Received: 1 February 2022 | Accepted: 1 March 2022

DOI: 10.1111/poms.13859

SPECIAL ISSUE ARTICLE

Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions

Subodha Kumar[1] | **Rakesh R. Mallipeddi**[2]

[1]Fox School of Business, Temple University, Philadelphia, Pennsylvania, USA

[2]Fisher College of Business, The Ohio State University, Columbus, Ohio, USA

Correspondence
Rakesh R. Mallipeddi, Fisher College of Business, The Ohio State University, 618 Fisher Hall, Columbus, OH 43210, USA.
Email: mallipeddi.1@osu.edu

Handling Editor: Christopher S. Tang

Abstract

The new age economy is primarily driven by Industry 4.0 and Industry 5.0, which facilitate smartification of organizations by helping them integrate and automate decision making. Recent advances in information and communication technologies, such as the cloud, big data, Internet of things, and artificial intelligence and nanotechnology, have accelerated the adoption of Industry 4.0 and Industry 5.0. Because of these advancements, organizations are now facing new challenges in the form of cybersecurity risks that are partly caused by these technologies. In recent years, there has been a spike in the number of cyberattacks, and organizations are taking steps to minimize the impacts of these attacks. To address this critical issue, in this article, we discuss possible future research directions that production and operations management (POM) researchers can undertake to help organizations, supply chains, and governments develop robust strategies for reducing the number of attacks and their repercussions. In particular, we identify several avenues for future research in the following domains of POM: (1) global operations strategy, (2) healthcare operations management, (3) public policy, (4) management of technology, (5) supply chain management, and (6) disruptive technologies. Research on the topic of cybersecurity is not only an opportunity for operations management researchers but also critical for industry and society to overcome the challenges of cybersecurity risks.

KEYWORDS

cybersecurity, Industry 4.0, Industry 5.0, information and communication technologies, production and operations management

1 | INTRODUCTION

Industry 4.0 and Industry 5.0 technologies are transforming how organizations operate. Industry 4.0 refers to the "*smartification*" of organizations relying on new information and communication technology (ICT) devices and systems that facilitate design of smart products and smart factories (Schwab, 2017). ICT devices such as Internet of things (IoT) sensors enable machines to communicate with other machines and components in the production line and make necessary decisions autonomously. In addition, recent advances in increased computing speed enabled by cloud computing, big data analytics tools, artificial intelligence, and nanotechnology have driven the growth of newer and more affordable devices and systems that organizations can leverage to create smart industries. Industry 5.0 complements Industry 4.0 technologies by enabling collaboration between humans and Industry 4.0 technologies for sustainable, human-centric operations, and mass customizable manufacturing (European Commission, 2021).

Organizations are increasingly relying on Industry 4.0 and Industry 5.0 technologies to improve their operational efficiencies, supply chain coordination and responsiveness, quality, and customer experience (Lydon, 2019). Indeed, organizations are taking steps to leverage the benefits of these technologies. A recent survey conducted by Deloitte found that over 90% of 361 executives across 11 countries believe that adapting their process for Industry 4.0 is their organization's top strategic objective (Hanley, 2018). Apart from organizations, governments have started to take steps to increase investments in ICT systems related to Industry 4.0 and Industry 5.0. In 2020, the U.S. government announced a

Accepted by Christopher S. Tang, after two revisions.

plan to spend $1 billion toward research on newer ICT systems (Hockett, 2020). This trend is global and not limited to a few countries (PwC, 2019). For instance, the "*Make in India*" initiative by the Government of India is aimed toward leveraging ICT systems to modernize its industry and infrastructure (Mittal, 2021). Likewise, China's "*Made in China* 2025" is a push to embrace advanced ICT systems (Buntz, 2019).

With increased investments in Industry 4.0 and Industry 5.0 across the globe, there have been calls for research in operations management (OM) and supply chain management (SCM) (e.g., Kumar et al., 2018; Olsen & Tomlin, 2020). Answering this call for research, recent studies have examined how cloud (Li & Kumar, 2018), IoT (Choi et al., 2021), big data analytics (Kumar, 2015; Kumar & Qiu, 2022; Mallipeddi et al., 2021, 2022), and artificial intelligence (Kumar et al., 2019) create value for organizations. While the advantages of smartification of industries are multifold, as discussed in some of the recent papers published in the *Production and Operations Management* (POM) Journal (e.g., Choi et al., 2018; Feng & Shanthikumar, 2018; Guha & Kumar, 2018; Kumar et al., 2018), the extensive reliance on ICT also presents significant threats to organizations and their supply chains. More specifically, ICT systems are vulnerable to attacks on their communication networks, which allows intruders to halt operations, steal data, and alter outcomes that subsequently cause long-lasting damage (IBM, 2018). There has been a rapid upsurge in the number of cyberattacks in recent years with industry reports suggesting a 50% increase in the number of cyberattacks in 2021 compared to 2020 (Check Point Research, 2022). The costs of cyberattacks are significant as well. In 2021, 10 different cyberattacks costed organizations nearly $600 million (Insurance Journal, 2022). The growing number of cyberattacks has alarmed both industry and regulators, who have stressed the importance and necessity of cybersecurity.

Despite the increased risks related to cyberattacks and severe consequences of cyberattacks, research on factors that affect cybersecurity from the OM and SCM perspective is limited. Future research related to cybersecurity risks in the domain of POM, which encompasses several subareas, is necessary to help organizations develop strategies to mitigate the negative consequences of cyberattacks and to develop efficient response strategies to recover from cyberattacks. In this article, we offer our perspective on promising areas for future research related to cybersecurity risks within different subareas of POM. We also believe that research in this domain will be a guiding force for both industry and society to overcome the challenges that ICT systems present in the smart world.

The rest of the article is organized as follows. In Section 2, we explain the sources of different cyberattacks and present a few examples of cyberattacks on various industries. Next, we identify opportunities for cybersecurity research within six different subareas of POM in Section 3. We conclude in Section 4.

TABLE 1 Cyberattacks, sources, and examples

Type of cyberattack	Sources of attack	Recent examples
Vulnerability exploit	Software defects	A defect in Apache Log4j allowed unauthorized remote access to systems (Fowler, 2021).
Man-in-the-Middle (MitM)	Weak network security; network intrusion due to software defects	The 2017 MitM attack on Equifax led to data breach of 143 million customers and cost $700 million in settlements (Roy, 2017).
Distributed-denial-of-service (DDoS)	Intruders overwhelming the network; Software defects and/or weak network security	The 2021 attack overwhelmed Bandwidth Inc's network that cost the company several millions (Bandwidth, 2021).
Ransomware	Software defects and/or weak network security	Cyberattacks on Colonial pipeline (Sanger & Perlroth, 2021) and shippers (Kapadia, 2020).
Phishing	Network intrusion through firm's personnel	The 2013 cyberattack on Target cost $200 million to the company (Reuters, 2017).

2 | CYBERTHREATS

Firms are exposed to a variety of cyberthreats and the consequences of these threats are multifold including loss of proprietary information, damage to equipment, and severe financial costs (Worth, 2018). In this section, we first categorize and discuss different types of cyberattacks and possible sources of these attacks. Next, we briefly discuss a few examples of recent cyberattacks on firms and identify the type of cyberattack in each of these examples. In Table 1, we summarize the subsequent discussion on type of cyberattack, its possible sources, and recent examples of different types of cyberattacks.

2.1 | Sources of cyberattacks

The use of ICT systems provides cyberattackers with multiple access points to intrude into the systems. More specifically, the two main sources of intrusion are (1) software defects and (2) networked systems, which we elaborate below.

2.1.1 | Software defects

ICT devices are run by software, and they are often released into the market with defects (although not intentionally). These defects are identified by either external (e.g., users of the products) or internal (e.g., firms' software employees) resources after the product is rolled out into the market (Sen et al., 2020). For example, a software defect led to Tesla recalling 11,704 cars in 2021 (Fernandez, 2021). The issue of software bugs or defects is in fact a common problem in the industry with billions of new defects introduced each year, and they continue to be discovered over the lifetime of the software that power different ICT devices. The ratio of number of defects to lines of codes is around 1 to 35 on average (Anderson, 2001; Schryen, 2009), and it is estimated that more than 100 billion lines of codes are released to the market annually (Morgan, 2017)—implying billions of defects each year.

The large number of defects being introduced into the market led to several instances of vulnerability exploits. In particular, *vulnerability exploit* refers to cyberattackers taking advantage of the defects in the software to intrude into an organization's devices or network. We summarize the discussion related to vulnerability exploits in the first row of Table 1.

