (2019) finds scant evidence of effective risk-based management of cyber risk. They advocate a holistic approach based on a systems perspective considering interactions between risks and developing risk governance that promotes resilience in dealing with adaptive adversaries. The resilience concept originated in material sciences, was adopted by psychology in the 1970s, and later applied to urban resilience and disaster management (Dupont, 2019). This multidisciplinary interest indicates the broad appeal of the concept, but research is still fragmented and difficult to generalize and apply to the cyber domain (Bagheri & Ridley, 2017; Linkov et al., 2013a).

Efficiency and resiliency tend to have an inverse relationship. Decisions made to increase economic efficiency often lead to less diversity and less redundancy, which reduces resiliency and increases vulnerability, resulting in complex, fragile socio-technical systems (Holling, 1996; Park et al., 2013). In an early paper aimed at the difficulties of managing supply chain risk, Starr et al. (2003) describe the difference between enterprise resilience and ERM. They define enterprise resilience as "the ability and capacity to withstand systemic discontinuities and adapt to new risk environments." In a discussion that could easily apply to cyber risk, they argue that a resilient enterprise can gain competitive advantage over less adaptive rivals by identifying, adjusting, and rapidly recovering from continuously changing risks. Lambert et al. (2013) argue that the complex, dynamic nature of cyber risk necessitates moving beyond typical risk management and technical approaches to include a variety of methods including resilience

TABLE 3 Falco et al. (2019) examples of interdisciplinary collaboration in cyber risk research

			Involved disciplines	Example
Cyber risk management process	Cyber risk identification		Computer Science + Law	Legislation is being proposed about technical attributes of cyber risk. Computer scientists should contribute to proposed technical regulatory requirements and definitional boundaries. Without collaboration here, legislators will continue to develop reactive measures that run the risk of rapid obsolescence as newer technologies are more widely adopted.
	Cyber risk analysis		Data Science + Economics	Data scientists could use clustering techniques to determine what other types of catastrophic-loss scenarios are most akin to cyber. Then, economists could develop cyber loss scenarios that are consistent with and comparable with the other types of catastrophic-event loss scenarios.
	Cyber risk treatment	Avoidance	Political Science + Management Science	Many political scientists have sought to apply nuclear weapons– deterrence doctrine to cyber, but the parallels are often weak at best. Deterrence scholars could work with management scientists who have studied nontechnical attack and defense dynamics to understand what social dynamics theories may fit with their deterrence conceptualization. Together, they could arrive at alternative mechanisms to avoid risk.
		Mitigation	Economics + Behavioral Science	Economists could investigate mechanisms to reduce cyber risk through incentives, which would benefit from working with behavioral scientists, who could provide insight into what drives human interactions and how they engage with technology.
		Transfer	Law + Management Science	Legal scholars could investigate contract mechanisms that would enable risk sharing and transfer—research that would benefit from management scientists, who could

TABLE 3 (Continued)

	Involved disciplines	Example
		provide insight as to how such a contract would affect business operations and a company's balance sheet.
Retention	Computer Science + Political Science	Political scientists are actively studying how cyber capabilities contribute to power dynamics across nations. This would benefit from a computer scientist's ability to actively monitor cyberattacks and capabilities.

engineering, scenario analysis, and multiple-perspectives systems analysis. Risk management and resilience are complementary. Risk management attempts to residual risk to acceptable levels whereas resilience is designed to enable complex, coupled systems to adapt in the face of disruption and changing conditions by sensing, anticipation, and learning (Park et al., 2013).

The risk management process involves the identification, analysis, and treatment of known threats. The extreme unpredictability and rapid development of cyber risk renders the risk identification step close to useless (Linkov & Kott, 2019). Resilience is useful for risks that are unexpected (impossible to identify in advance) and for which risk analysis is not effective (Linkov et al., 2014). Collier et al. (2014) argue that the standard risk analysis triplet of "threat × vulnerability × consequence" cannot keep up with cyber adversaries who change tactics in response to cyber defenses. Resilience management prepares for quick recovery from rapidly evolving and unknown threats (Linkov et al., 2013b). Cyber resilience has the objective to consistently "deliver the intended business outcome" even in the face of adverse cyber incidents, therefore the focus must be the business not the IT system (Björck et al., 2015). A cyber risk resiliency approach requires a move beyond a computer science view to include behavioral perspectives from psychology, economics, and human factors (Gisladottir et al., 2017). Measuring the effectiveness of a resiliency approach for organizations to deal with natural hazards is complex (Lee et al., 2013). This measurement is even more problematic when the exposure is from an intelligent, adaptive enemy as in the case cyberattacks. Linkov et al. (2013b) propose a general method for assessing cyber resilience while Jacobs et al. (2018) focus on measuring cyber resilience related to control system. The measurement of cyber resilience effectiveness will be an important direction for future research.

