E-Commerce Supply Chains with Considerations of Cyber-Security: Should Governments Play a Role?

Suyuan Luo[1], Tsan-Ming Choi[2]

E-commerce supply chains and their members face risks from cyber-attacks. Consumers who purchase goods online also risk having their private information stolen. Thus, businesses are investing to improve cyber-security at a non-trivial cost. In this paper, we conduct a Stackelberg game theoretical analysis. In the basic model, we first derive the equilibrium pricing and cyber-security level decisions in the e-commerce supply chain. Based on real-world practices, we then explore whether or not governments should impose cyber-security penalty schemes. Our findings show that when the government is characterized by having sufficiently high emphasis on consumer surplus, implementing the penalty scheme is beneficial to social welfare. Then, we extend the analysis to examine how adopting systems security enhancing technologies (such as blockchain) will affect the government's choice of imposing penalty. We uncover that when it is beneficial to have government's penalty scheme, the technology benefit-to-cost ratio is a critical factor which governs whether the optimal penalty will be lower or higher with the adoption of systems security enhancing technologies. To generate more insights, we conduct further analyses for various extended modeling cases (e.g., with alliance, competition, and the defense-level dependent penalty scheme) and find that our main results remain robust. One important insight we have uncovered in this study is that imposing government penalty schemes on cybersecurity issues may do more harm than good; while once it is beneficial to implement, the government should charge the heaviest possible fine. This finding may explain why in the real-world, governments basically always adopt a polarized strategy, i.e., either do not impose penalty or impose a super heavy penalty, on cyber-security issues.

Keywords: Cyber-security, blockchain technologies; e-commerce supply chains; government; social welfare.

History: Received: July 2020; Accepted: November 2021 by Jayashankar Swaminathan, after three revisions

---

1. Introduction

Cyber-security issues are becoming a daily challenge for businesses worldwide and must be addressed in e-commerce supply chains. The number of cyber-attacks has grown steadily during the last few years. According to Kaspersky Lab, a cyber-attack was launched every 40 seconds in 2016[3] and the rate of phishing attacks in 2018 was almost doubled compared to 2017[4]. Cyber-attacks may take the form of impersonation, fraudulent banking data use, blackmail, random demands, and power cuts, and their effects range from the theft of individuals' personal information to the theft of confidential industrial product data. For example, in October 2013, the personal information of 2.9 million account holders (logins, passwords, names, and credit card numbers and expiration dates) was stolen from the software company Adobe.

---

[1] Department of Transportation Economics and Logistics Management, College of Economics, Shenzhen University, Shenzhen, China. suyuanluo@126.com

[2] Corresponding author. Department and Graduate Institute of Business Administration, College of Management, National Taiwan University, Roosevelt Road, Taipei 10617, Taiwan, ROC. jasonchoi@ntu.edu.tw

[3] https://www.kaspersky.com/about/press-releases/2016_attacks-on-business-now-equal-one-every-40-seconds (accessed 16 March 2020).

[4] https://usa.kaspersky.com/about/press-releases/2019_kaspersky-lab-finds-phishing-attacks-hit-almost-500-million (accessed 16 March 2020).

Both e-commerce platforms and governments treat cyber-attacks very seriously, as they can compromise users' privacy and may be disastrous for the companies involved. To enjoy the convenience of shopping online, consumers typically need to submit their private information. This exposes their information to serious threats. A security breach of the giant U.S. retailer Target Corporation in December 2013, for example, exposed the personal data of over 110 million consumers, leading to a nearly 50% drop in profits. In January 2014, data from 100 million South Korean credit cards were stolen. As a result, more than 2 million South Koreans had their cards blocked or replaced, as they feared that their bank accounts would be emptied. In 2016, 3 billion Yahoo accounts were hacked, and in 2018, Under Armor reported that its "MyFitnessPal" service had been hacked, affecting 150 million users. Consumers' perceptions of information security can affect their online purchase behavior and can lead to business losses, including an abnormally high turnover of customers and increased customer acquisition activities (Wu et al. 2018). For example, when Sony's PlayStation Network was attacked in April 2011, the personal data of 77 million users were leaked and the banking information of tens of thousands of players was compromised. To appease users, Sony paid out US$15 million in compensation, plus a few million dollars in legal fees, as well as refunding the people whose bank accounts had been illegally used. Cyber-security issues are thus becoming a daily challenge for e-businesses.

To prevent consumer information from being stolen, e-commerce companies are obligated to implement the right technologies (see Section 1.2) at a non-trivial cost. In fact, worldwide spending on information security products and services exceeded US$114 billion in 2018, representing an increase of 12.4% from US$101.54 billion in 2017, according to Gartner, a leading research firm. Gartner also predicted that end-user spending for the information security and risk management market will grow at a "compound annual growth rate" of 8.7% from 2018 through 2023 to reach $188.4 billion in constant currency.[5] In addition to e-commerce companies' cyber-security measures, governments all around the world take different measures for cyber-security related challenges. In 2019, the U.K. government invested £100m in new cyber-security R&D and launched a fund to drive diversity across the industry. Chinese legislators passed an e-commerce law to improve online regulation and protect consumer privacy, which took effect on January 1, 2019, and stated that platforms have the responsibility to protect the security of personal information held by e-commerce platforms. Platform operators would face a penalty of 500,000 yuan (i.e., US$73,260) if they fail to take necessary steps, or up to 2 million yuan in serious cases. On February 28, 2019, Thailand passed its Cybersecurity Act, and legislators in Europe also unanimously passed the Personal Data Protection Act, based on the European Union's General Data Protection Regulation (GDPR). In 2016, the Australian government rolled out its Cyber Security Strategy, which included investments of more than US$230 million across "five areas of action" up until 2020. Some U.S. state governments also implemented regulations to ensure the security of online shopping environments. The four main data oversight categories addressed in this legislation are breach notifications, data security, data disposal, and the privacy of non-personally identifiable information. The Department of Justice of the US government announced in April 2015 its "Best Practices for Victim Response and Reporting of Cyber Incidents,"

[5] https://www.gartner.com/en/documents/3969990/forecast-information-security-and-risk-management-worldw (accessed 16 March 2020)

which supplements its cyber-security regulations[6]. However, not every state in the U.S. has imposed the penalty rule for cyber-security issues. For example, California recently passed the SB-317 Bill, which imposes penalties for non-compliance, but New York has no such restriction (see Table 1.1a). Why this is the case and whether the government should play a more central regulatory role in cyber-security should be examined further. Moreover, as shown in Table 1.1.b (Appendix), in all the real-world cases that we have found, governments basically always adopt a polarized strategy, i.e., either do not impose penalty or impose a super heavy penalty, on cyber-security issues. Whether there is a scientific explanation for the existence of this type of polarized strategy deserves deeper investigation.

Table 1.1a. Some examples of cyber-security rules in different places [7]

Rules	**Details of penalty**
European Union (General Data Protection Regulation)	Very heavy penalty: The maximum fine for non-compliance is €10 million or 2% of "worldwide annual revenue."
New York regulations	No clear penalty imposed for non-compliance
California regulations	Starting from January 1, 2020, "any manufacturer of a device that connects to the internet must equip it with 'reasonable' security features, designed to prevent unauthorized access, modification, or information disclosure." A penalty will be imposed for non-compliance cases.[8]

Motivated by the importance of cyber-security for e-commerce supply chains and the different associated government practices, we explore the following research questions in this paper. (1) In terms of e-tailer's cyber-security investments, what are the optimal retail prices, level of cyber-security, and wholesale pricing decisions in the supply chain, with and without government penalty schemes? (2) How does the presence of a government cyber-security penalty scheme affect the supply chain (and its members), consumers and social welfare? Are there any cases in which having government's penalty scheme does more harm than good? If it is beneficial to implement the penalty scheme, is it wise for the government to impose a very heavy penalty? (3) What are the impacts brought by the e-tailer's deployment of technologies (such as blockchain) on our findings? How robust are the findings? To address the above research questions, we formally build a consumer utility based stylized analytical model and conduct a Stackelberg game-theoretic analysis. We also include extended modeling analyses to show robustness of the findings. Table 1.2 (Appendix) shows features of cyber-security for e-commerce platforms as well as how they are being considered and modeled in this paper to address the research issues. We argue that the models and analyses conducted in this paper are specific to the domain on cybersecurity and hence the derived insights are relevant and applicable to e-commerce supply chains.

To the best of our knowledge, our paper is one of the first analytical operations management (OM) studies that explore cyber-risk in e-commerce supply chains with the considerations of government cyber-security penalty policies and other associated issues (such as the use of technologies). Cyber-attacks in e-commerce supply chains are a serious real-world problem. Our findings give important guidance for policy makers on how to enhance cyber-security and may explain why in the real-world, governments basically always adopt a polarized strategy on cyber-security issues.