2.1.2 | Networked systems

Recent advancements in ICT systems have led to networked organizations. More specifically, different business entities (both within an organization and across organizations) are increasingly connected to each other through ICT devices. This provides cyberattackers several avenues to intrude and exploit the security weakness of the networked system. A common form of network-based intrusion is the *Man-in-the-Middle* (also referred to as MitM) attack. This type of attack occurs when a cyberattacker gains access to the network connecting two different entities, which allows them to steal the information between these entities (Liu et al., 2020). *Distributed-denial-of-service* (also referred to as DDoS) is another type of cyberattack, where the intruder overwhelms an organization's network, causing the network to exceed its bandwidth (Liu et al., 2020).

It also important to note that these two sources of intrusion are not isolated. Rather, attackers may use weakness in one source to gain entry to the other source. More specifically, bugs in the software of network devices allow attackers to carry out MitM or DDoS attacks. Likewise, after gaining access to unsecured networks of organizations, attackers can install malware to block the functioning of ICT devices or steal proprietary data. We summarize the discussion related to MitM and DDoS attacks in the second and third rows of Table 1, respectively.

Ransomware attacks have become increasingly prevalent in recent times. For instance, a survey of 1100 cybersecurity professionals revealed that more than 80% of the respondents' organizations were victims of ransomware attacks in 2021 (Segal, 2022). In this type of attack, attackers block an organization's access to ICT systems (which they may have gained due to defects in the software and/or weak network security) and demand payment before restoring access (Tang & Whinston, 2020). In addition to utilizing the vulnerabilities in the software or networks, cyberattackers also exploit the weaknesses of employees to intrude into a network; for example, in phishing, attackers gain access to a system by tricking employees into clicking on fraudulent emails. *Phishing* has been reported to be the most common source of cyberattack, responsible for more than 80% of attacks (Cisco, 2021). We summarize the discussion related to ransomware and phishing in the fourth and fifth rows of Table 1, respectively. Next, we discuss a few examples of recent cyberattacks on different organizations.

2.2 | Cyberattacks on organizations

Over the last few years, a plethora of popular press reports have highlighted cyberattacks on organizations, their impacts, and responses by the organizations to recover from these cyberattacks. To highlight the significant impacts of cyberattacks, we provide a few instances of such attacks on major organizations and identify the type of each attack. The below examples are summarized in the last column of Table 1.

- **Vulnerabilities in** *Apache Log4j*: A defect in the Java-logging library Apache Log4j was detected in December 2021 with a vulnerability severity score of 10 out of 10. This vulnerability could have allowed unauthorized remote access to intruders. Indeed, several million attempts were made by cyberattackers to exploit the software defect and gain access to various organization's servers (Fowler, 2021).
- **MitM attack on** *Equifax*: The 2017 MitM attack on Equifax led to data breach of 143 million customers. In particular, an existing vulnerability allowed intruders to gain access to the data as its users accessed their accounts (i.e., usernames and passwords). The attack cost $700 million in settlements to Equifax (Roy, 2017).
- **DDoS attack on** *Bandwidth Inc*: Bandwidth, a voice over Internet Protocol services company, was subject to a DDoS attack, wherein the attackers overwhelmed Bandwidth Inc.'s network. This disrupted the services (e.g., calling and messaging) of Bandwidth. The 2021 attack cost the company several millions and disruptions lasted for several days (Bandwidth, 2021).
- **Ransomware attacks on industrial equipment**: Apart from targeting organizations to gain access to proprietary information, in recent years, intruders have also targeted industrial equipment causing "physical" damages to the manufacturing plants in addition to significant financial losses. A security report by the German government revealed that intruders targeted a German steel mill causing significant damages to industrial equipment (a blast furnace in a steel mill) (Cobb, 2015). More recently, in 2021, the cyberattack through network intrusion on Colonial Pipeline forced the company to shut down its operations, which led to fuel shortages and higher prices along the East Coast of the United States (Sanger &

Perlroth, 2021). While we provide a couple of instances of cybersecurity-related incidents, there are several such instances of breaches on industrial equipment worldwide as reported by Hemsley and Fisher (2018) in a study conducted by the U.S. Department of Energy National Laboratory.

- **Ransomware attacks on supply chains**: Recent reports suggest that major shippers have also been subject to ransomware attacks. Three major carriers were reported to have been targeted by cyberattackers between 2017 and 2020 (Kapadia, 2020). In all these cases, shipping operations were significantly affected, costing several million dollars. These operational glitches could potentially lead to further disruptions in the downstream.
- **Phishing attack on Target** : The 2013 cyberattack on Target Corporation exposed personal and credit card data of over 100 million customers and cost Target over $200 million (Reuters, 2017). The intruders gained access to Target's systems and installed malware software on majority of its point-of-sale systems. This type of attack is referred to as phishing, which we discuss in the next subsection. Following the attack, Target initiated short-term and long-term actions to remove the malware from its systems and to prevent future attacks on its systems.

The above examples provide a glimpse of how cyberattacks can affect organizations from different industries. In addition to economic damage, organizations should be wary of the damage to their reputations, such as negative perception from the customers, harsh media scrutiny, and damaged relationships with suppliers and customers (Worth, 2018).

3 | OPPORTUNITIES FOR RESEARCH IN POM

The number of digital transactions both within an organization and between organizations is increasing with the advent of Industry 4.0 and Industry 5.0 technologies. Consequently, the intruders also have a growing number of avenues to gain access to the network with a malicious intent. Therefore, it is imperative that organizations recognize the risks associated with adopting Industry 4.0 and Industry 5.0 and devise necessary strategies to mitigate these risks. We define cybersecurity risk as the extent to which supply chains are susceptible to disruptions as a direct consequence of a breach or a cyberattack.

In this article, we identify the research gaps in the following streams within POM that are closely related to current departments in the *POM Journal*: (1) global operations strategy, (2) healthcare operations management, (3) public policy, (4) management of technology, (5) supply chain management, and (6) disruptive technologies. We summarize the POM domains and subareas for cybersecurity–POM research in Figure 1. Below, we delve into each of these research domains to propose future research agenda.

3.1 | Global operations strategy

Over the last few decades, supply chains have become fragmented and globally dispersed with the total market for global sourcing reaching $92.5 billion (Statista, 2022). Firms are turning to suppliers from different parts of the world to meet their requirements in terms of quality, speed, and cost (Tsay et al., 2018). Previous literature has studied the factors that affect an organization's decision to source to other countries. Among many factors, product cost (including production, transportation, and inventory holding costs) (Allon & Van Mieghem, 2010; Tate et al., 2014), market-seeking decisions (i.e., organizations offshoring their operations, locating their operations to gain entry to foreign markets or be closer to the demand) (Ellram et al., 2013), tax benefits (Wang et al., 2016), and access to raw materials and technology (Fifarek et al., 2008) are most commonly studied in the literature. While global sourcing has several advantages including lower prices, higher quality, access to advanced technology, and shorter development time, there are several risks associated with it. Global sourcing is associated with economic challenges, political instability, and higher uncertainties, exposing supply chains to higher risks. The effects of these risks have been studied in the literature (e.g., see Cohen & Kouvelis, 2021; Dittman, 2005; Jung, 2020).

The advent of newer ICT systems is seen as an enabler of improved efficiency in global sourcing. For example, ICT such as IoT and cloud, facilitate networking of all the entities in a supply chain, allowing firms to track their supply chain in real time. Thus, in addition to the abovementioned risks, supply chains need to also deal with cybersecurity risks associated with the use of ICT. There have been several instances wherein a firm was targeted via a supply chain partner in a different country. For example, in 2021, the Taiwanese supplier Quanta was hit by a ransomware attack, which led to cyberattackers gaining access to Apple and setting a $50 million ransom for the proprietary information they acquired (Newman, 2021).

The above example highlights the critical need for firms to develop an overarching strategy to secure their global supply chains. A few research questions (summarized in Figure 2) that POM researchers can address in this domain include the following: **RQ 1.1**: *What are the impacts of heightened cybersecurity risks on global sourcing policies?* **RQ 1.2**: *How will the risks associated with cybersecurity affect a firm's procurement strategy related to number of suppliers and dealing with short-term and long-term suppliers?***RQ 1.3**: *How will the risks associated with cybersecurity affect a firm's offshoring and outsourcing decisions?* and **RQ 1.4**: *Are more diverse and geographically dispersed supply chains more prone to cyberattacks? What factors affect these decisions?* Answering these questions will help firms quantify the impacts of cybersecurity risks associated with global sourcing strategies and provide guidance on how to determine their sourcing strategies.