The relationship between risk management and resilience needs to be further investigated. Many questions come to mind in a world of complex, dynamic risks such as cyber. Should risk management and resilience be conducted as complementary or independent activities? Should risk management be generalized and integrated with resiliency? Are risk management and resilience inversely related depending on the time frame used? For example, if short-term driven, they may be inversely related; if long-term then complementary. Is resiliency just the next step in the evolution from traditional risk management to ERM to resiliency.

Various disciplines have investigated cyber risk separately, but collaboration across disciplines is essential but scant (Falco et al., 2019; Soomro et al., 2016). Overall, research to integrate cyber risk into ERM and move toward cyber resilience requires interdisciplinary collaboration (Falco et al., 2019); Table 3 summarizes potential avenues for interdisciplinary collaboration. Efforts to advance the science of cyber risk must draw upon not only computer science, but also in fields such as behavioral science, economics, law, management science, and political science.

REFERENCES

Alavi, M., & Weiss, I. R. (1985). Managing the risks associated with end-user computing. *Journal of Management Information Systems*, *2*(3), 5–20.

Alshaikh, M., Ahmad, A., Maynard, S. B., & Chang, S. (2014). Towards a taxonomy of information security management practices in organizations. ACIS.

Althonayan, A., & Andronache, A. (2018, September). Shifting from information security towards a cybersecurity paradigm. In *Proceedings of the 2018 10th International Conference on Information Management and Engineering* (pp. 68–79).

Althonayan, A., & Andronache, A. (2019, June). Resiliency under Strategic Foresight: The effects of Cybersecurity Management and Enterprise Risk Management Alignment. In *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)* (pp. 1–9). IEEE.

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, *23*(3), 1177–1206.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (Ed.), *The economics of information security and privacy* (pp. 265–300). Springer-Verlag.

Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, *314*(5799), 610–613.

Artemis (2018). Operational Re, Credit Suisse's op-risk cat bond, settles at CHF220m. https://www.artemis.bm/news/operational-re-credit-suisses-op-risk-cat-bond-settles-at-chf220m/. Accessed: 2020-12-01.

Ashby, S., Buck, T., Nöth-Zahn, S., & Peisl, T. (2018). Emerging IT risks: Insights from German banking. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *43*(2), 180–207.

Aven, T. (2011). On the new ISO guide on risk management terminology. *Reliability Engineering & System Safety*, *96*(7), 719–726.

Bagheri, S., & Ridley, G. (2017). Organisational cyber resilience: research opportunities. In *ACIS2017: Australasian Conference on Information Systems* (1–10).

Ball, L., & Harris, R. (1982). SMIS members: A membership analysis. *MIS Quarterly*, *6*, 19–38.

Bandyopadhyay, K., Mykytyn, K., Mykytyn, P. P., McKinney, V. R., & Bordoloi, B. (1999). A framework for integrated risk management in information technology. *Management Decision*, *37*(5), 437–445.

Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems*, *71*, 62–77.

Belani, G. (2020). Cybersecurity threats to be aware of in 2020. IEEE Computer Society (online). https://www.computer.org/publications/tech-news/trends/5-cybersecurity-threats-to-be-aware-of-in-2020. Accessed on Oct 28, 2020.

Bharadwaj, A., & Keil, M. (2001). The effect of information technology failures on the market value of firms: An empirical examination. INFORMS 2001 Miami.

Bharathy, G., & McShane, M. (2014). Applying a systems model to enterprise risk management. *Engineering Management Journal*, *26*(4), 38–46. https://doi.org/10.1080/10429247.2014.11432027

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*(1), 131–158.

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience–fundamentals for a definition, *New contributions in information systems and technologies* (pp. 311–316). Springer.

Blakley, B., McDermott, E., & Geer, D. (2001, September). Information security is information risk management. In Proceedings of the 2001 workshop on New security paradigms (pp 97–104).

Boasiako, K. A., & Keefe, M. O. C. (2020). Data breaches and corporate liquidity management. *European Financial Management*.