[6] https://globalcompliancenews.com/cyber-security/cyber-security-around-the-world/ (accessed 2 March 2020)
[7] https://www.globalsign.com/en/blog/four-cybersecurity-regulations-you-should-know (accessed March 2, 2020).
[8] https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law (accessed March 2, 2020).

The remainder of this paper is organized as follows. Section 2 presents the literature review. Section 3 describes the basic analytical models for the e-commerce supply chains without government intervention (Model NG) and with a government cyber-security penalty scheme (Model G). In Section 4, the two models are compared and the value of government cyber-security penalty schemes (VGCPs) is examined. Section 5 provides extended analyses and Section 6 concludes the study. All proofs as well as some extended modelling analyses and supplementary results are placed in E-Companions (available online).

2. Related Literature

The problems examined in this study are related to research on e-commerce, cyber-security, and the role of government in OM.

OM has entered the digital era. The advancement of e-commerce has led to extensive research on ways of optimizing e-commerce supply chains (Tsay and Agrawal 2004; Cai 2010; Wu et al. 2015; Scholz et al. 2017; Lim and Srai 2018; Zhang and Choi 2021). Earlier studies have explored how consumer behaviors affect e-tailing operations (e.g., Carrillo et al. 2014). In recent years, the operations of online platforms are widely explored, as they support e-commerce (for example, Hao and Fan 2014; Kuruzovich and Etzion 2018). For instance, Niu et al. (2019) model the incentives of competing e-commerce firms for logistics cooperation. They find that if "Firm A" forms a logistics sharing alliance with 'Firm B", then "Firm B" can guarantee customers a promised delivery time (PDT). Wang et al. (2019) conduct a Stackelberg game analysis of electronic business platform financing. The authors empirically examine the effect of offline call intensity on the probability of online consumers' purchasing digital services, and the "carryover effect of call intensity". Zhang and Yao (2020) study a similar problem and consider similar effects. Shen et al. (2019) focus on exploring the problem of a manufacturer's optimal channel selection between a platform retailer and a traditional reseller. Yan et al. (2019) examine whether a marketplace platform should be introduced to e-commerce. The role of using online platforms in e-commerce supply chain strategies has also been examined (Hagiu and Wright 2015; Abhishek et al. 2016; Kwark et al. 2017; Tan and Carrillo 2017; Liang et al. 2020). In particular, Tian et al. (2018) conduct a study of e-commerce platform operations to investigate the role of e-tailers, and find that the interaction between order-fulfilment costs and upstream competition intensity moderates the e-tailer's selection of an optimal mode. In this study, we also address the e-commerce operations problem and the e-tailer in our paper can be an e-platform (such as Amazon.com and JD.com), but we focus on tackling the cyber-security challenge. Unlike other studies, we also examine the government's role in the cyber-security of e-commerce supply chains.

Cyber-security problems are known to be important in the OM literature (Choi et al. 2018; Bier and Gutfraind 2019; Paul and Zhang 2021) but not yet well-explored analytically. For instance, Guha and Kumar (2018) indicate that data and cyber-security are future research directions in the fields of OM and information systems. As Tang and Whinston (2020) argue, security negligence is a major cause of data breaches and can occur if a firm's information technology managers cannot adequately address security vulnerabilities. Cohen (2018) notes that the availability of sensitive personal data can attract hackers and lead to serious cyber-security problems, including "information leakage, fraud, and identity theft". The information privacy issue in e-

commerce platforms is non-trivial, as it may affect consumers' confidence in e-platforms and ultimately reduce profits.

In the context of analytical OM studies, Nagurney and Shukla (2017) claim that firms and governments are sharing threat information to arrange coordinated defenses against attacks. The authors argue that governments and policy-makers are pushing firms to exchange information in the cyber space as a possible defensive mechanism. Wu et al. (2018) explore a firm's information security decisions using game theory. The authors highlight that competition plays a critical role in affecting the optimal security decisions. Khouzani et al. (2019) present a framework to efficiently solve a multi-objective optimization problem for cyber-security defense. Cheung and Bell (2019) present a novel "attacker-defender" model against a "quantal response adversary" to protect critical assets. Eling and Wirfs (2019) conduct an analysis of over 1500 cyber risk incidents extracted from an operational risk dataset. They note that cyber-risk is a special risk category that warrants more research, and their results can help insurance companies with limited data and experience of cyber-risks to develop cyber insurance policies. More recently, Simon and Omar (2020) investigate the cybersecurity investment with the consideration of coordination and strategic attacker. Following this stream of literature, this paper assumes the related information in the supply chain is public. This paper supplements the OM literature on cyber-security analyses. We focus on e-commerce supply chains and analytically study the optimal cyber-security level and the roles played by the government.

Governments can affect supply chain operations through various means. For example, Arya and Mittendorf (2015) note that governments have increasingly attempted to direct business behavior to achieve specific socially desirable outcomes. Hua et al. (2016) study competition and coordination in two-tier public service systems under government fiscal policies. The authors claim that a relatively low tax-subsidy rate can almost perfectly coordinate the two public service providers to achieve almost the maximum possible benefits from the two-tier service system. Berenguer et al. (2017) investigate the effects of subsidies on increasing consumption through for-profit and not-for-profit newsvendors. They show that subsidy programs provide stronger incentives for not-for-profit than for-profit firms to increase consumption. Xiao and Xu (2018) find that it is wise for the retailer to adopt a lost-sale penalty contract, which can incentivize the seller to install the right level of capacity and extract the full surplus. Zhang and Zhang (2018) examine the interactions between customer purchasing behaviours and trade-in remanufacturing. They uncover how a social planner (such as the government) should design a public policy to maximize social welfare. Xu et al. (2018) conduct a study of the impacts of markets and tax on transnational corporations' procurement strategies. They highlight the significance of a company's global supply chain management decisions while taking international taxation rules into consideration. Yu et al. (2018) investigate government subsidy programs and find that governments can improve consumer welfare by developing subsidy programs that involve multiple (competing) manufacturers with different market sizes and adequate capacities. More recently, Hsu et al. (2019) find that a quality subsidy offered by the government to farmers can decrease the quality of their dairy products and their profits. Similar to the above studies, we also explore the role played by governments in the business operations. However, different from them, we focus on exploring whether governments should play a role on cyber-security, which

are motivated by real world observed practices.

In the digital era (Choi et al. 2018; Swaminathan 2018), cybersecurity threats are being a priority for global business. Many researchers investigate how to use systems security enhancing technologies (such as blockchain) to fight against cyber-attacks and improve operations. Doroudi et al. (2021) explore how to mitigate the performance drop and data breaching problems under cyber-attacks by using technologies. Cheung and Bell (2021) propose that real-time recovery technology is crucial in managing real-time cyber-attacks. The authors propose how to improve connectivity of cyber networks. Ji et al. (2016) discuss how big data analysis and optimization tools can be used to tackle advanced cyber-attacks. Bensoussan et al. (2020) reveal that intrusion prevention is a crucial point for overcoming cybersecurity risk. The authors explore how to guarantee the information system's security from the perspective of maintenance practice related to an "intrusion detection system". They mention that companies should continuously employ and update the relevant technologies to be "sustainable" against cyber-attacks. Cohen and Lee (2020) uncover that technologies including robotic automation, artificial intelligence (AI) and Internet-of-Things (IoT) applications can help improve the design of worldwide business networks. They claim that the incomplete integration of networks leads to cyber-security issues. Olsen and Tomlin (2020) discuss the practical values of the technologies for business operations in the industry 4.0 era. The authors point out that blockchain is a possible solution for dealing with the data security challenges. Cui et al. (2021) explore how to make use of technologies such as AI to improve the performance of supply chains. To enhance systems security as well as many business operations, the blockchain technology is commonly known to be useful. In fact, blockchain can be viewed as a distributed ledger which can provide secure data platform and enhance transparency and tractability of data. In the OM literature, Babich and Hilary (2019) discuss how blockchain can be employed to face cyber incident and safety issues. The authors share their visions on the field, including many proposals for future research. Choi and Luo (2019) discuss the "data quality challenges" for sustainable operations in emerging economies. The authors investigate how blockchain may help to enhance operations by dampening data quality related problems. Choi et al. (2020) examine the service pricing problems in "on-demand-service-platform" operations. The authors uncover how blockchain can be used to improve service operations by considering the risk sensitivity of customers. Cai et al. (2021) analytically explore how blockchain can help to address the cheating problems in the use of markdown contract in a supply chain with a rental platform. Luo and Choi (2021) conduct a review related to AI and blockchain. They highlight that the integration of these two critical disruptive technologies can help improve cybersecurity. Choi and Shi (2021) explore the use of blockchain for ride-hailing operations under COVID-19. For more details of using blockchain in supply chain systems, refer to Hastig and Sodhi (2020) and Choi et al. (2021). Note that even though it is known that using the systems security enhancing technology such as blockchain is helpful to deal with challenges in cyber-security, to the best of our knowledge, no prior studies in OM have ever analytically examined this issue. This paper bridges this gap.