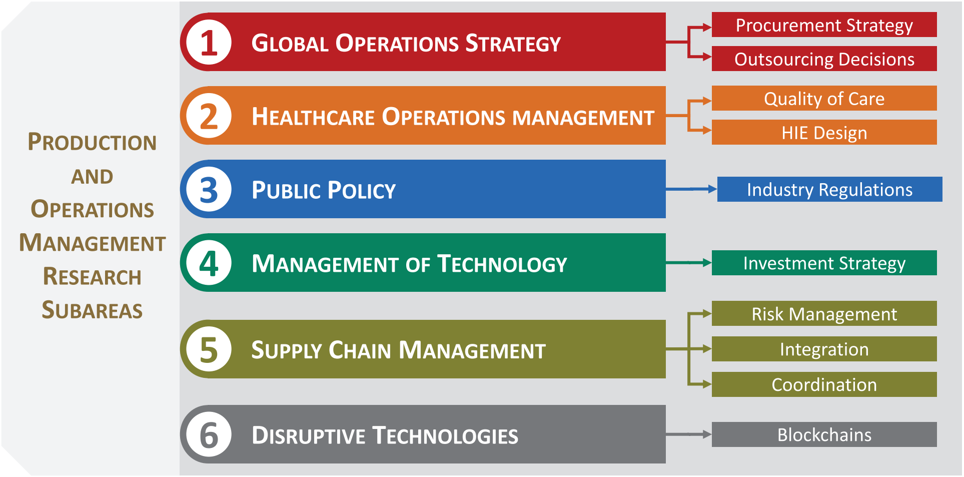
Production and Operations Management Research Subareas
1 Global Operations Strategy
Procurement Strategy
Outsourcing Decisions
2 Healthcare Operations Management
Quality of Care
HIE Design
3 Public Policy
Industry Regulations
4 Management of Technology
Investment Strategy
5 Supply Chain Management
Risk Management
Integration
Coordination
6 Disruptive Technologies
Blockchains

FIGURE 1 Summary of cybersecurity-POM research landscape [Color figure can be viewed at wileyonlinelibrary.com]

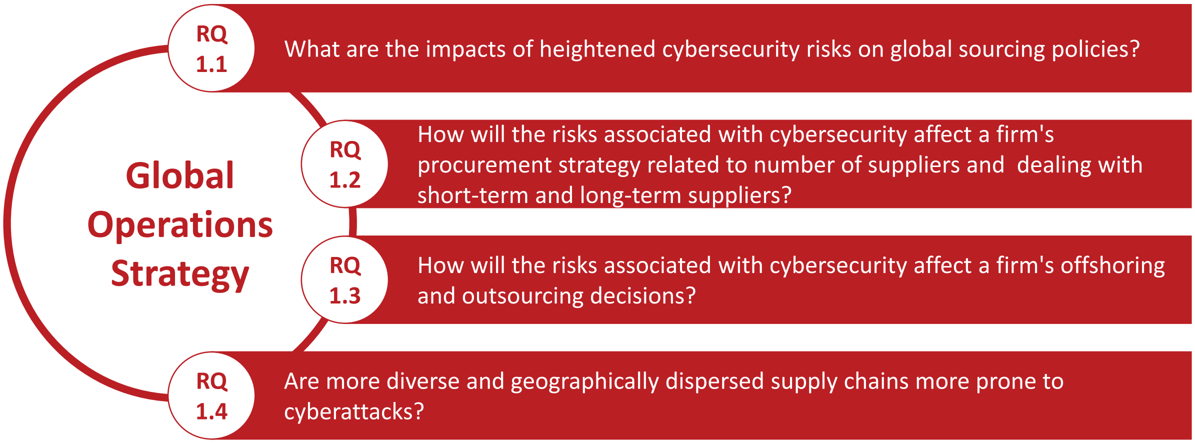
Global Operations Strategy
RQ 1.1
What are the impacts of heightened cybersecurity risks on global sourcing policies?
RQ 1.2
How will the risks associated with cybersecurity affect a firm's procurement strategy related to number of suppliers and dealing with short-term and long-term suppliers?
RQ 1.3
How will the risks associated with cybersecurity affect a firm's offshoring and outsourcing decisions?
RQ 1.4
Are more diverse and geographically dispersed supply chains more prone to cyberattacks?

FIGURE 2 Open-ended research questions on global operations strategy [Color figure can be viewed at wileyonlinelibrary.com]

3.2 | Healthcare operations management

The adoption of electronic healthcare records (EHRs) led to the aggregation of large volumes of data that healthcare providers and insurance companies can use to make relevant decisions. While EHRs allow sharing of information with an organization, recent efforts to improve coordination between different entities in the healthcare supply chain, including healthcare providers, diagnostic centers, insurance companies, and pharmacies, have led to the emergence of health information exchanges (HIEs). HIEs are often powered by cloud storage and computing technologies to handle large volumes of high dimensional data (Miller, 2020). HIEs allow electronic transfer of patient information from one supply entity to another, which is shown to improve quality and efficiency of care (Demirezen et al., 2016; Janakiraman et al., 2022). In addition to relying on cloud technology to collect and manage data, healthcare providers are turning to different Industry 4.0 and Industry 5.0 technologies, such as IoT and artificial intelligence, to collect data in order to improve patient care and provide telemedicine and virtual care.

While sharing of information among different entities can help improve healthcare outcomes, privacy of patient information is also of extreme importance in the healthcare industry. The Health Insurance Portability and Accountability Act (HIPAA) requires healthcare organizations to protect patient's medical records.[1] This rule requires organizations to apply certain measures to protect patient information and to obtain patients' permission prior to sharing information with other entities. Hence, protection of data is crucial for all entities in the healthcare supply chain.

The dependence on ICT poses a huge cybersecurity challenge to healthcare providers. Recent years have seen an increase in the number of cybersecurity incidents targeting clinics and hospitals by halting the operations of these providers. In 2020, an attack on University of Vermont (UVM) Medical Center cost nearly $50 million (Drees,

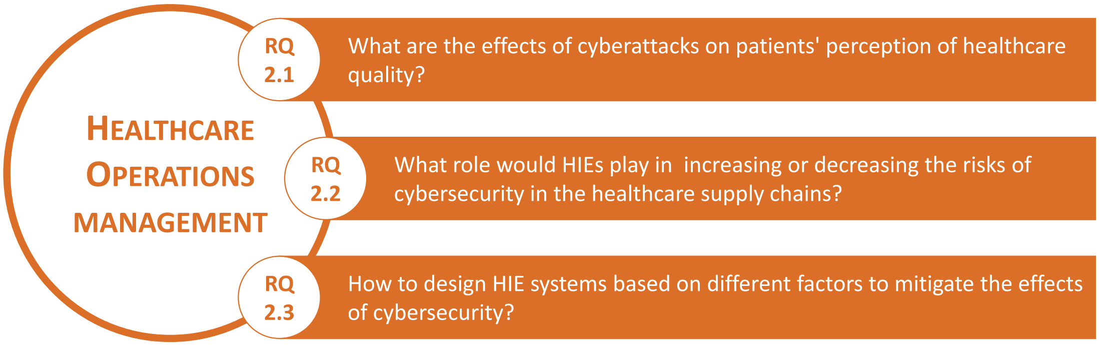
HEALTHCARE
OPERATIONS
MANAGEMENT
RQ 2.1
What are the effects of cyberattacks on patients' perception of healthcare quality?
RQ 2.2
What role would HIEs play in increasing or decreasing the risks of cybersecurity in the healthcare supply chains?
RQ 2.3
How to design HIE systems based on different factors to mitigate the effects of cybersecurity?

FIGURE 3 Open-ended research questions on healthcare operations management [Color figure can be viewed at wileyonlinelibrary.com]

2021). Their chief information officer cautioned healthcare providers: *"If cybersecurity isn't one of your top two priorities, it needs to be"* (Weiner, 2021). The increasing number of cyberattacks on the healthcare providers raises several cybersecurity-related challenges for all the supply chain entities and HIEs to ensure proper safeguarding of information. Despite the importance of the problem, the research on the topic of cybersecurity in the healthcare industry is limited. POM researchers can take a lead in tackling these important issues and providing implementable solutions to mitigate cybersecurity risks in healthcare.

There are several interesting and important research avenues that POM researchers can undertake. First, **RQ 2.1**: *What are the effects of cyberattacks on patients' perception of healthcare quality?* More specifically, do patients' associate cybersecurity with healthcare quality. The findings of this study may highlight the importance of cybersecurity in the healthcare industry and help providers determine their cybersecurity investment levels. Another important research question in this domain is: **RQ 2.2**: *What role would HIEs play in increasing or decreasing the risks of cybersecurity in the healthcare supply chains?* and **RQ 2.3**: *How to design HIE systems based on different factors to mitigate the effects of cybersecurity?* While there are several benefits to HIEs, their sustainability is a widely debated topic (Demirezen et al., 2016). Furthermore, given the significant costs associated with cyberattacks, it is crucial for HIEs to incorporate cybersecurity risks when designing their systems. We summarize the above discussed research questions in Figure 3.