Bojanc, R., & Jerman-Blaič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, *28*(5), 413–422. https://doi.org/10.1016/j.ijinfomgt.2008.02.002

Bose, I., & Leung, A. C. M. (2014). Do phishing alerts impact global corporations? A firm value analysis. *Decision Support Systems*, *64*, 67–78.

Boyer, M. M. (2020). Cyber insurance demand, supply, contracts and cases. *The Geneva Papers on Risk and Insurance: Issues and Practice*, *45*, 559–563. https://doi.org/10.1057/s41288-020-00188-1

Brancheau, J. C., & Wetherbe, J. C. (1987). Key issues in information systems management. *MIS Quarterly*, *11*, 23–45.

Broad, W. J. (1983). Computer security worries military experts. *New York Times*, 25.

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique and research directions. *Long Range Planning*, *48*(4), 265–276. https://doi.org/10.1016/j.lrp.2014.07.005

Böhme, R., & Kataria, G. (2006, June). Models and measures for correlation in cyber-insurance. In *WEIS* (Vol. 2, p. 3).

Böhme, R., & Schwartz, G. (2010, June). Modeling cyber-insurance: Towards a unifying framework. In *WEIS*.

Burch, J. G., Strater, F. R., & Grudnitski, G. (1979). Information systems: Theory and practice. 2nd Edition, Canada: John Wiley & Sons, Inc.

Cannoy, S., Palvia, P. C., & Schilhavy, R. (2006). A research framework for information systems security. *Journal of Information Privacy and Security*, *2*(2), 3–24.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70–104.

Chen, T. M., & Robert, J. M. (2004). The evolution of viruses and worms. *Statistical methods in computer security*, 1. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.115.639&rep=rep1&type=pdf

Chittester, C. G., & Haimes, Y. Y. (2004). Risks of terrorism to information technology and to critical interdependent infrastructures. *Journal of Homeland Security and Emergency Management*, *1*(4), 1–20.

Cohen, R. D., Humphries, J., Veau, S., & Francis, R. (2019). An investigation of cyber loss data and its links to operational risk. *Journal of Operational Risk*, *14*(3), 1–25.

Cole, C., & Fier, S. (2020). An empirical analysis of insurer participation in the U.S. cyber insurance market. *North American Actuarial Journal*, 1–23. https://doi.org/10.1080/10920277.2020.1733615

Collier, Z. A., DiMase, D., Walters, S., Tehranipoor, M. M., Lambert, J. H., & Linkov, I. (2014). Cybersecurity standards: Managing risk and creating resilience. *Computer*, *47*(9), 70–76.

Collier, Z. A., Linkov, I., & Lambert, J. H. (2013). Four domains of cybersecurity: A risk-based systems approach to cyber decisions. *Environment Systems and Decisions*, *4*(33), 469–470.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://timreview.ca/article/835

Das, S., Mukhopadhyay, A., & Anand, M. (2012). Stock market response to information security breach: A study using firm and attack characteristics. *Journal of Information Privacy and Security*, *8*(4), 27–55.

Doe, A. (2019). When CIO Means Chief Insight Officer (online). https://risk-management.cioreview.com/cxoinsight/when-cio-means-chief-insight-officer-nid-15131-cid-141.html. Accessed on Nov 8, 2020.

Doherty, J., & Watson, M. (2017). Cyber and the C-Suite: New cyberrisk responsibilities for Chief Risk Officers. *Risk Management*, *64*(6), 30–34.

Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity*, *5*(1), 1–17.

Edwards, B., Hofmeyr, S., & Forrest, S. (2016). Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity*, *2*(1), 3–14.

Eling, M. (2018). Cyber risk and cyber risk insurance: Status quo and future. *Research. The Geneva Papers on Risk and Insurance: Issues and Practice*, *43*(2), 175–179.

Eling, M., & Loperfido, N. (2017). Data breaches: Goodness of fit, pricing, and risk measurement. *Insurance: Mathematics and Economics*, *75*, 126–136.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, *17*(5), 474–491.

Eling, M., & Schnell, W. (2020). Capital requirements for cyber risk and cyber risk insurance: An analysis of solvency II, the US Risk-based capital standards, and the swiss solvency test. *North American Actuarial Journal*, *24*(3), 370–392.

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research*, *272*(3), 1109–1119.