3. Basic Models

3.1 Model NG: Without a Government Penalty Scheme

Cyber-attacks potentially affect all members of e-commerce supply chains in an online market. When consumers make purchases online, their private information, including their names, addresses, purchasing records, telephone numbers, and credit card numbers etc., may be at risk of being stolen. Thus, both supply chains and consumers are affected. To enhance readability, the definitions of different models and some important variables are described in Table 3.1. For other notation, please refer to E-Companion A5.

Table 3.1. Definitions of different models and variables

Notation	Meaning
Model NG	E-Commerce supply chains without the government cyber-security penalty scheme.
Model G	E-Commerce supply chains with the government cyber-security penalty scheme.
Model NT	E-Commerce supply chains with technologies and without government penalty.
Model GT	E-Commerce supply chains with technologies and with government penalty.
γ	The likelihood that e-commerce supply chains suffer cyber-attacks.
a	Consumer's sensitivity to cyber-attacks.
β	The "rate of success in detecting the attack", which is the same as "the level of defense effort of the e-tailer" in this paper.
α	The level of cyber-security risk, which is defined as $\alpha = \gamma(1-\beta)$.
m	The unit product cost for the supplier.
w	The product is supplied by the supplier to the e-tailer at a unit wholesale price w.
p	the product's selling price from e-tailer.
F	The penalty the government imposes on the e-tailer when the e-tailer (E) fails to defend against cyber-attack.
π_E	The profit of e-tailer.
π_S	The profit of supplier.
π_{SC}	The profit of supply chain.
CS	The consumer surplus.
SW	The social welfare.
$K_{DE}(\beta)$	The defense effort cost.

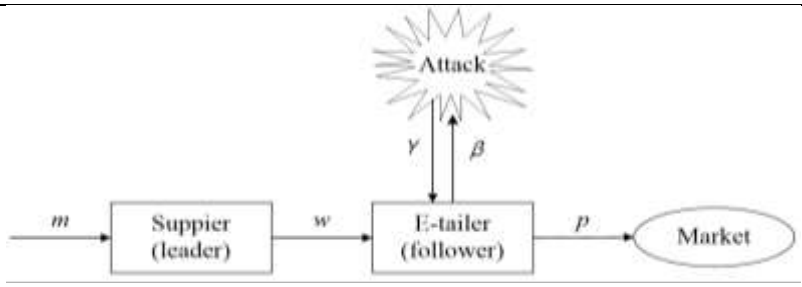

Figure 3.1. An e-commerce supply chain with cyber-attack (Model NG).

In our study, we consider an e-commerce supply chain with a supplier and an e-tailer, as shown in Figure 3.1. The likelihood that e-commerce supply chains suffer cyber-attacks is γ[9]. Following Agurney and Shukla (2017) and Simon and Omar (2020), we explore the case in which the e-tailers and consumers have a perception of the probability of cyber-attack. Both of them form "rational expectations" regarding the likelihood that e-commerce supply chains suffer cyber-attacks. Intuitively, consumers perceive their personal information being exposed and other risks associated with cyber-attacks as negative. Their sensitivity to the level of cyber-security

[9] Note that we mainly focus on the significant cyber-attacks which lead to public awareness. If we take a look at Amazon.com, a lot of public news such as those from Wall Street Journal and others, would report cyberattacks associated with it. This relates to γ. In our analytical model, we assume that γ is public information, which is also based on the fact that major e-tailers have to disclose major cyber-attack events as a part of its corporate social responsibility in any open markets.

risk is denoted by the coefficient a. To protect the online shopping environment, companies implement measures to increase the level of cyber-security. In terms of the e-tailer's attempts to defend against cyber-attack, β represents the rate of success in detecting the attack[10], and $(1-\beta)$ represents the likelihood of failure. Thus, following Nagurney and Shukla (2017), we call the likelihood of "having trouble" (i.e., being attacked and failing to successfully defend against it) when the e-tailer operates online the *level of cyber-security risk* (α), which is defined as $\gamma(1-\beta)$. Note that $\gamma\beta$ represents the level of successful defense from cyber-attack. In this paper, we assume that α and β are common knowledge to the supplier and e-tailer. Firstly, we assume that the e-tailer can communicate the information of cyber security with the supplier. Previous studies have adopted the same assumption that information sharing between the e-tailer and supplier is common. For example, Li (2002), Ha and Tian (2017), and Zhang and Zhang (2020). This is also in line with what the US government is advocating now with the information sharing among private companies on cyber-attacks[11]. Secondly, for *α (level of cyber-security risk)*, it relates to the cyber-attack cases. From news, consumers will have the experience and feeling regarding it because major cyber-attacks cases cannot be hidden. So, we argue that this kind of data is publicly available, and there are lots of cyber-attack news for companies like JD and Amazon. For *β (the rate of success in detecting cyber-attacks)*, it can be judged according to the technology adopted by the platform. Thirdly, from history and experience, and for the analysis purpose, this paper assumes that the level of cyber-security risk and the rate of success in detecting cyber-attacks are publicly known. In other words, in this paper, we consider the symmetry of information and postpone the asymmetry case to future research.

We consider a case in which consumers have a heterogeneous valuation, u, of the product, in which u follows a distribution $f(\cdot)$. Following the literature and for analytical tractability, we consider a case in which $f(u)$ is a uniform distribution with a lower bound of 0 and upper bound of 1, denoted by U [0, 1].[12] In addition, to focus on our main areas of exploration and to simplify the notation, we normalize the market population as 1. E-tailers implement measures to increase their cyber-security, and these measures incur a non-trivial cost. As β denotes the e-tailer's level of defense effort, when an e-tailer exerts an effort β, a defense effort cost $K_{DE}(\beta)$ is incurred, which is given by $k\beta^2/2$, where $k > 0$. Note that k can be treated as the cost coefficient of defense. A higher cyber-security improvement requires more complicated configuration and better functionality of the software system. This leads to a higher level of systems complexity and the cost becomes much higher when the desirable level of cyber-security is higher. It is therefore reasonable to apply a quadratic cost structure, which reflects the fact that the marginal defense cost increases for achieving a higher cybersecurity level (Kim et al., (2011)). What is more, the quadratic cost structure is in line with the extant literature as follows. Shetty et al. (2010) claim that the defense effort costs should increase with the security level. As in Nagurney and Shukla (2017), to reach a security level β, the e-tailer invests $K_{DE}(\beta)$ with the function assumed to be continuously differentiable and convex. Similar to Kim et al., (2011), Nagurney and Shukla (2017) and Yang et al. (2021),

[10] In this paper, β represents "the rate of success in detecting the attack", which is the same as "the level of defense effort of the e-tailer."
[11] https://www.nytimes.com/2021/05/09/us/politics/biden-cyberattack-response.html (accessed 9 May 2021).
[12] In this paper, the consumer utility is equal to $u - a\gamma(1-\beta) - p$, where γ represents the likelihood of being attacked. As such, if the cyber-security risk increases, the consumer utility will be hurt. Following this argument, the derived consumer utility is linear.

we consider the defense effort cost $K_{DE}(\beta)$ given by $k\beta^2/2$ as a convex function of β, indicating that $K'_{DE}(\beta) > 0$ and $K''_{DE}(\beta) > 0$; namely, the cost increases as the rate of success in detecting the attack increases at a growing rate.

When consumers decide whether to shop on an e-tailer platform, they will consider factors such as (i) the product's selling price from e-tailer p; (ii) the level of security regarding their private information, which can be interpreted by the cyber-security risk level of the platform, which is equal to $\gamma(1-\beta)$, where γ and β represent the likelihood of being attacked and the success rate of detecting the attack, respectively; and (iii) consumer sensitivity to the level of cyber-security risk, which we denote by a. Thus, we can derive the number of consumers who will buy the product at a price p and with effort level β. Noting that consumers choose to use the platform when their valuation u is greater than or equal to $p + a\gamma(1-\beta)$, the demand function is given as follows: $D_{(NG)} = \int_{p+a\alpha}^{1} f(u)\,du = 1\left(1 - \left(p_{(NG)} + a\gamma\left(1-\beta_{(NG)}\right)\right)\right)$

$$= 1 - e + e\beta_{(NG)} - p_{(NG)}, \text{ where } e = a\gamma. \quad (3.1)$$

Observe that we use the subscript (*NG*) to represent the functions and optimal decisions under Model NG.