3.3 | Public policy

As a response to the increase in the number of incidents related to cybersecurity, several governments have taken (or are taking) actions to initiate stringent regulatory oversight to minimize the likelihood of cyberattacks and to mitigate the subsequent ramifications. For example, the U.S. government recognizes the significance of threats related to cybersecurity and considers cybersecurity as "*a critical element of the Department of Homeland Security's (DHS) mission, a top priority for the Biden-Harris Administration at all levels of government*."[2] In response, the U.S. government's Department of Defense actively identifies "high risk" supply chain sources, and creates a list of "do not buy" software products to minimize the risks of disruptions (Metzger, 2018). For example, the Department of Defense has prohibited the Pentagon, General Services Administration, and National Aeronautics and Space Administration (NASA) from using Kaspersky software (Marks, 2018). Similarly, in 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy released a new cybersecurity policy to mitigate the risks of cyberattacks and respond to cyberattacks.[3]

While prior POM research has examined the effects of policies of various industry regulators (such as the Food and Drug Administration), Joglekar et al. (2016) argue that future POM research is required not to only study the effects of policies on firms' operations, but also to understand the bidirectional interactions between various public policy and operational decisions. Given the number of cybersecurity incidents and the severe consequences of these incidents, it is crucial and necessary to design strong policies to reduce the number of incidents and improve recovery from cyberattacks. It is also important to understand the interactions between the policy and firms' operations, that is, how do these policies affect firms' optimal decisions?

In addition to government regulations, third-party certifications, such as ISO 9000, are often seen as a way to standardize processes for improved performance (Anderson et al., 1999). Prior research has consistently demonstrated the benefits of firms adopting ISO certifications (Corbett et al., 2005). Likewise, it may be interesting to determine whether third-party certifications can help firms improve their cybersecurity performance. The above discussion leads us to the following related research questions (summarized in Figure 4): **RQ 3.1**: *How can policy regulations improve a supply chain's cybersecurity?* **RQ 3.2**: *Will third-party certifications complement government regulations in reducing cybersecurity risks?* and **RQ 3.3**: *What factors affect how regulations increase or decrease supply chain risks associated with cybersecurity?* Assessing the viability of government policies and third-party certifications may help firms and governments alike to design better regulations to reduce cybersecurity risks.

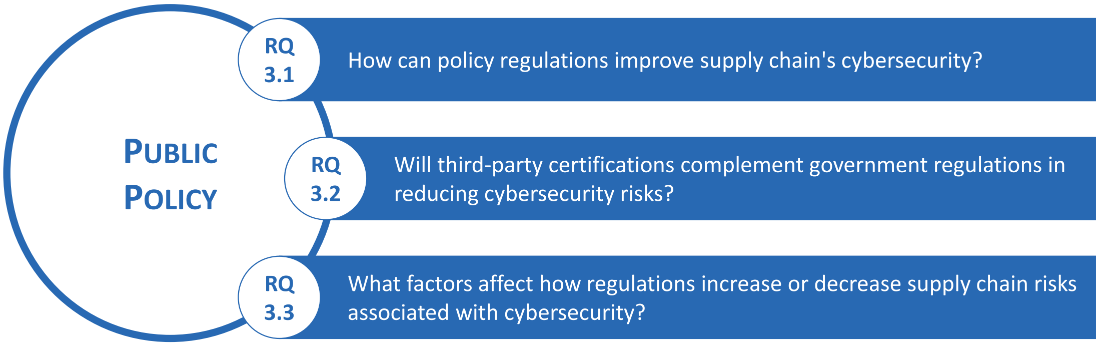
PUBLIC POLICY
RQ 3.1
How can policy regulations improve supply chain's cybersecurity?
RQ 3.2
Will third-party certifications complement government regulations in reducing cybersecurity risks?
RQ 3.3
What factors affect how regulations increase or decrease supply chain risks associated with cybersecurity?

FIGURE 4 Open-ended research questions on public policy [Color figure can be viewed at wileyonlinelibrary.com]

3.4 | Management of technology

The growing number of cyberattacks on organizations in the recent years has led to organizations increasing their spending on cybersecurity. Industry reports suggest that firms were expected to spend more than $124 billion in 2019 toward managing technology for prevention of cyberattacks (Gartner, 2018). As discussed earlier, ICT devices are not free of software bugs, which significantly increases the probability of a cyberattack. Thus, firms need to actively invest in managing their technologies and making strategic decisions on when to upgrade to newer versions. A stream of research on information systems and OM has examined firms' technology management strategies to effectively maintain existing technologies (i.e., find and fix vulnerabilities). In particular, the technology maintenance literature mainly deals with finding optimal policies to minimize the overall cost of maintenance or maximize net revenues (e.g., Arora et al., 2006; Ji et al., 2011; Kulkarni et al., 2009; Mallipeddi et al., 2019). Researchers have also examined the trade-offs between the cost of maintaining existing technology and replacing it with a newer version (e.g., Ji et al., 2011; Tan & Mookerjee, 2005).

Given that trade-offs of value creation and increased risk of cyberattacks, hybrid strategies (i.e., selective and partial adoption of ICT systems) may be an optimal strategy for firms. In a hybrid strategy, firms can strategically decide to upgrade only a fraction of existing equipment with ICT to limit the risks associated with them while leveraging Industry 4.0 and Industry 5.0. Future research is needed to analyze the feasibility of these hybrid strategies. Consequently, the POM domain can seek to answer the following research questions (summarized in Figure 5): **RQ 4.1**: *How much to rely on Industry* 4.0 *technologies?* **RQ 4.2**: *How can firms leverage Industry* 4.0 *technologies by balancing value creation and increased risk of cyberattacks?* Analyzing these questions may provide possible directions for managing of existing and new technology to prevent cyberattacks.

3.5 | Supply chain management

Anecdotal evidence suggests that a majority of cybersecurity breaches originate from supply chain partners. Not surprisingly, industry experts argue that "*supply chains present a weak link for cybersecurity*" (Duca, 2019). It is, therefore, crucial to understand factors that affect cybersecurity risks and strategies to mitigate the effects of these risks. Below, we present several exciting research directions in the following subareas within SCM: (1) supply chain risk management, (2) supply chain integration, and (3) supply chain coordination and information sharing.

3.5.1 | Supply chain risk management

Tang and Tomlin (2008) define supply chain risk management as "*the management of supply chain risks through coordination or collaboration among the supply chain partners so as to ensure profitability and continuity*." In recent years, there has been an increasing interest among supply chain researchers to study risk management. For example, Tang and Tomlin (2008) reviewed around 200 journal articles (published between 1964 and 2005) that studied mitigating various supply chain risks, while Ho et al. (2015) found a total of 224 journal articles published between 2003 and 2013. Research in this area has identified and quantified the impact of various sources of risk on a firm's performance (e.g., Anderson Jr et al., 2000; Kleindorfer & Saad, 2005; Sodhi, 2005; Sodhi et al., 2012). Yet, surprisingly, research that explicitly studies the risk management induced by cyberattacks on supply chain is quite limited. Below, we discuss the state of current research on the topic of supply chain risk management literature and identify possible future research directions on the topic of cybersecurity risk management in supply chain.

The supply chain literature on risk management has focused on strategies to alleviate the negative consequences of a disruption and recover from it. For example, Tang and Tomlin (2008) propose three mechanisms to reduce the impact of supply chain risks in the long, medium, and short term. These mechanisms are based on Lee's (2004) "*Triple-A*" principles: *alignment*, *adaptability*, and *agility*. To reduce risks in the long term, Tang and Tomlin (2008) argue that alignment of interests will increase trust between supply chain partners. Aligning supply chain interests include sharing of profits/costs, resources, and information among

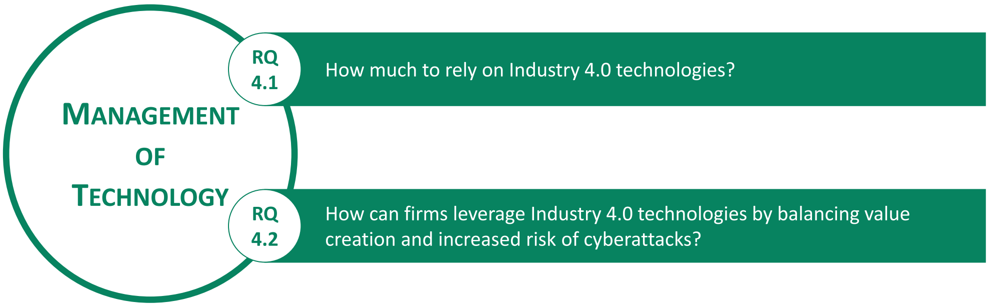
MANAGEMENT OF TECHNOLOGY
RQ 4.1
How much to rely on Industry 4.0 technologies?
RQ 4.2
How can firms leverage Industry 4.0 technologies by balancing value creation and increased risk of cyberattacks?

FIGURE 5 Open-ended research questions on management of technology [Color figure can be viewed at wileyonlinelibrary.com]

supply chain partners. Adaptive supply chains can recover from uncertainties due to changing market dynamics in the medium term. To reduce the impact of short-term risks, agile supply chains adopt strategies such as postponement, modular design, and flexible manufacturing systems.