Elliott, M. W. (2019). *Risk in an evolving world* (1st ed., pp. 1.23–1.27). The Institutes.

Eloff, J. H., Labuschagne, L., & Badenhorst, K. P. (1993). A comparative framework for risk analysis methods. *Computers & Security*, *12*(6), 597–603.

Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564–585.

Ettredge, M., & Richardson, V. (2002). Assessing the risk in e-commerce. In R.H. Sprague, Jr. (ed.), *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*. IEEE Computer Society Press: Los Alamitos, CA (USA).

Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V., Gordon, L. A., Wang, S. S., Schmit, J., Thomas, R., Elvedi, M., Maillart, T., Donavan, E., Dejung, S., Durand, E., Nutter, F., Scheffer, U., Arazi, G., Ohana, G., & Lin, H. (2019). Cyber risk research impeded by disciplinary barriers. *Science*, *366*(6469), 1066–1069.

Finne, T. (2000). Information systems risk management: key concepts and business processes. *Computers & Security*, *19*(3), 234–242.

Fitzgerald, K. (1989). The quest for intruder-proof computer systems. *IEEE Spectrum*, *26*(8), 22–26.

Flitner, A. (2010). *Foundations of risk management and insurance* (1st ed., pp. 4.7–4.36). The Institutes.

Fried, L. (1994). Information security and new technology Potential Threats and Solutions. *Information System Management*, *11*(3), 57–63.

Frosdick, S. (1997). The techniques of risk analysis are insufficient in themselves. *Disaster Prevention and Management*, *6*(3), 165–177.

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, *40*(1), 183–199.

Garg, A., Curtis, J., & Halper, H. (2003). The financial impact of IT security breaches: What do investors think? *Information Systems Security*, *12*(1), 22–33.

Garg, P. (2020). Cybersecurity breaches and cash holdings: Spillover effect. *Financial Management*, *49*(2), 503–519.

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*, *13*(1), 61–83.

Gerber, M., & Von Solms, R. (2001). Special features: From risk analysis to security requirements. *Computers and Security*, *20*(7), 577–584.

Gerber, M., & Von Solms, R. (2005). Management of risk in the information age, *Computers & Security* (24, pp. 16–30.1.

Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J., & Linkov, I. (2017). Resilience of cyber systems with over- and underregulation. *Risk Analysis*, *37*(9), 1644–1651.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, *5*(4), 438–457.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81–85.

He, C. Z., Frost, T., & Pinsker, R. E. (2020). The impact of reported cybersecurity breaches on firm innovation. *Journal of Information Systems*, *34*(2), 187–209.

Henrie, M. (2013). Cyber security risk management in the SCADA critical infrastructure environment. *Engineering Management Journal*, *25*(2), 38–45.

Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems*, *30*(3), 79–98.

Hiscox (2020). Hiscox Cyber Readiness Report 2020 (online). https://www.hiscox.com/sites/default/files/content/documents/2020-Hiscox-Cyber-Readiness-Report_USA.pdf. Accessed on Nov 05, 2020.

Hoar, S. (2005). Trends in cybercrime: The dark side of the internet. *Westlaw*, *20*(4), 1–13.

Hoffer, J. A., & Straub Jr, D. W. (1989). The 9 to 5 underground: are you policing computer crimes? *MIT Sloan Management Review*, *30*(4), 35.

Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations*. Sage publications.

Holling, C. S. (1996). Engineering resilience versus ecological resilience. Engineering within ecological constraints. *National Academy of Sciences*, *31*(1996), 32.

Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review*, *6*(2), 97–121.

Howard, J. D., & Longstaff, T. A. (1998). A common language for computer security incidents (No. SAND98-8667). Sandia National Labs., Albuquerque, NM (US); Sandia National Labs., Livermore, CA (USA).

Hurst, W., Merabti, M., & Fergus, P. (2014, May). Big data analysis techniques for cyber-threat detection in critical infrastructures. In *Proceedings of the 2014 28th International Conference on Advanced Information Networking and Applications Workshops* (pp. 916–921). IEEE.

IBM Ponemon (2020). Cost of a data breach report 2020 (online). https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf. Accessed on Nov 05, 2020.

Imboden, T. R., Phillips, J. N., Seib, J. D., & Fiorentino, S. R. (2013). How are nonprofit organizations influenced to create and adopt information security policies? *Issues in Information Systems*, *14*(2), 166–173.