As shown in Figure 3.1, the unit product cost for the supplier under Model NG is m. The product is provided by the supplier to the e-tailer at a unit wholesale price of w. We build a consumer utility based stylized analytical model to conduct a Stackelberg game-theoretical analysis. In our model, the supplier determines the wholesale price as the leader and the e-tailer controls p and β simultaneously as the follower. The sequence of events is illustrated in Figure 3.2.

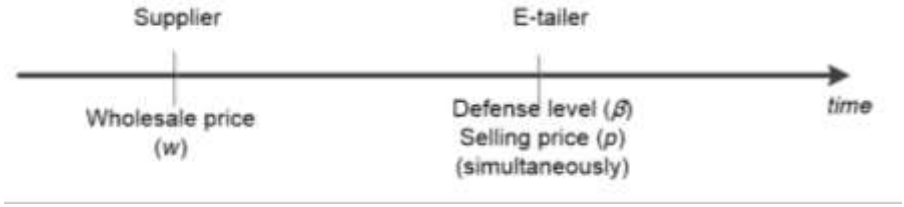

Figure 3.2. Sequence of events for Model NG.

Thus, the profit functions of supplier (*S*) and e-tailer (*E*) are given as follows:

$$\pi_{S(NG)} = \left(w_{(NG)} - m_{(NG)}\right)D_{(NG)} = \left(w_{(NG)} - m_{(NG)}\right)\left(1 - e + e\beta_{(NG)} - p_{(NG)}\right), \quad (3.2)$$

$$\pi_{E(NG)} = \left(p_{(NG)} - w_{(NG)}\right)D - K_{DE}(\beta_{(NG)}) = \left(p_{(NG)} - w_{(NG)}\right)\left(1 - e + e\beta_{(NG)} - p_{(NG)}\right) - k\beta^2_{(NG)}/2. \quad (3.3)$$

We solve this game by backward induction. By checking the Hessian matrix, we find that π_E is jointly concave in $p_{(NG)}$ and $\beta_{(NG)}$, when $k > e^2/2$. In this paper, we consider the case with $k > e^2/2$ which is the common situation because it means exerting effort to defend against cyber-attacks is expensive. If it is not the case, the effort will go to the upper bound, which is unlikely to be the case in practice. For any given wholesale price $w_{(NG)}$, we characterize the equilibrium retail price p and the likelihood of the successful defense β that will maximize $\pi_{E(NG)}$.

We can then determine the wholesale price for the supplier by maximizing the supplier's profit function. As we assume that $k > e^2/2$, it is straightforward to establish that $\pi_{S(NG)}\left(p^*_{(NG)}|_w, \beta^*_{(NG)}|_w\right)$ is concave in w (P.S.: $\partial^2\pi_S/\partial w^2 = -2k/(2k-e^2) < 0$) and optimizing it yields the optimal wholesale price and further

yields the optimal selling price and the likelihood of successful defense in Model NG. We can thus summarize the results as follows. Under Model NG, if $k > e^2/2$, there is a unique equilibrium with the selling price $p^*_{(NG)} = A + \tau B$, the defense effort set by e-tailer $\beta^*_{(NG)} = \frac{eJ}{2\varepsilon}$, and the wholesale price set by the supplier $w^*_{(NG)} = \tau$, where $A = \frac{k(1-e)}{2k-e^2}$, $B = \frac{k-e^2}{2k-e^2}$, $\tau = \frac{1-e+m}{2}, \varepsilon = 2k - e^2$ and $J = 1 - e - m$. We can further derive the corresponding optimal supplier's profit and optimal e-tailer's profit. As β^* and w^* are positive and $1 - B > 0$, we can derive that $\tau > 0$ and $J > 0$. We denote *CS* as the consumer surplus, which can be derived as follows:

$$CS_{(NG)} = \frac{1}{2}(1 - e + e\beta_{(NG)} - p_{(NG)})^2. \quad (3.4)$$

Under Model NG, at the equilibrium, the supplier's profit, the e-tailer's profit, consumer surplus ($CS_{(NG)}$), and social welfare ($SW_{(NG)}$) are given as follows (P.S.: See E-Companion A2 and A3 for more details):$\pi^*_{S(NG)} = 2k\psi$, $\pi^*_{E(NG)} = k\psi$, $CS^*_{(NG)} = k\psi(1 - B)$, $SW^*_{(NG)} = \pi^*_{S(NG)} + \pi^*_{E(NG)} + CS^*_{(NG)} = (4 - B)k\psi$, where $\psi = \frac{(1-e-m)^2}{8(2k-e^2)}$. A complete list of abbreviations is given in E-Companion A5. The results reveal that under Model NG, the equilibrium profit of the supplier is twice that of the e-tailer's profit. i.e., $\pi^*_{S(NG)} = 2\pi^*_{E(NG)}$. Thus, we can clearly see that when m, *a,* k, or γ varies, the effects on the suppler and the e-tailer are the same.

Now, we explore how the cost of the product affects the wholesale price, the selling price, and cyber-security. We have the following findings: If the unit product cost for the supplier *(m)* increases, (i) the optimal wholesale price $w^*_{(NG)}$ will monotonically increase; (ii) the optimal selling price $p^*_{(NG)}$ will increase when $k \geq e^2$ and decrease when $e^2/2 < k < e^2$; (iii) the optimal level of cyber-security $\beta^*_{(NG)}$ will monotonically decrease. By differentiating $w^*_{(NG)}$, $p^*_{(NG)}$, and $\beta^*_{(NG)}$ with respect to *m*, we find that the optimal wholesale price increases in *m*. Intuitively, if the cost of the product increases, the supplier will increase the wholesale price. From $\frac{\partial \beta^*_{(NG)}}{\partial m} < 0$, we see that when the cost (*m*) of the product increases, the e-tailer should pay a higher wholesale price (*w*) to the supplier. Then the e-tailer's motivation to defend against a cyber-attack will also decrease. If $k \geq e^2$, the optimal price will increase when *m* increases. However, if $e^2/2 < k < e^2$, the optimal price will decrease when *m* increases. As β^* decreases, the cyber-security cost for the e-tailer decreases; thus, even if the wholesale price increases, the retail price decreases.

Next, we examine how the likelihood of being attacked (γ) will affect these optimal decisions at the Stackelberg equilibrium. If the likelihood of being attacked (γ) increases, (a) the optimal wholesale price $w^*_{(NG)}$ will monotonically decrease, (b) the optimal selling price $p^*_{(NG)}$ will increase when $\frac{e^2}{2} < k < k_1$, where $k_1 = \frac{1}{12}(e(2 + 3e - 2m) + e\sqrt{4(1-m)^2 + 12e(1-m) - 15e^2})$, else $p^*_{(NG)}$ will decrease when $k > k_1$. and (c) the optimal level of cyber-security $\beta^*_{(NG)}$ will increase when (i) $0 < e \leq \frac{1-m}{2}$; or (ii) $\frac{1-m}{2} < e < \frac{3(1-m)}{2}$ and $\frac{e^2}{2} < k < \frac{e^2(1-m)}{(2e+m-1)}$. Otherwise, $\beta^*_{(NG)}$ will decrease. Thus, we can see that if e and k are within specific ranges, the optimal level of cyber-security $\beta^*_{(NG)}$ will increase as the risk of being attacked increases. This is

because e-tailer is willing to input more effort to reduce the chance of being attacked when the cost of improving the level of security is relatively low. Note that the level of cyber-security risk is defined as $\gamma(1-\beta)$. From (3.3), it indicates that the e-tailer's demand and profit both decrease with *e*. If γ increases, the e-tailer is willing to increase $\beta^*_{(NG)}$ to make the shopping environment safer when $0 < a \leq \frac{1-m}{2\gamma}$, (i.e., e is sufficiently small). However, when e is over a threshold, the e-tailer will increase the likelihood of successful defense $\beta^*_{(NG)}$ to maintain the safety level of the platform when *k* is relatively low. The wholesale price also decreases when the likelihood of being attacked increases. As the online shopping environment will then become more unsafe, the supplier must lower the wholesale price to attract more demand. However, as the probability of the platform being attacked increases, the optimal selling price $p^*_{(NG)}$ will increase when *k* is within a specific range. This can be attributed to the increasing cyber-security cost for the e-tailer.

We now examine how consumer sensitivity to cyber-risk (a) will affect these optimal decisions (equilibrium). We find that under Model NG, at the Stackelberg equilibrium: (i) when the consumer's sensitivity (a) to the cyber-security risk increases, the optimal wholesale price $w_{(NG)}{}^*$ will decrease, and if the given likelihood of being attacked (γ) is higher, this effect will be more obvious; (ii) when a increases, $p^*_{(NG)}$ will increase when k is within the same range as the counterpart for γ; and (iii) the effect of a to $\beta^*_{(NG)}$ is the same as γ. When (i) $0 < \gamma \leq \frac{1-m}{2a}$ (i.e., e is sufficiently small), or (ii) $\frac{1-m}{2a} < \gamma < \frac{3(1-m)}{2a}$ and $\frac{e^2}{2} < k < \frac{e^2(1-m)}{(2e+m-1)}$, the optimal level of cyber-security $\beta^*_{(NG)}$ will increase as consumers are more sensitive to cyber-attack.