In addition to the Triple-A strategies discussed earlier, another common strategy to effectively recover from an unlikely event is to create redundancies in the supply chain, for example, creating redundancies with multiple suppliers and multiple inventory locations. Sheffi (2001) analyzes strategies to manage supply chain risks with growing threat of international terrorism and argues that this strategy can minimize the adverse effects and in some cases create value. However, this increases the risk of a cyberattack, as it opens up more avenues for intruders to breach the system, and it remains uncertain whether strategies to handle supply chain disruption increase exposure to cybersecurity risks. Massimino et al. (2018) postulate that strategies designed to reduce the effects of supply chain disruption can decrease data confidentiality performance. A similar argument can be made that supply chain disruption strategies can decrease a firm's performance in the context of cybersecurity. Given this ambiguity, relevant research questions are: **RQ 5.1A**: *How will cybersecurity risks affect existing supply chain strategies to recover from a disruption?* and **RQ 5.1B**: *How to design the supply chain networks to recover from disruptions caused by a cyberattack?*

Another potential research direction is to consider a real options approach to buying cloud computing capacity. A real option gives a firm the right, but not the obligation, to buy additional capacity (or an asset) in the future at a predetermined price (Black & Scholes, 1973). OM and SCM scholars have taken real options approaches to manage their operations and hedge against uncertainty in capacity and prices of technologies and commodities (Lai et al., 2010; Ziedonis, 2007). Given the growing risk of cyberattacks, an important research question is: **RQ 5.1C**: *How to design and exercise option contracts to hedge against disruption in cloud services?* We summarize these research questions in Figure 6.

3.5.2 | Supply chain integration

The emergence of ICT devices has facilitated better integration of different entities within the supply chain. For example, the use of cloud technology allows seamless sharing of data between multiple supply chain partners. Similarly, IoT devices help supply chain partners to exchange information in real time, which can help supply chain partners in both upstream and downstream to coordinate the flow of materials and thus improve the efficiency. While previous POM research has consistently demonstrated the impact of supply chain integration on firm performance (e.g., Koufteros et al., 2001) and the role of Internet on integration (Johnson & Whang, 2002), the use of ICT devices for integration could also have severe negative consequences.

Integration of supply chains facilitated by Industry 4.0 and Industry 5.0 has increased the risks associated with cybersecurity. Given that intruders can gain access to the entire supply chain through any of the connected supply chain partners, various factors such as type of industry, firm size, level of supply chain integration, and level of Industry 4.0 and Industry 5.0 adoption can impact cybersecurity risk levels. Future empirical research can investigate the following questions:

RQ 5.2A: *What supply chain factors strengthen or diminish the consequences of cybersecurity breaches?* and **RQ 5.2B**: *How to design and integrate Industry* 4.0- *and Industry* 5.0-*enabled supply chains to reduce the likelihood of cyberattacks?*

It is also critical for firms to strategically determine the optimal life of their ICT systems. With increased risk of cybersecurity, firms need to coordinate with other supply chain partners to constantly upgrade their ICT to enhance the security of the entire supply chain. This leads us to the following questions: **RQ 5.2C**: *Is it beneficial for firms to maintain and handle supplier's ICT infrastructure?* **RQ 5.2D**: *How will centralizing ICT infrastructure through cloud technologies aggravate or mitigate the cybersecurity supply chain risks?* and **RQ 5.2E**: *How can firms utilize cloud to mitigate the risks arising from other Industry* 4.0 *and Industry* 5.0 *technologies?* We summarize these research questions in Figure 7.

3.5.3 | Supply chain coordination with information sharing

With the increasing complexity of supply chains, coordinating the activities of all supply chain partners is critical

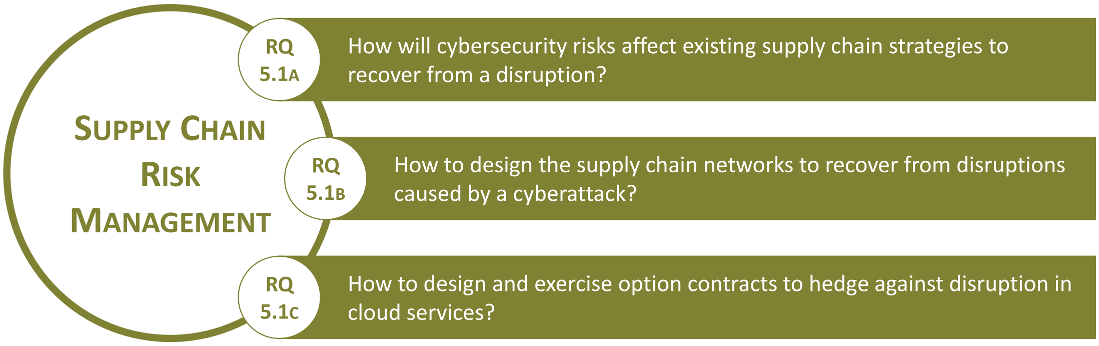
SUPPLY CHAIN RISK MANAGEMENT
RQ 5.1A
How will cybersecurity risks affect existing supply chain strategies to recover from a disruption?
RQ 5.1B
How to design the supply chain networks to recover from disruptions caused by a cyberattack?
RQ 5.1C
How to design and exercise option contracts to hedge against disruption in cloud services?

FIGURE 6 Open-ended research questions on risk management [Color figure can be viewed at wileyonlinelibrary.com]

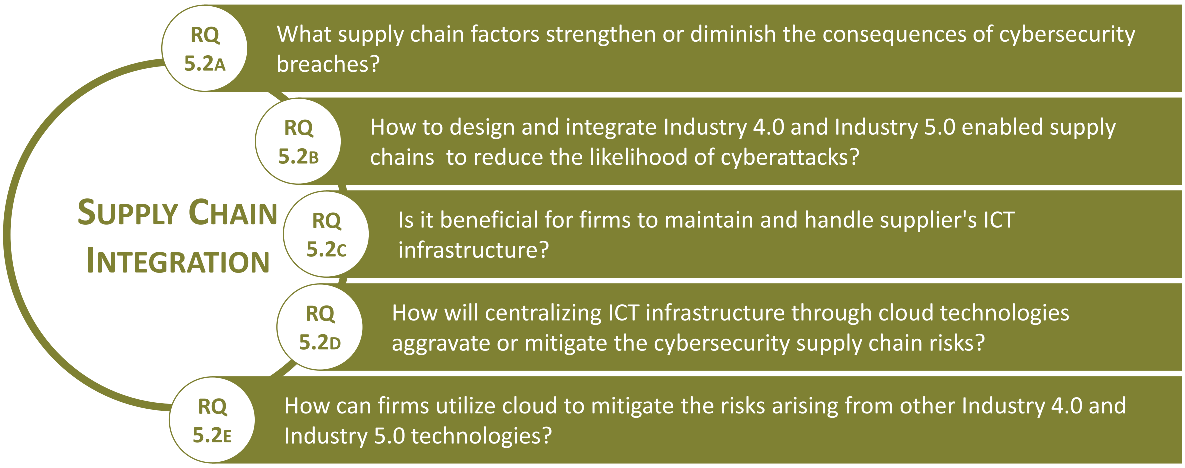
SUPPLY CHAIN INTEGRATION
RQ 5.2A
What supply chain factors strengthen or diminish the consequences of cybersecurity breaches?
RQ 5.2B
How to design and integrate Industry 4.0 and Industry 5.0 enabled supply chains to reduce the likelihood of cyberattacks?
RQ 5.2C
Is it beneficial for firms to maintain and handle supplier's ICT infrastructure?
RQ 5.2D
How will centralizing ICT infrastructure through cloud technologies aggravate or mitigate the cybersecurity supply chain risks?
RQ 5.2E
How can firms utilize cloud to mitigate the risks arising from other Industry 4.0 and Industry 5.0 technologies?

FIGURE 7 Open-ended research questions on integration [Color figure can be viewed at wileyonlinelibrary.com]

for supply chain performance. A broad base of operations and supply chain literature has consistently demonstrated the need to coordinate the actions of all the supply chain partners in order to optimize the performance (Boyaci & Gallego, 2004). Although there are several ways to achieve supply chain coordination, coordination achieved through information sharing is of primary relevance with emerging cybersecurity risks.