Information Security Forum (2019). Threat Horizon 2019: Disruption. Distortion. Deterioration. Information Security Forum (online). https://www.securityforum.org/research/threat-horizon-2019/. Accessed on Oct 28, 2020.

Insua, D. R., Couce-Vieira, A., Rubio, J. A., Pieters, W., Labunets, K., & G. Rasines, D. (2019). An adversarial risk analysis framework for cybersecurity. *Risk Analysis*, https://doi.org/10.1111/risa.13331

Iyer, S. R., Simkins, B. J., & Wang, H. (2020). Cyberattacks and impact on bond valuation. *Finance Research Letters*, *33*, 101215.

Jacobs, J., Romanosky, S., Adjerid, I., & Baker, W. (2020). Improving vulnerability remediation through better exploit prediction. *Journal of Cybersecurity*, *6*(1):tyaa015. https://doi.org/10.1093/cybsec/tyaa015

Jacobs, N., Hossain-McKenzie, S., & Vugrin, E. (2018, August). Measurement and analysis of cyber resilience for control systems: An illustrative example. In *2018 Resilience Week (RWS)* (pp. 38–46). IEEE.

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, *82*(2), 85–105.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*.

Kelly, S., Leverett, E., Oughton, E. J., Copic, J., Thacker, S., Pant, R., & Hall, J. W. (2016). Integrated infrastructure: Cyber resiliency in society, mapping the consequences of an interconnected digital economy. *Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge*.

Ko, M., & Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology Management*, *17*(2), 13–22.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *arXiv preprint arXiv*, *2006*, 11929.

Lambert, J. H., Keisler, J. M., Wheeler, W. E., Collier, Z. A., & Linkov, I. (2013). Multiscale approach to the security of hardware supply chains for energy systems. *Environment Systems and Decisions*, *33*(3), 326–334.

Lee, A. V., Vargo, J., & Seville, E. (2013). Developing a tool to measure and compare organizations' resilience. *Natural hazards review*, *14*(1), 29–41.

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. *Financial Review*, *53*(2), 413–455.

Lilli, E. (2021). Redefining deterrence in cyberspace: Private sector contribution to national strategies of cyber deterrence. *Contemporary Security Policy*, 1–26.

Lin, Z., Sapp, T. R., Ulmer, J. R., & Parsa, R. (2020). Insider trading ahead of cyber breach announcements. *Journal of Financial Markets*, *50*, 100527.

Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., Lambert, J. H., Levermann, A., Montreuil, B., Nathwani, J., Renn, O., Scharte, B., Scheffler, A., Schreurs, M., Thiel-Clemen, T., & Nyer, R. (2014). Changing the resilience paradigm. *Nature Climate Change*, *4*(6), 407–409.

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., Flynn, S. E., & Seager, T. P. (2013a). Measurable resilience for actionable policy. *Environmental Science & Technology*, *47*(18), 10108–10110.

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013b). Resilience metrics for cyber systems. *Environment Systems and Decisions*, *33*(4), 471–476.

Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview, *Cyber Resilience of Systems and Networks* (pp. 1–25). Springer.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly*, *16*, 173–186.

Lukasik, S. (2010). Why the ARPANET was built. *IEEE Annals of the History of Computing*, *33*(3), 4–21.

Madnick, S. E. (1978). Management policies and procedures needed for effective computer security. *Sloan Management Review*, *20*(1), 61–74.

Maillart, T., & Sornette, D. (2010). Heavy-tailed distribution of cyber-risks. *The European Physical Journal B*, *75*(3), 357–364.

Makridis, C., & Dean, B. (2018). Measuring the economic effects of data breaches on firm outcomes: Challenges and opportunities. *Journal of Economic and Social Measurement*, *43*(1-2), 59–83.

Malhotra, A., & Kubowicz Malhotra, C. (2011). Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research*, *14*(1), 44–59.

Marotta, A., & McShane, M. (2018). Integrating a proactive technique into a holistic cyber risk management approach. *Risk Management and Insurance Review*, *21*(3), 435–452.

Mazzoccoli, A., & Naldi, M. (2020). Robustness of optimal investment decisions in mixed insurance/investment cyber risk management. *Risk Analysis*, *40*(3), 550–564.

McAfee, J., & Haynes, C. (1989). Computer viruses, worms, data diddlers, killer programs, and other threats to your system: what they are, how they work, and how to defend your PC, Mac or mainframe (No. BOOK). St. Martin's Press.