Consumers' concerns about cyber-security affect their shopping decisions on the online platform. As consumers become more sensitive to the risk of cyber-attack, the supplier has to lower the wholesale price to attract more demand. If the cost coefficient *k* is moderate, the e-tailer will take the decision to price higher when consumers become more sensitive to an attack, mainly because the e-tailer's cyber-security costs increase. As we can see in the previous paragraph, the likelihood of a successful defense cyber-attack ($\beta^*_{(NG)}$) also increases when *e* is sufficiently small or *k* is within a specific range. The sensitivity analysis for Model NG is summarized in Table 3.2 in Section 3.2. We demonstrate above that the supplier's expected benefit is double of the e-tailer's $\left(\pi^*_{S(NG)} = 2\pi^*_{E(NG)} = 2k\frac{(1-e-m)^2}{8(2k-e^2)} = 2k\psi\right)$.

In summary, the results above show how the supplier's profit $\pi^*_{S(NG)}$ and the e-tailer's profit $\pi^*_{E(NG)}$ are affected by different factors. Under Model NG, (i) If the unit manufacturing cost *(m)* increases, both the supplier's and the e-tailer's profits will decrease. (ii) When $\frac{e^2}{2} < k < \frac{e(1-m)}{2}$, both profits will increase with the chance of being attacked *(*γ). When $k > \frac{e(1-m)}{2}$, their profits will decrease. (iii) When $\frac{e^2}{2} < k < \frac{e(1-m)}{2}$, both profits will increase as consumers become more sensitive to the cyber-security risk. When $k > \frac{e(1-m)}{2}$, their profits will decrease.

Under Model NG, when the cost of product increases, both the supplier's and e-tailer's profits decrease. For the supplier, when γ or a increases, the wholesale price decreases, but the demand increases. The change in

profit depends on the tradeoff between the revenue per product $(w - m)$ and demand. As shown in (3.3), the e-tailer's profit depends on two factors, namely the revenue from selling the product $\left(\left(p^*_{(NG)} - w\right)D\right)$ and the cost of exerting effort for cyber-security ($\frac{k\beta^2}{2}$). When γ or a increases, both the revenue and cost of exerting effort increase simultaneously. The change in the e-tailer's profit is decided by the tradeoff between these two parts. The details of the respective thresholds are given in Table 3.3. When k is relatively low, i.e.,$\frac{e^2}{2} < k < \frac{e(1-m)}{2}$, both profits increase with γ and a.

3.2 Model G: With a Government Penalty Scheme

As mentioned in Section 1.1, in some countries or cities, various government rules and regulations require companies to maintain certain levels of cyber-security. If a breach occurs, companies are subject to significant fines, fees, penalties, and punitive consequences. Violating cyber-security laws is an expensive and disruptive process. For example, the European Union's General Data Protection Regulation (GDPR) is designed to protect the personal information of all its citizens. The GDPR is particularly punitive, with very heavy fines potentially totaling up to tens of millions of dollars. Based on real-world observations, after exploring Model NG, we then consider Model G, in which the government imposes a penalty of cyber-security issue (see Figure 3.3).

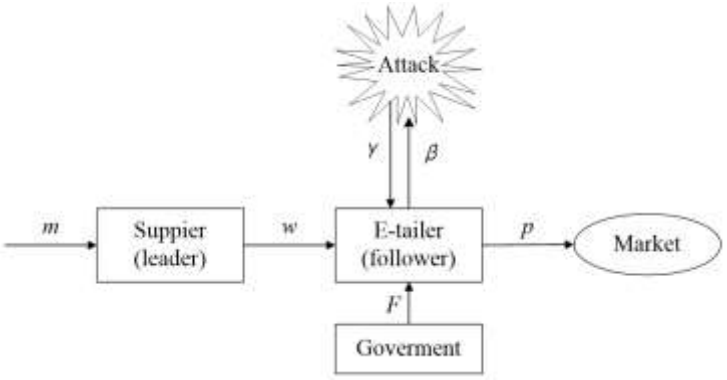

Figure 3.3. An e-commerce supply chain with government penalty scheme (Model G).

In this scheme, the government imposes a penalty *F* when the e-tailer (*E*) fails to defend against cyber-attack (P.S.: In the extended model, we consider the case when the penalty depends on the effort of defense). Note that compared to Model NG, the only difference of Model G is that the e-tailer will suffer a penalty *F* if he fails to defend against the cyber-attack. Thus, the number of consumers who will buy the product at a given price p and effort level β under Model G is given in the following: (P.S.: The subscript (*G*) represents the functions and optimal decisions under Model G):

$$D_{(G)} = \int_{P+a\alpha}^{1} f(u)\,du = 1 - e + e\beta_{(G)} - p_{(G)}. \tag{3.5}$$

Then, the profit functions of the e-tailer and the supplier are shown as follows:

$$\begin{aligned}\pi_{E(G)} &= \left(p_{(G)} - w_{(G)}\right)D_{(G)}\left(1 - \gamma\left(1 - \beta_{(G)}\right)\right) + \left[\left(p_{(G)} - w_{(G)}\right)D_{(G)} - F\right]\gamma\left(1 - \beta_{(G)}\right) - \frac{k\,\beta^2_{(G)}}{2} \\ &= \left(p_{(G)} - w_{(G)}\right)D_{(G)} - F\gamma\left(1 - \beta_{(G)}\right) - \frac{k\beta_{(G)}{}^2}{2}, \end{aligned} \tag{3.6}$$

$$\pi_{S(G)} = \left(w_{(G)} - m_{(G)}\right)D_{(G)} = \left(w_{(G)} - m_{(G)}\right)\left(1 - e + e\beta_{(G)} - p_{(G)}\right). \tag{3.7}$$

We can simplify (3.6) and then find that the difference in the e-tailer's profit function between Model G and Model NG is the term $F\alpha$, which denotes that the e-tailer will suffer a penalty F when failing to detect the cyber-attack. This is the situation in places like European Union, and California. Following Jiang et al. (2017), Choi (2019), and Pun and Hou (2021), we define social welfare as the sum of supplier's profit, e-tailer's profit, and consumer surplus: $SW^*_{(G)} = \pi^*_{S(G)} + \pi^*_{E(G)} + \vartheta CS^*_{(G)}$, where $\vartheta > 0$ represents the relative importance (weight) of consumer surplus in the social welfare. In most prior literature, this value is set to be 1 but as we will see later on, ϑ is in fact critical for our analysis and hence we explicitly define it here. In our model, the government decides the optimal F under a given emphasis on CS. Then the supplier determines the wholesale price as the leader and the e-tailer controls p and β simultaneously as the follower. The sequence of events is illustrated in Figure 3.4.

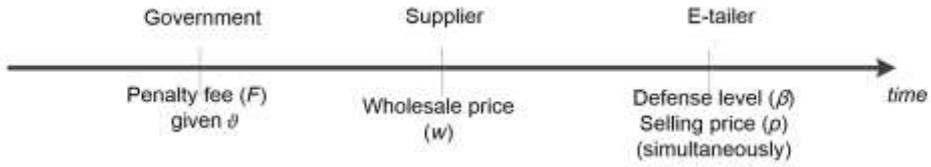

Figure 3.4. Sequence of events for Model G.