Information sharing between supply chain partners is vital for coordinating the activities of partners. A large body of literature has highlighted the benefits of information sharing (between the supply chain partners) and the value of information in improving firms' performances (e.g., Ahmad & Schroeder, 2001; Croson & Donohue, 2003; Delen et al., 2007; Whitaker et al., 2007). Literature has consistently demonstrated the value of downstream information (i.e., upstream members of the supply chain have access to downstream information) and upstream information (i.e., downstream members of the supply chain have access to upstream information) on supply chain performance (Chen, 2003).[4]

Chen (1998) find that having downstream information (i.e., information on demand of downstream partner) increases the performance of the entire supply chain by up to 9%. Gavirneni et al. (1999) study the value of different pieces of information and consistently find the significance of additional value of information. In particular, they find that information on a downstream partner's demand distribution and inventory policies reduces total costs of a supply chain by up to 90%, and the total costs further decrease by up to 35% if the downstream partner's day-to-day inventory levels are revealed. Cachon and Fisher (2000) find that the value of downstream information is greater for highly uncertain demand. Prior research has also demonstrated the importance of the value of upstream information on reducing lead times (Chen & Yu, 2005), increasing supplier capacity (Ketzenberg, 2009; van der Schouten et al., 1994), and increasing profits for retailers handling perishable products (Ketzenberg & Ferguson, 2008). On the empirical side, Zhou and Benton Jr (2007) demonstrate that information sharing is positively associated with supply chain practices and higher information quality is associated with better delivery performance. Furthermore, it is shown that delays in information sharing could affect supply chain performance (Chen, 1999). To sum up, the broad literature has shown the significance of information sharing on supply coordination and performance.

The increased use of ICT systems and the shift toward Industry 4.0 and Industry 5.0 have enhanced information

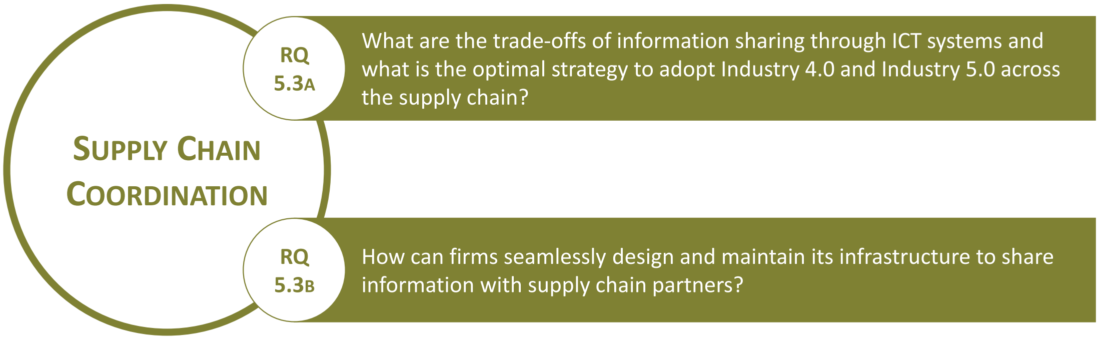
SUPPLY CHAIN COORDINATION
RQ 5.3A
What are the trade-offs of information sharing through ICT systems and what is the optimal strategy to adopt Industry 4.0 and Industry 5.0 across the supply chain?
RQ 5.3B
How can firms seamlessly design and maintain its infrastructure to share information with supply chain partners?

FIGURE 8 Open-ended research questions on coordination [Color figure can be viewed at wileyonlinelibrary.com]

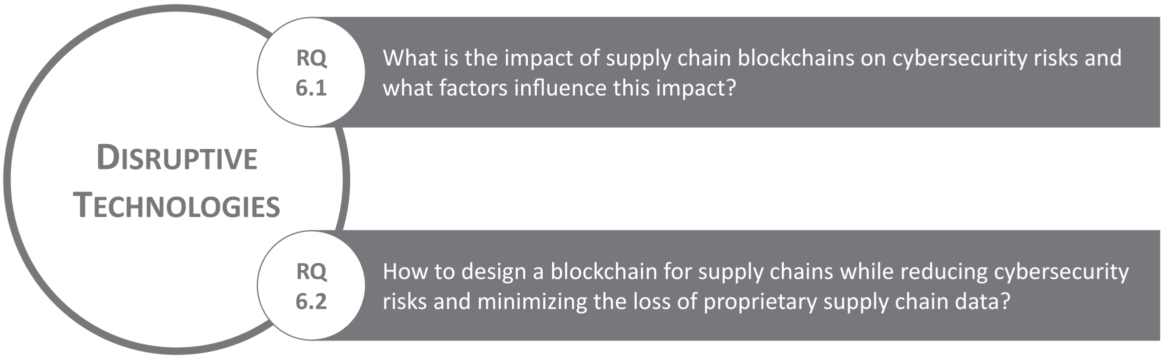
DISRUPTIVE TECHNOLOGIES
RQ 6.1
What is the impact of supply chain blockchains on cybersecurity risks and what factors influence this impact?
RQ 6.2
How to design a blockchain for supply chains while reducing cybersecurity risks and minimizing the loss of proprietary supply chain data?

FIGURE 9 Open-ended research questions on disruptive technologies and operations management

quality and completeness (Olsen & Tomlin, 2020; Saghafian et al., 2018). Although sharing of high quality and complete information in real time facilitates better coordination between partners, there are severe negative consequences of data confidentiality and data leakage due to cybersecurity risks. Thus, potential future research directions include the following:

RQ 5.3A: *What are the trade-offs of information sharing through ICT systems and what is the optimal strategy to adopt Industry* 4.0 *and Industry* 5.0 *across the supply chain?***RQ 5.3B**: *How can firms seamlessly design and maintain its infrastructure to share information with supply chain partners?* We summarize these research questions in Figure 8.

3.6 | Disruptive technologies

Blockchain is a shared ledger of transactions distributed across a network of computers (Wang et al., 2021). Blockchain technologies has attracted applications in several industries including finance, healthcare, and supply chains. In the context of supply chains, blockchains can improve visibility and traceability in supply chains (Hastig & Sodhi, 2020) and also reduce frauds (Pun et al., 2021). Several major firms have started to invest in blockchain technologies specifically to improve the efficiency of supply chains (Sodhi et al., 2022). A recent study finds that announcing the adoption of blockchain technology elicits a positive reaction to a firm's market value (Klöckner et al., 2021).

Since the record of transactions in the blockchain is permanent and copies of these transactions are distributed in a network of computers, experts argue that blockchains could reduce the risks associated with cybersecurity (Kanal, 2019). For instance, in a ransomware attack, intruders take control of a firm's database infrastructure and deny organizations access to data until a certain amount of ransom is paid to them. In case of blockchain, since the data are decentralized and distributed across a network of computers, it cannot be held for ransom as there are multiple copies of it in the network (McConville, 2017). However, it is important to note that cyberattacks are not entirely preventable in blockchain. A DDoS type of attack, which we discussed in Section 2.2, is considered a major treat to blockchains as the attack can increase the transaction times (Behnke, 2021).

Although blockchains have several benefits, such as reduced cybersecurity risks, experts point out several disadvantages as well, including high energy consumption, longer transaction time, high costs, and visibility of data to the entire network that can lead to loss of proprietary data. These unique trade-offs present several exciting research questions in this domain in the context of cybersecurity. **RQ 6.1**: *What is the impact of supply chain blockchains on cybersecurity risks and what factors influence this impact?* While it is argued that blockchain-based supply chains have better cybersecurity, a systematic study is needed to quantify this effect. Furthermore, future research is needed to understand how different factors can influence the relationship between blockchain and cybersecurity. Providing answers to these questions will help firms understand the impact of blockchains and subsequently make better decisions related to investment in this technology.

Given that most firms are still in the nascent stages of incorporating blockchains, future research is necessary to understand how to effectively design a blockchain in the context of a supply chain. Thus, the following research question is importance to firms (summarized in Figure 9): **RQ 6.2**: *How to design a blockchain for supply chains while reducing cybersecurity risks and minimizing the loss of proprietary supply chain data? How does the design change for different industries?*

4 CONCLUSION

While the extensive use of ICT systems has increased the efficiency of organizations and their supply chains, these systems pose several risks. In particular, organizations now face increased cybersecurity risks that cyberattackers seek to exploit, which in turn has severe repercussions. Organizations and governments alike are taking steps to reduce the number of cyberattacks while also seeking ways to mitigate the impact of these attacks and quickly recover from them. In this article, we identify various avenues for future research within different subareas of POM. These are not just an opportunity for academic researchers but also critical for industry and society to overcome the various challenges presented by cybersecurity risks.

ENDNOTES

[1] https://www.hhs.gov/hipaa/for-individuals/index.html

[2] https://www.dhs.gov/topics/cybersecurity

[3] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

[4] We refer readers to Chen (2003) for review of information sharing literature.

REFERENCES

Ahmad, S., & Schroeder, R. G. (2001). The impact of electronic data interchange on delivery performance. *Production and Operations Management*, *10*(1), 16–30.

Allon, G., & Van Mieghem, J. A. (2010). Global dual sourcing: Tailored base-surge allocation to near and offshore production. *Management Science*, *56*(1), 110–124.

Anderson, R. (2001). Why information security is hard-an economic perspective. In *Seventeenth annual computer security applications conference* (pp. 358–365). IEEE, New Orleans, LA, USA.