McShane, M. (2018). Enterprise risk management: History and a design science proposal. *The Journal of Risk Finance*, *19*(2), 137–153. https://doi.org/10.1108/JRF-03-2017-0048

McShane, M., Nair, A., & Rustambekov, E. (2011). Does enterprise risk management increase firm value? *Journal of Accounting, Auditing, and Finance*, *26*(4), 641–658. https://doi.org/10.1177/0148558X11409160

McShane, M., & Nguyen, T. (2020). Time varying effects of cyberattacks on firm value. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *45*(4), 580–615. https://doi.org/10.1057/s41288-020-00170-x

Mikhed, V., & Vogan, M. (2018). How data breaches affect consumer credit. *Journal of Banking & Finance*, *88*, 192–207.

Miller, H., & Griffy-Brown, C. (2018). Developing a framework and methodology for assessing cyber risk for business leaders. *Journal of Applied Business & Economics*, *20*, 3.

Modi, S. B., Wiles, M. A., & Mishra, S. (2015). Shareholder value implications of service failures in triads: The case of customer information security breaches. *Journal of Operations Management*, *35*, 21–39.

Morse, E. A., Raval, V., Wingender Jr, J. R. (2011). Market price effects of data security breaches. *Information Security Journal: A Global Perspective*, *20*(6), 263–273.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, *56*, 11–26.

Murciano-Goroff, R. (2019). Do Data Breach Disclosure Laws Increase Firms' Investment in Securing Their Digital Infrastructure? In *Workshop on the Economics of Information Security*.

Nair, A., Rustambekov, E., McShane, M., & Fainshmidt, S. (2014). Enterprise risk management as a dynamic capability: A test of its effectiveness during a crisis. *Managerial and Decision Economics*, *35*(8), 555–566. https://doi.org/10.1002/mde.2641

Oracle.com (2020). The Oracle and KPMG Cloud Threat Report 2020. Oracle (online). https://www.oracle.com/cloud/cloud-threat-report.html. Accessed on Oct 28, 2020.

Orman, H. (2003). The Morris worm: A fifteen-year perspective. *IEEE Security & Privacy*, *1*(5), 35–43.

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security*, *88*, 101608. https://doi.org/10.1016/j.cose.2019.101608

Park, J., Seager, T. P., Rao, P. S. C., Convertino, M., & Linkov, I. (2013). Integrating risk and resilience approaches to catastrophe management in engineering systems. *Risk Analysis*, *33*(3), 356–367.

Parker, D. B. (1972). Computer-Related Crime and Data Security. SRI International Long Range Planning Service Division, SRI International.

Parker, D. B. (2007). The dark side of computing: SRI International and the study of computer crime. *IEEE Annals of the History of Computing*, *29*(1), 3–15.

Porta, R. L., Lopez-de-Silanes, F., Shleifer, A., & Vishny, R. W. (1998). Law and finance. *Journal of Political Economy*, *106*(6), 1113–1155.

Poyraz, O. I., Canan, M., McShane, M., Pinto, C. A., & Cotter, T. S. (2020). Cyber assets at risk: Monetary impact of US personally identifiable information mega data breaches. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *45*(4), 616–638. https://doi.org/10.1057/s41288-020-00185-4

Rainer Jr, R. K., Snyder, C. A., & Carr, H. H. (1991). Risk analysis for information technology. *Journal of Management Information Systems*, *8*(1), 129–147.

Ramirez, R., & Choucri, N. (2016). Improving interdisciplinary communication with standardized cyber security terminology: A literature review. *IEEE Access*, *4*, 2216–2243.

Roberts, L. (1988). The Arpanet and computer networks, *A history of personal workstations* (pp. 141–172). ACM Digital Library.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121–135.

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, *5*(1), tyz002.

Romanosky, S., & Goldman, Z. (2017). Understanding cyber collateral damage. *Journal of National Law Security and Policy*, *9*(2), 233–257.

Roy, P. P. (2020, February). A high-level comparison between the NIST cyber security framework and the ISO 27001 Information Security Standard. In *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)* (pp. 1-3). IEEE.

Ruffle, S. J., Bowman, G., Caccioli, F., Coburn, A. W., Kelly, S., Leslie, B., & Ralph, D. (2014). Stress test scenario: Sybil logic bomb cyber catastrophe. *Cambridge Risk Framework Service Centre for Risk Studies. University of Cambridge*.