Following the similar approach to that in Section 3.1, we summarize the equilibrium decisions and results as follows. Under Model G, if $k > e^2/2$: (a) the optimal wholesale price set by the supplier, the optimal selling price set by the e-tailer and the optimal defense effort determined by the e-tailer are respectively given as follows (P.S.: *A, B, C, F* and other notation can be found in E-Companion A5; we bold some of them as we will refer to them later on):

$$w^*_{(G)} = \frac{k(1-e+m)+eF\gamma}{2k} = \tau + \boldsymbol{C}\cdot\boldsymbol{F}, \tag{3.8}$$

$$p^*_{(G)} = A + \tau B + (\boldsymbol{2}-\boldsymbol{B})\boldsymbol{C}\cdot\boldsymbol{F}, \tag{3.9}$$

$$\beta^*_{(G)} = \frac{e\mathrm{J}}{2\varepsilon} + \frac{(\boldsymbol{3}-\boldsymbol{2B})\boldsymbol{C}\cdot\boldsymbol{F}}{\boldsymbol{e}}, \tag{3.10}$$

where $C = \frac{e\gamma}{2k}$. (3.11)

(b) The supplier's and the e-tailer's profits are given as follows: $\pi^*_{S(G)} = \frac{(k(1-e-m)+eF\gamma)^2}{4((2k-e^2)k} = \frac{2d\varepsilon}{k}$, $\pi^*_{E(G)} = \frac{k^2(1-e-m)^2-2Fk\gamma(8k-e(1+3e-m))+F^2\gamma^2(8k-3e^2)}{8(2k-e^2)k} = M_1$.(c) The consumer surplus and social welfare are given as follows: $CS^*_{(G)} = d, SW^*_{(G)} = \frac{2d\varepsilon}{k} + M_1 + \vartheta d$, where $d = \frac{(k(1-e-m)+eF\gamma)^2}{8(2k-e^2)^2}$. Note that in our analysis, we only discuss the case when e-tailer's profit is positive and the effort level is less than the upper bound. Then we find out that the penalty fee should be less than $\overline{F} \equiv \frac{k(4k-e(1+e-m))}{(4k-e^2)\gamma}$ and $4k > e(1+e-m)$ under Model G. In Table 3.2, we report the sensitivity analysis results for the equilibrium decisions under Models G and NG.

Table 3.2. Sensitivity analyses for Models G and NG

	Model	Equilibrium w	Equilibrium p	Equilibrium β
$m\uparrow$	NG	↑	↓: $(e^2/2 < k < e^2)$ ↑: $k > e^2$	↓

	G	↑	↓: $(e^2/2 < k < e^2)$ ↑: $k > e^2$	↓
γ ↑	NG	↑	↓: $k > k_1$ ↑: $\frac{e^2}{2} < k < k_1$	↓ :1) $0 < e \leq \frac{1-m}{2}$ or 2) $\frac{1-m}{2} < e < \frac{3(1-m)}{2}$ and $\frac{e^2}{2} < k < \frac{e^2(1-m)}{(2e+m-1)}$ ↑: else
	G	↑: $F > \frac{k}{2\gamma}$	↑: $F > \frac{k(k(6k+e(-2-3e+2m))+e^4)}{2(e^4-4e^2k+6k^2)\gamma}$	↑: $F > \frac{ak(4ek+e^2(-1+m)+2k(-1+m))}{e^4-2e^2k+8k^2}$
a ↑	NG	↑	↓: $k > k_1$ ↑: $\frac{e^2}{2} < k < k_1$	↓ :1) $0 < e \leq \frac{1-m}{2}$ or 2) $\frac{1-m}{2} < e < \frac{3(1-m)}{2}$ and $\frac{e^2}{2} < k < \frac{e^2(1-m)}{(2e+m-1)}$ ↑: else
	G	↑: $F > \frac{k}{\gamma}$	↑: $12k \geq k_2$ and $F > \frac{k(e^4-3e^2k+6k^2-2ek(1-m))}{(e^4-3e^2k+6k^2)\gamma}$	↓: $F > \frac{k}{\gamma} - \frac{(e^2+2k)(1-m)}{4e\gamma}$
F ↑	G	↑	↑	↑

We can see that the equilibrium decisions under Model G are very similar to those for Model NG, but with two differences. First, compared with Model NG, each optimal decision has a positive increment (as highlighted in bold, see (3.8) to (3.9)). The details will be discussed in Section 4. Second, under the current model, as the government's cyber-security penalty scheme is enforced, the optimal decisions are affected by F. We also conduct a sensitivity analysis for Model G and its comparison with Model NG is given in Table 3.2.

By differentiating $w^*_{(G)}$, $p^*_{(G)}$ and $\beta^*_{(G)}$ with respect to m, we derive similar results under Model NG. $w^*_{(G)}$ will increase with the unit manufacturing cost (m); the optimal selling price $p^*_{(G)}$ will increase when $k > e^2$, and vice versa. $\beta^*_{(G)}$decreases as m increases. If the cost of the product increases, the supplier will raise the wholesale price and the e-tailer should pay a higher wholesale price to the supplier, and the e-tailer's motivation to defend against a cyber-attack will decrease. If the cost for cyber-security is relatively high ($k > e^2$), the optimal price will increase when m increases. However, if $e^2/2 < k < e^2$, the optimal price will decrease when m increases. As $\beta^*_{(G)}$ decreases, the cyber-security cost for the e-tailer decreases, so although the wholesale price increases, the retailing price decreases.

As the likelihood of being attacked (γ) increases, the optimal wholesale price $w^*_{(G)}$ will increase when $F > \frac{k}{2\gamma}$; the optimal selling price $p^*{}_{(G)}$ will increase when $F > \frac{k(k(6k+e(-2-3e+2m))+e^4)}{2(e^4-4e^2k+6k^2)\gamma}$; and (c) the optimal level of cyber-security $\beta^*_{(G)}$ will increase when $F > \frac{ak(4ek+e^2(-1+m)+2k(-1+m))}{e^4-2e^2k+8k^2}$. Thus, when F is set over a threshold, $w^*_{(G)}$, $p^*_{(G)}$ and $\beta^*_{(G)}$ all increase with γ.

The sensitivity analysis of consumer sensitivity to the cyber-security risk (i.e., a) under Model G is also conducted. Consumers' concerns about cyber-security affect their shopping decisions on online platforms. When consumer sensitivity (a) to the cyber-security risk increases, the optimal wholesale price $w^*_{(G)}$ will increase if $F > k/\gamma$, and vice versa. $p^*_{(G)}$ will increase with a when $12k \geq k_2$ and $F > \frac{k(e^4-3e^2k+6k^2-2ek(1-m))}{(e^4-3e^2k+6k^2)\gamma}$, and vice versa. $\beta_{(G)}{}^*$ will decrease with a when $F > \frac{k}{\gamma} - \frac{(e^2+2k)(1-m)}{4e\gamma}$. k_2 denotes $(2 + 3e + \sqrt{4 + 3(4 - 5e)e})$.

Under Model G, if the unit manufacturing cost (m) increases, both the supplier's and the e-tailer's profits will decrease. If $F > max\{\frac{2k-e(1-m)}{2\gamma}, 0\}$, both profits will increase with the consumer's sensitivity (a). If $F > max\{\frac{k(2k-e+em)}{4k\gamma-e^2}, 0\}$, the supplier's profit will increase with γ. As $\frac{\partial \pi_{E(G)}{}^*}{\partial \gamma} = \gamma_1 = \left[6a^2F^2\gamma^3 - 2ak^2(-1+m+a\gamma) + 2F^2\gamma(-8k+3a^2\gamma^2) + 2Fk\gamma\left(-3a^2\gamma + a(-1+m-3a\gamma)\right) + 2Fk\left(8k + a\gamma(-1+m-3a\gamma)\right)\right]/8k(-2k+a^2\gamma^2)$,when the numerator is positive, the e-tailer's profit increases with γ, and vice versa.

After deriving the equilibrium decisions under Model G, we summarize the impacts of F in Lemma 3.1:

Lemma 3.1. *If the penalty fee F increases, (a) the optimal wholesale price $w^*_{(G)}$, the optimal selling price $p^*_{(G)}$, and the optimal level of cyber-security $\beta^*_{(G)}$ will all monotonically increase. (b) The supplier's profit $\pi_{S(G)}{}^*$ will monotonically increase. (c) If $F > \max\{0, \frac{k(8k+em-e-3e^2)}{(8k-3e^2)\gamma}\}$, the e-tailer's profit will increase with F. (d) The consumer surplus $CS^*_{(G)}$ will be greater if the government raises the penalty fee.*

From Lemma 3.1, we find that as the government increases the intensity of penalty (F), the cyber-environment will be more secure, and consumer surplus will increase, although consumers must pay more for the same product. When the government increases F, the supplier will benefit unconditionally. Intuitively, the e-tailer's profit is always positive under Model NG, while for Model G, it depends on the penalty F.

From the analysis above, we summarize how the supplier's and the e-tailer's profits will be affected by the different factors under the two models in Table 3.3. We then obtain Lemma 3.2.

Lemma 3.2. *i) When the manufacturing cost (m) increases, the supplier's and the e-tailer's profits will be reduced under both models. ii) If the cost of cyber-security is relatively high, both the supplier and the e-tailer will incur losses under model NG when the likelihood of being attacked (γ) increases or the consumers become more sensitive (a) to the cyber-security risk. iii) When F is over a threshold, increases of a or γ have a positive effect on the supplier's and the e-tailer's profits (the existence of β must be guaranteed.)*

Lemma 3.2 (i) shows that when the manufacturing cost rises, both the supplier's and the e-tailer's profits will decrease.