Anderson, S. W., Daly, J. D., & Johnson, M. F. (1999). Why firms seek ISO 9000 certification: Regulatory compliance or competitive advantage? *Production and Operations Management*, *8*(1), 28–43.

Anderson Jr, E. G., Fine, C. H., & Parker, G. G. (2000). Upstream volatility in the supply chain: The machine tool industry as a case study. *Production and Operations Management*, *9*(3), 239–261.

Arora, A., Caulkins, J. P., & Telang, R. (2006). Research note—Sell first, fix later: Impact of patching on software quality. *Management Science*, *52*(3), 465–471.

Bandwidth (2021). *Bandwidth issues statement on recent DDoS Attack*. https://www.prnewswire.com/news-releases/bandwidth-issues-statement-on-recent-ddos-attack-301393578.html

Behnke, R. (2021). *How blockchain DDoS attacks work*. https://halborn.com/how-blockchain-ddos-attacks-work/

Black, F., & Scholes, M. (1973). The pricing of options and corporate liabilities. *Journal of Political Economy*, *81*(3), 637–654.

Boyaci, T., & Gallego, G. (2004). Supply chain coordination in a market with customer service competition. *Production and Operations Management*, *13*(1), 3–22.

Buntz, B. (2019). *Made in China 2025 plan still controversial in the west*. https://www.iotworldtoday.com/2019/05/01/made-in-china-2025-plan-still-controversial-in-the-west/

Cachon, G. P., & Fisher, M. (2000). Supply chain inventory management and the value of shared information. *Management Science*, *46*(8), 1032–1048.

Check Point Research. (2022). *Cyber attacks increased 50% year over year*. https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/

Chen, F. (1998). Echelon reorder points, installation reorder points, and the value of centralized demand information. *Management Science*, *44*(12-part-2), S221–S234.

Chen, F. (1999). Decentralized supply chains subject to information delays. *Management Science*, *45*(8), 1076–1090.

Chen, F. (2003). Information sharing and supply chain coordination. *Handbooks in Operations Research and Management Science*, *11*, 341–421.

Chen, F., & Yu, B. (2005). Quantifying the value of leadtime information in a single-location inventory system. *Manufacturing & Service Operations Management*, *7*(2), 144–151.

Choi, T., Kumar, S., Yue, X., & Chan, H. (2021). Disruptive technologies and operations management in the Industry 4.0 era and beyond. *Production and Operations Management*, *31*(1), 9–31.

Choi, T., Wallace, S. W., & Wang, Y. (2018). Big data analytics in operations management. *Production and Operations Management*, *27*(10), 1868–1883.

Cisco. (2021). *Cyber security threat trends*. https://learn-umbrella.cisco.com/ebook-library/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

Cobb, P. (2015). *German steel mill meltdown: Rising stakes in the internet of things*. https://www.secureworldexpo.com/industry-news/supply-chain-attack-solar-winds-software

Cohen, M. A., & Kouvelis, P. (2021). Revisit of AAA excellence of global value chains: Robustness, resilience, and realignment. *Production and Operations Management*, *30*(3), 633–643.

Corbett, C. J., Montes-Sancho, M., & Kirsch, D. A. (2005). The financial impact of ISO 9000 certification in the United States: An empirical analysis. *Management Science*, *51*(7), 1046–1059.

Croson, R., & Donohue, K. (2003). Impact of POS data sharing on supply chain management: An experimental study. *Production and Operations Management*, *12*(1), 1–11.

Delen, D., Hardgrave, B. C., & Sharda, R. (2007). RFID for better supply-chain management through enhanced information visibility. *Production and Operations Management*, *16*(5), 613–624.

Demirezen, E. M., Kumar, S., & Sen, A. (2016). Sustainability of healthcare information exchanges: A game-theoretic approach. *Information Systems Research*, *27*(2), 240–258.

Dittman, J. P. (2005). Managing risk in the global supply chain. *Production and Operations Management*, *14*(1), 2.

Drees, J. (2021). *We just got caught up in a broader attack': UVM Medical Center details $50M ransomware strike*. https://tinyurl.com/43k4nuzr

Duca, S. (2019). *Supply chain remains the weakest link in cybersecurity*. https://www.supplychaindigital.com/technology/supply-chain-remains-weakest-link-cybersecurity

Ellram, L. M., Tate, W. L., & Petersen, K. J. (2013). Offshoring and reshoring: An update on the manufacturing location decision. *Journal of Supply Chain Management*, *49*(2), 14–22.

European Commission. (2021). *Industry 5.0: Human-centric, sustainable and resilient*. https://data.europa.eu/doi/10.2777/073781

Feng, Q., & Shanthikumar, J. G. (2018). How research in production and operations management may evolve in the era of big data. *Production and Operations Management*, *27*(9), 1670–1684.

Fernandez, R. (2021). *Over 11,000 Teslas just got recalled because of a dangerous software bug*. https://screenrant.com/teslas-recalled-self-driving-beta-vehicles-software-bug/

Fifarek, B. J., Veloso, F. M., & Davidson, C. I. (2008). Offshoring technology innovation: A case study of rare-earth technology. *Journal of Operations Management*, *26*(2), 222–238.

Fowler, B. (2021). *Log4j software bug: What you need to know*. https://tinyurl.com/ycktnjw5

Gartner. (2018). *Gartner forecasts worldwide information security spending to exceed $124 billion in 2019*. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

Gavirneni, S., Kapuscinski, R., & Tayur, S. (1999). Value of information in capacitated supply chains. *Management Science*, *45*(1), 16–24.

Guha, S., & Kumar, S. (2018). Emergence of big data research in operations management, information systems, and healthcare: Past contributions and future roadmap. *Production and Operations Management*, *27*(9), 1724–1735.

Hanley, T. (2018). *The Industry 4.0 paradox*. https://www2.deloitte.com/insights/us/en/focus/industry-4-0/challenges-on-path-to-digital-transformation/summary.html

Hastig, G. M., & Sodhi, M. S. (2020). Blockchain for supply chain traceability: Business requirements and critical success factors. *Production and Operations Management*, *29*(4), 935–954.

Hemsley, K. E., & Fisher, E. (2018). *History of industrial control system cyber incidents*. Tech. rep., Idaho National Lab.(INL), Idaho Falls, ID.

Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply chain risk management: A literature review. *International Journal of Production Research*, *53*(16), 5031–5069.

Hockett, M. (2020). *U.S. government announces $1 billion investment in researching Industry 4.0 technologies*. https://tinyurl.com/2p8zwbz7

IBM. (2018). *Learn about cyber attacks and how to defend against them*. https://www.ibm.com/services/business-continuity/cyber-attack

Insurance Journal. (2022). *10 cyber attacks in 2021 cost $600M with 40,000 businesses put at risk*. https://www.insurancejournal.com/news/international/2022/02/10/653554.htm

Janakiraman, R., Park, E., Demirezen, E., & Kumar, S. (2022). The effects of health information exchange access on healthcare quality and efficiency: An empirical investigation. *Management Science*, (forthcoming).

Ji, Y., Kumar, S., Mookerjee, V. S., Sethi, S. P., & Yeh, D. (2011). Optimal enhancement and lifetime of software systems: A control theoretic analysis. *Production and Operations Management*, *20*(6), 889–904.

Joglekar, N. R., Davies, J., & Anderson, E. G. (2016). The role of industry studies and public policies in production and operations management. *Production and Operations Management*, *25*(12), 1977–2001.

Johnson, M. E., & Whang, S. (2002). E-business and supply chain management: An overview and framework. *Production and Operations Management*, *11*(4), 413–423.

Jung, S. H. (2020). Offshore versus onshore sourcing: Quick response, random yield, and competition. *Production and Operations Management*, *29*(3), 750–766.

Kanal, E. (2019). *Could blockchain improve the cybersecurity of supply chains?* https://insights.sei.cmu.edu/blog/could-blockchain-improve-the-cybersecurity-of-supply-chains/

Kapadia, S. (2020). *3 years, 3 cyberattacks on major ocean carriers. How can shippers protect themselves?* https://www.supplychaindive.com/news/ocean-carrier-cybersecurity-maersk-msc-cosco/576754/

Ketzenberg, M. (2009). The value of information in a capacitated closed loop supply chain. *European Journal of Operational Research*, *198*(2), 491–503.

Ketzenberg, M., & Ferguson, M. E. (2008). Managing slow-moving perishables in the grocery industry. *Production and Operations Management*, *17*(5), 513–521.

Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and Operations Management*, *14*(1), 53–68.

Klöckner, M., Schmidt, C. G., & Wagner, S. M. (2021). When blockchain creates shareholder value: Empirical evidence from international firm announcements. *Production and Operations Management*, *31*(1), 46–64.

Koufteros, X., Vonderembse, M., & Doll, W. (2001). Concurrent engineering and its consequences. *Journal of Operations Management*, *19*(1), 97–115.