Scala, N. M., Reilly, A. C., Goethals, P. L., & Cukier, M. (2019). Risk and the five hard problems of cybersecurity. *Risk Analysis*, *39*(10), 2119–2126.

Schatz, D., & Bashroush, R. (2017). Economic valuation for information security investment: A systematic literature review. *Information Systems Frontiers*, *19*(5), 1205–1228.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), 53–74.

Sentuna, A., Alsadoon, A., Prasad, P. W. C., Saadeh, M., & Alsadoon, O. H. (2020). A novel enhanced naïve bayes posterior probability (ENBPP) using machine learning: Cyber threat analysis. *Neural Processing Letters*, 1–33.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, *57*, 14–30.

Shankar, K. S. (1977). Special feature the total computer security problem: An oveview. *Computer*, *10*(6), 50–73.

Shetty, S., McShane, M., Zhang, L., Kesan, J. P., Kamhoua, C. A., Kwiat, K., & Njilla, L. L. (2018). Reducing informational disadvantages to improve cyber risk management. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *43*(2), 224–238.

Siegel, C. A., Sagalow, T. R., & Serritella, P. (2002). Cyber-risk management: Technical and insurance controls for enterprise-level security. *Information Systems Security*, *11*(4), 33–49.

Siponen, M., & Willison, R. (2007). A critical assessment of IS security research between 1990–2004, In Proceedings of the 15th European Conference on Information Systems St. Gallen, Switzerland (pp. 1551–1559).

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *38*(1), 60–80.

von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Starr, R., Newfrock, J., & Delurey, M. (2003). Enterprise resilience: managing risk in the networked economy. *Strategy and Business*, *30*, 70–79.

Stine, K., Quinn, S., Witte, G., Scarfone, K., & Gardner, R. (2020). Integrating Cybersecurity and Enterprise Risk Management (ERM). (No. NIST Internal or Interagency Report (NISTIR) 8286 (Draft)). National Institute of Standards and Technology.

Straub Jr, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255–276.

Straub, D. W., & Hoffer, J. A. (1987). Computer abuse and computer security: An empirical study of contemporary information security systems. IRMIS (Institute for Research on the Management of Information Systems, Indiana University School of Business, Bloomington, IN 47405), Working Paper W, 801, 1987.

Stubley, D. (2013). What is cyber security? (online). https://www.7elements.co.uk/resources/blog/what-is-cyber-security/. Accessed on Nov 05, 2020.

Valentine, E. L. (2016). Enterprise technology governance: New information and technology core competencies for boards of directors (Doctoral dissertation, Queensland University of Technology).

Wang, H. E., Wang, Q. E., & Wu, W. (2020). Short Selling Surrounding Data Breaches. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3554487

Weill, P., & Ross, J. W. (2004). *IT governance: how top performers manage IT decision rights for superior results*. Harvard Business School Press.

Wheatley, S., Maillart, T., & Sornette, D. (2016). The extreme risk of personal data breaches and the erosion of privacy. *The European Physical Journal B*, *89*(1), 1–12.

World Economic Forum (2020). The global risks report 2020 (online). https://www.weforum.org/reports/the-global-risks-report-2020. Accessed on Nov 05, 2020.

Wrede, D., Stegen, T., & von der Schulenburg, J. M. G. (2020). Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *45*(4), 657–689.

Xu, H., Guo, aS., Haislip, J. Z., & Pinsker, R. E. (2019). Earnings management in firms with data security breaches. *Journal of Information Systems*, *33*(3), 267–284.

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, *26*(1), 60–77.

Yen, J. C., Lim, J. H., Wang, T., & Hsu, C. (2018). The impact of audit firms' characteristics on audit fees following information security breaches. *Journal of Accounting and Public Policy*, *37*(6), 489–507.

Young, D., Lopez Jr, J., Rice, M., Ramsey, B., & McTasney, R. (2016). A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*, *14*, 43–57.

Zeller, G., & Scherer, M. A. (2020). A comprehensive model for cyber risk based on marked point processes and its application to insurance. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3668228

Öğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. *Risk Analysis: An International Journal*, *31*(3), 497–512.

How to cite this article: Eling, M., McShane, M., & Nguyen, T. Cyber risk management: History and future research directions. *Risk Manag Insur Rev*. 2021;24: 93–125. https://doi.org/10.1111/rmir.12169