Table. 3.3 Sensitivity analysis of the supplier's and the e-tailer's profits

	Model	$\pi_S{}^*$	$\pi_E{}^*$
$m\uparrow$	NG	↓	↓
	G	↓	↓
$\gamma\uparrow$	NG	↑: $\frac{e^2}{2} < k < \frac{e(1-m)}{2}$. ↓: $k > \frac{e(1-m)}{2}$.	↑: $\frac{e^2}{2} < k < \frac{e(1-m)}{2}$. ↓: $k > \frac{e(1-m)}{2}$.
	G	↑: $F > max\{\frac{k(e-2k-em)}{e^2\gamma-4k}, 0\}$.	↑: $\gamma_1 > 0$. Vice versa.
$a\uparrow$	NG	↑: $\frac{e^2}{2} < k < \frac{e(1-m)}{2}$. ↓: $k > \frac{e(1-m)}{2}$.	↑: $\frac{e^2}{2} < k < \frac{e(1-m)}{2}$. ↓: $k > \frac{e(1-m)}{2}$.

	G	↑: $F > max\{\frac{2k-e(1-m)}{2\gamma}, 0\}$. (Equivalently, if $\frac{e^2}{2} < k < \frac{e(1-m)}{2}$ is satisfied or the penalty fee (F) is greater than $\frac{2k-e(1-m)}{2\gamma}$ when $k > \frac{e(1-m)}{2}$.)	↑: $F > max\{\frac{2k-e(1-m)}{2\gamma}, 0\}$.
F↑	G	↑	↑: $F > \max\{0, \frac{k(e+3e^2-8k-em)}{(3e^2-8k)\gamma}\}$

From Table 3.3, we find that γ and a have different effects on $\pi^*_{S(G)}$ and $\pi^*_{E(G)}$. For Model G, if the likelihood of being attacked through an e-commerce platform increases or the consumers become more sensitive to cyber-attack risk, the supplier's profit will increase when the penalty fee is over a threshold. On one hand, the wholesale price ($i.e., w_{(G)} - w_{(NG)} = CF > 0$) and demand (i.e., $D_{(G)} - D_{(NG)} = (1-B)CF > 0$) increase with the presence of government penalty scheme. On the other hand, as shown in Table 3.2, the wholesale price increases with γ and a when F is greater than $\frac{k}{2\gamma}$. For the e-tailer, compared to Model NG, we have shown above that the e-tailer's demand increases under Model G. However, it doesn't mean that the e-tailer's profit will increase because the e-tailer has to bear the penalty. As Equation (3.6) shows, the e-tailer's profit depends on three factors, the revenue from selling ($\left(p_{(G)} - w_{(G)}\right)D_{(G)}$), the cost of maintain cyber security ($\frac{k\beta_{(G)}{}^2}{2}$) and the penalty ($F\gamma\left(1-\beta_{(G)}\right)$). The details of the thresholds are listed in Table 3.3. Under Model NG, when k is relatively low, i.e., $\frac{e^2}{2} < k < \frac{e(1-m)}{2}$, both profits increase with γ or a. Thus, the determining factor is k for Model NG. For Model G, the determining factor is the relationship between F and k.

If $F > max\{\frac{k(2k-e+em)}{4k-e^2\gamma}, 0\}$, then the supplier's profit will increase with γ. If $F > max\{\frac{2k-e(1-m)}{2\gamma}, 0\}$, (or equivalently, if $\frac{e^2}{2} < k < \frac{e(1-m)}{2}$ is satisfied, or the penalty fee (F) is greater than $\frac{2k-e(1-m)}{2\gamma}$ when $k > \frac{e(1-m)}{2}$), then both the supplier's and e-tailer's profits will increase with the consumer's sensitivity (a). As we have proven that $\frac{e(1-m)}{2} > \frac{e^2}{2}$, when $\frac{e^2}{2} < k < \frac{e(1-m)}{2}$, it yields $\frac{2k-e(1-m)}{2\gamma} < 0$. Both the supplier's and e-tailer's profits will increase with the consumer's sensitivity (a) under Model G. The results reveal that k and F are the key factors.

The supplier's profit and consumer surplus are greater under Model G than under Model NG, and we examine why in Section 4.

4. Values of Government Cyber-Security Penalty Schemes

After deriving the equilibrium decisions and performance measures in the e-commerce supply chains under Models NG and G, we define the following terms, which respectively represent the values of government cyber-security penalty schemes (VGCPS) for the supplier, the e-tailer, consumers, and social welfare when Model G is used (rather than e-commerce supply chains without cyber-security penalty schemes, i.e., Model NG):

$$VGCPS_{(S)} = \pi^*_{S(G)} - \pi^*_{S(NG)}, \quad (4.1)$$

$$VGCPS_{(E)} = \pi^*_{E(G)} - \pi^*_{E(NG)}, \quad (4.2)$$

$$VGCPS_{(CS)} = CS^*_{(G)} - CS^*_{(NG)}, \quad (4.3)$$
$$VGCPS_{(SW)} = SW^*_{(G)} - SW^*_{(NG)}. \quad (4.4)$$

We then compare Models NG and G, and obtain Proposition 4.1.

Proposition 4.1. *For given a, m, k and γ:* $w^*_{(G)} > w^*_{(NG)}$; $p^*_{(G)} > p^*_{(NG)}$; $\beta^*_{(G)} > \beta^*_{(NG)}$; ${\pi_S}^*_{(G)} > {\pi_S}^*_{(NG)}$; $CS^*_{(G)} > CS^*_{(NG)}$.

With the presence of government cyber-security penalty schemes, the wholesale price, the selling price, and the defense effort all increase, as do the supplier's profit and consumer surplus. The optimal decisions under Model G are similar to those under Model NG. Under Model NG, the government is absent, so *F* is not a concern when making the optimal decision. Under Model G, the government provides a cyber-security penalty scheme to improve e-commerce supply chain performance. When the e-tailer fails to detect and prevent a cyber-attack, the fine (*F*) is imposed. Through the equilibrium analysis, we find that the role of government does affect the final decision of the player. First, the wholesale price ($w^*_{(G)} = \tau + CF$) in Model G is higher than that in Model NG and the difference term is *CF*, where $C = \frac{e\gamma}{2k}$. Thus, the higher *F* is, the greater the difference between "the wholesale prices of the two models" becomes. Second, the optimal selling price set by the e-tailer is given as: $p^*_{(G)} = A + \tau B + (2 - B)CF$, which is different from $p^*_{(NG)} = A + \tau B$ in the term $(2 - B)CF$. The penalty increases the selling price $(2 - B)CF$. Third, when there is a government penalty scheme, we find that the defense effort from the e-tailer $\beta^*_{(G)}$ will be greater than that in the situation without the participation of government through the term $\frac{1}{e}(3 - 2B)CF$. As shown above, when the government is involved in supervising the e-tailer's defense effort against cyber-risk, the increment of the wholesale price is *CF*. The unit product cost for the supplier *m* remains unchanged. Thus, the profit per product also increases with *CF*, and the demand for the product also increases (i.e., $D_{(G)} - D_{(NG)} = (1 - B)CF > 0$). The supplier's profit under Model G is therefore greater than that under Model NG. Consumers benefit from government cyber-security penalty schemes. Although they must pay more for the same product $p^*_{(G)} > p^*_{(NG)}$, the likelihood of a successful defense goes up more significantly $\beta^*_{(G)} > \beta^*_{(NG)}$. Thus, the consumer surplus $CS^*_{(G)}$ rises compared with $CS^*_{(NG)}$.

Proposition 4.1 clearly demonstrates the impact of the government intervention, and the differences in the equilibrium decisions between Model NG and Model G are highlighted (see (3.8) to (3.10)). The results also show that the supplier always benefits from the penalty scheme. After switching from Model NG to Model G, the selling price increases more than the wholesale price (P.S.: From (3.8) and (3.9), since $(2 - B) > 1$, we have: $p^*_{(G)} - p^*_{(NG)} > w^*_{(G)} - w^*_{(NG)}$.). Compared to Model NG, we have shown above that the e-tailer's demand increases under Model G. However, it doesn't mean that the e-tailer's profit will increase because the e-tailer has to bear the penalty. To avoid being punished, the e-tailer attempts to further increase the level of cyber-security as $\beta^*_{(G)} > \beta^*_{(NG)}$. This is also shown in Proposition 4.1. From (4.1) to (4.4) as well as Proposition 4.1, we can see that $VGCPS_{(S)}$ and $VGCPS_{(CS)}$ are always positive whereas $VGCPS_{(E)}$ is negative. For $VGCPS_{(SW)}$, we find that it is negative when $\vartheta = 1$.