Kulkarni, V. G., Kumar, S., Mookerjee, V. S., & Sethi, S. P. (2009). Optimal allocation of effort to software maintenance: A queuing theory approach. *Production and Operations Management*, *18*(5), 506–515.

Kumar, N., Venugopal, D., Qiu, L., & Kumar, S. (2019). Detecting anomalous online reviewers: An unsupervised approach using mixture models. *Journal of Management Information Systems*, *36*(4), 1313–1346.

Kumar, S. (2015). *Optimization issues in web and mobile advertising: Past and future trends*. Springer.

Kumar, S., Mookerjee, V., & Shubham, A. (2018). Research in operations management and information systems interface. *Production and Operations Management*, *27*(11), 1893–1905.

Kumar, S., & Qiu, L. (2022). *Social media analytics and practical applications: The change to the competition landscape*. CRC Press.

Lai, G., Margot, F., & Secomandi, N. (2010). An approximate dynamic programming approach to benchmark practice-based heuristics for natural gas storage valuation. *Operations Research*, *58*(3), 564–582.

Lee, H. L. (2004). The Triple-A supply chain. *Harvard Business Review*, *82*(10), 102–113.

Li, B., & Kumar, S. (2018). Should you kill or embrace your competitor: Cloud service and competition strategy. *Production and Operations Management*, *27*(5), 822–838.

Liu, Z., Wang, Q., & Tang, Y. (2020). Design of a cosimulation platform with hardware-in-the-loop for cyber-attacks on cyber-physical power systems. *IEEE Access*, *8*, 95997–96005.

Lydon, B. (2019). *How Industry 4.0 and digitization improves manufacturing responsiveness, quality and efficiency*. https://tinyurl.com/5n8sdsmu

Mallipeddi, R., Demirezen, E., Kumar, S., & Gopal, R. (2019). *How much to open, how fast to fix and develop? Impacts of openness on software development and maintenance*. Working Paper. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3470713

Mallipeddi, R. R., Janakiraman, R., Kumar, S., & Gupta, S. (2021). The effects of social media content created by human brands on engagement: Evidence from Indian general election 2014. *Information Systems Research*, *32*(1), 212–237.

Mallipeddi, R. R., Kumar, S., Sriskandarajah, C., & Zhu, Y. (2022). A framework for analyzing influencer marketing in social networks: Selection and scheduling of influencers. *Management Science*, *68*(1), 75–104.

Marks, J. (2018). *Government's Kaspersky ban takes effect*. https://www.nextgov.com/cybersecurity/2018/07/governments-kaspersky-ban-takes-effect/149758/

Massimino, B., Gray, J. V., & Lan, Y. (2018). On the inattention to digital confidentiality in operations and supply chain research. *Production and Operations Management*, *27*(8), 1492–1515.

McConville, A. (2017). *Prevent ransomware attacks with blockchain*. https://www.ibm.com/blogs/cloud-archive/2017/05/blockchain-prevent-ransomware-attacks/

Metzger, R. (2018). *Why supply chain threats require a whole-of-government response*. https://www.federaltimes.com/opinions/2018/09/07/why-supply-chain-threats-require-a-whole-of-government-response/

Miller, G. (2020). *Three reasons COVID-19 is pushing health information exchanges to the cloud*. https://blog.cloudticity.com/three-reasons-covid19-pushing-health-information-exchanges-cloud

Mittal, S. (2021). *It's time for Industry 4.0*. https://www.thehindu.com/opinion/op-ed/its-time-for-industry-40/article36103800.ece

Morgan, S. (2017). *World will need to secure 111 billion lines of new software code in 2017*. https://www.csoonline.com/article/3151003/world-will-need-to-secure-111-billion-lines-of-new-software-code-in-2017.html

Newman, L. H. (2021). *Apple's ransomware mess is the future of online extortion*. https://www.wired.com/story/apple-ransomware-attack-quanta-computer/

Olsen, T. L., & Tomlin, B. (2020). Industry 4.0: Opportunities and challenges for operations management. *Manufacturing & Service Operations Management*, *22*(1), 113–122.

Pun, H., Swaminathan, J. M., & Hou, P. (2021). Blockchain adoption for combating deceptive counterfeits. *Production and Operations Management*, *30*(4), 864–882.

PwC. (2019). *Big investments with big impacts and rapid returns*. https://www.pwc.com/m1/en/publications/industry-40-survey/big-investments.html

Reuters. (2017). *Target pays millions to settle state data breach lawsuits*. https://fortune.com/2017/05/23/target-settlement-data-breach-lawsuits/

Roy, A. (2017). *Equifax to pay approx. %700 million in settlement of 2017 data breach charges*. https://www.appviewx.com/blogs/equifax-to-pay-approx-700-million-in-settlement-of-2017-data-breach-charges/

Saghafian, S., Tomlin, B., & Biller, S. (2018). *The internet of things and information fusion: Who talks to who?* HKS Working Paper 18-009.

Sanger, D., & Perlroth, N. (2021). *Pipeline attack yields urgent lessons about U.S. cybersecurity*. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html

Schryen, G. (2009). A comprehensive and comparative analysis of the patching behavior of open source and closed source software vendors. In *Proceedings of fifth international conference on IT security incident management and IT forensics*, Stuttgart, Germany (pp. 153–168). IEEE.

Schwab, K. (2017). *The fourth industrial revolution*. Currency.

Segal, E. (2022). *A majority of surveyed companies were hit by ransomware attacks in 2021 and paid ransom demands*. https://tinyurl.com/4rawmue8

Sen, R., Choobineh, J., & Kumar, S. (2020). Determinants of software vulnerability disclosure timing. *Production and Operations Management*, *29*(11), 2532–2552.

Sheffi, Y. (2001). Supply chain management under the threat of international terrorism. *The International Journal of Logistics Management*, *12*(2), 1–11.

Sodhi, M. S. (2005). Managing demand risk in tactical supply chain planning for a global consumer electronics company. *Production and Operations Management*, *14*(1), 69–79.

Sodhi, M. S., Seyedghorban, Z., Tahernejad, H., & Samson, D. (2022). Why emerging supply chain technologies initially disappoint: Blockchain, IoT, and AI. *Production and Operations Management*, *31*(6), 2517–2537.

Sodhi, M. S., Son, B., & Tang, C. S. (2012). Researchers' perspectives on supply chain risk management. *Production and Operations Management*, *21*(1), 1–13.

Statista. (2022). *Global market size of outsourced services from 2000 to 2019*. https://www.statista.com/statistics/189788/global-outsourcing-market-size/

Tan, Y., & Mookerjee, V. S. (2005). Comparing uniform and flexible policies for software maintenance and replacement. *IEEE Transactions on Software Engineering*, *31*(3), 238–255.

Tang, C., & Tomlin, B. (2008). The power of flexibility for mitigating supply chain risks. *International Journal of Production Economics*, *116*(1), 12–27.

Tang, Q., & Whinston, A. B. (2020). Do reputational sanctions deter negligence in information security management? A field quasi-experiment. *Production and Operations Management*, *29*(2), 410–427.

Tate, W. L., Ellram, L. M., Schoenherr, T., & Petersen, K. J. (2014). Global competitive conditions driving the manufacturing location decision. *Business Horizons*, *57*(3), 381–390.

Tsay, A. A., Gray, J. V., Noh, I. J., & Mahoney, J. T. (2018). A review of production and operations management research on outsourcing in supply chains: Implications for the theory of the firm. *Production and Operations Management*, *27*(7), 1177–1220.

van der Schouten, F. A., van Eijs, M. J., & Heuts, R. M. (1994). The value of supplier information to improve management of a retailer's inventory. *Decision Sciences*, *25*(1), 1–14.

Wang, Z., Gao, W., & Mukhopadhyay, S. K. (2016). Impact of taxation on international transfer pricing and offshoring decisions. *Annals of Operations Research*, *240*(2), 683–707.

Wang, Z., Zheng, Z., Jiang, W., & Tang, S. (2021). Blockchain-enabled data sharing in supply chains: Model, operationalization, and tutorial. *Production and Operations Management*, *30*(7), 1965–1985.

Weiner, S. (2021). *The growing threat of ransomware attacks on hospitals*. https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals

Whitaker, J., Mithas, S., & Krishnan, M. S. (2007). A field study of RFID deployment and return expectations. *Production and Operations Management*, *16*(5), 599–612.

Worth, D. (2018). *At least 57 negative impacts from cyber-attacks*. https://phys.org/news/2018-10-negative-impacts-cyber-attacks.html

Zhou, H., & Benton Jr, W. (2007). Supply chain practice and information sharing. *Journal of Operations Management*, *25*(6), 1348–1365.

Ziedonis, A. A. (2007). Real options in technology licensing. *Management Science*, *53*(10), 1618–1633.

How to cite this article: Kumar, S., & Mallipeddi, R. R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. *Production and Operations Management*, *31,* 4488–4500. https://doi.org/10.1111/poms.13859