To have a clearer picture regarding how various parameters affect $VGCPS_{(SW)}$ with different ϑ, we conduct a numerical analysis. We explore how the product cost (m), the likelihood of being attacked (γ), consumer sensitivity to the level of cyber-security risk (a) and the cost coefficient of defense (k) will affect $VGCPS_{(SW)}$ when the threshold of ϑ takes different values. We will also find the conditions when $VGCPS_{(SW)}$ becomes positive. In Figures 4.1 to 4.4, the basic parameters are set as follows (except for the parameter under study when we will vary it): $a = 1$, $\gamma = 0.18$, $e = 0.18$, $k = e^2/2 + 0.1 = 0.1162$, $F = 0.35$, $m \in [0,1]$. From Figures 4.1 to 4.4, we have the following observations: (i) Effects brought by some parameters such as m, k and a are monotone while the effect brought by γ is not. (ii) $VGCPS_{(SW)}$ becomes positive when ϑ is sufficiently big.

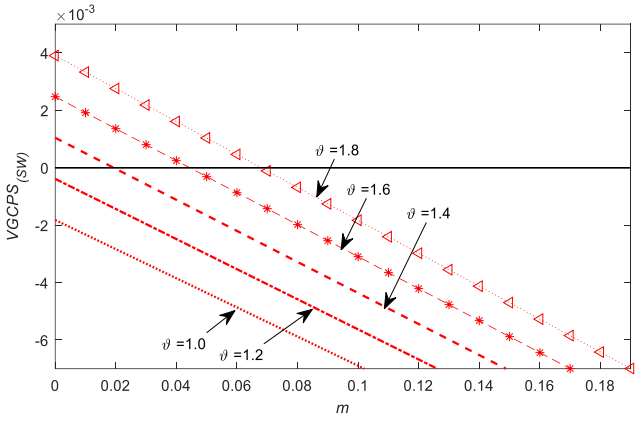

Figure 4.1. How m affects $VGCPS_{(SW)}$.

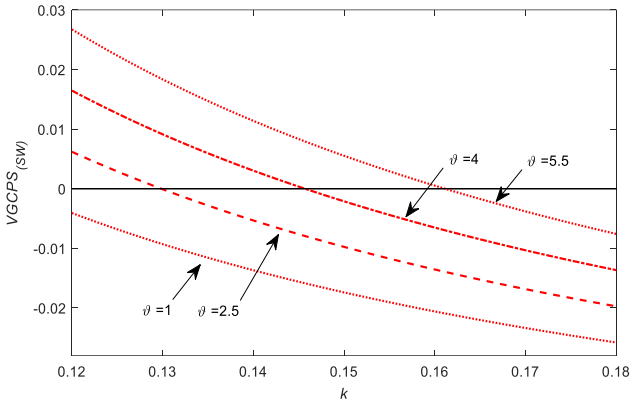

Figure 4.2. How k affects $VGCPS_{(SW)}$.

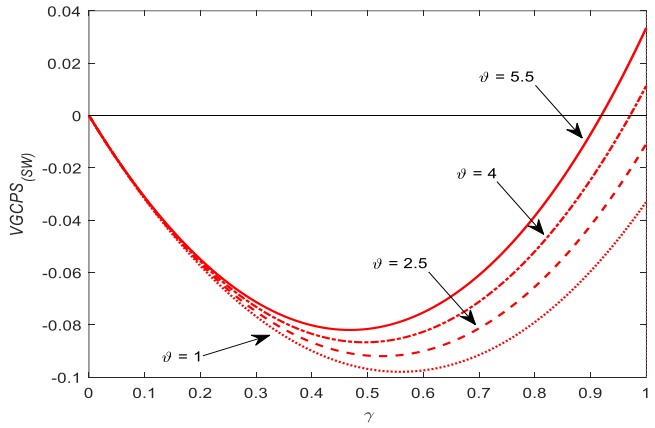

Figure 4.3. How γ affects $VGCPS_{(SW)}$.

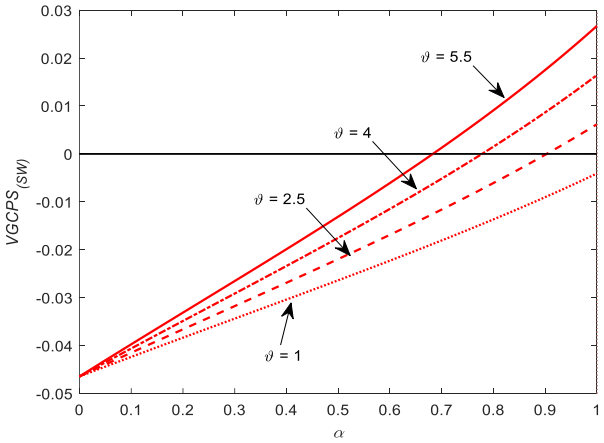

Figure 4.4. How a affects $VGCPS_{(SW)}$.

From the above numerical analysis, it is clear that if the government puts a higher emphasis on *CS,* then $VGCPS_{(SW)}$ will become positive. In fact, we can prove this result analytically. To be specific, $VGCPS_{(SW)} \geq 0$ if and only if $\vartheta \geq T \equiv \frac{(2k-e^2)(2k(8k-e(3+e-3m))-F(8k-e^2)\gamma)}{ek(2k(1-e-m)+eF\gamma)}$. Note that under Model G, F is bounded above by $\overline{F} \equiv \frac{k(4k-e(1+e-m))}{(4k-e^2)\gamma}$ (or else the e-tailer will quit the market). If F is positive and approaches zero, we get $\lim_{F\to 0} T = \frac{(2k-e^2)(8k-e(3+e-3m))}{ek(1-e-m)}$. When F is set to be the upper bound $\overline{F}$, then $T(F = \overline{F})$ is equal to the following $\frac{(2k-e^2)(e^4-12e^2k+32k^2+5e^3(1-m)-16ek(1-m))}{ek(e^3-4ek-3e^2(1-m)+8k(1-m))}$. We define $\overline{T} \equiv \frac{(2k-e^2)(8k-e(3+e-3m))}{ek(1-e-m)}$ and $\underline{T} \equiv$

$\frac{(2k-e^2)(e^4-12e^2k+32k^2+5e^3(1-m)-16ek(1-m))}{ek(e^3-4ek-3e^2(1-m)+8k(1-m))}$. Based on the above exploration, we have Theorem 4.1 (P.S.: The government aims to maximize the social welfare).

Theorem 4.1. *(a) It is wise for the government to impose the penalty scheme if and only if* $\vartheta > T \equiv \frac{(2k-e^2)(2k(8k-e(3+e-3m))-F(8k-e^2)\gamma)}{ek(2k(1-e-m)+eF\gamma)}$ *and the optimal* $F = \overline{F}$ *(i.e., the upper bound). Otherwise, if* $\vartheta \leq T$*, then the government should not impose the penalty. (b) Under Model G (in which the government imposes a penalty fee less than* $\overline{F}$*), then when the government's penalty fee increases: (i) Both the supplier and consumer are always benefited from the scheme. However, the e-tailer's profit is hurt. (ii) If the government puts a sufficiently high emphasis on CS (i.e.,* $\vartheta > \overline{T}$*), social welfare increases.*

Theorem 4.1(a) highlights the condition under which Model G outperforms Model NG. Theorem 4.1 (b) indicates the impacts brought by the government's penalty scheme. One interesting point to note is that, if the government has a sufficiently high emphasis on *CS* (when the weight of *CS* (i.e., ϑ) is over $\overline{T}$), social welfare is improved upon the implementation of the penalty scheme. As $VGCPS_{(SW)}$ increases with *F*, if the government has a sufficiently high emphasis on *CS* as mentioned in Theorem 4.1(b)(ii), then the government's optimal decision is to impose the highest penalty fee $\overline{F}$. As a remark, when $\underline{T} < \vartheta < \overline{T}$, Model G yields a higher social welfare than Model NG if the government imposes a penalty fee between $[\ddot{F}, \overline{F}]$, where $\ddot{F} = arg_F(T = \vartheta)$; if $\vartheta < \underline{T}$, the penalty scheme should not be implemented.

To better understand Theorem 4.1(b)(ii), we explore how the critical threshold T is affected by various factors. First, for the factor *m*, the impact is obvious in which a larger *m* will lead to a greater *T*. For other parameters, as the conditions are indeed rather complex, we conduct a numerical sensitivity analysis to show how the factors affect *T*. Please refer to the E-Companion for the details.

While if we look at individual stakeholders, we conclude that it is impossible to achieve the "all-win situation" under Model G (compared to Model NG) as some parties like the e-tailer is always worse off. An important implication from Theorem 4.1(a) is that: For the governments which treasure consumer welfare more, it is appropriate to implement penalty schemes. Theorem 4.1 may hence explain why some governments (such as European Union) have implemented the penalty scheme but some (e.g., New York) do not. Plus, in all the cases that we have found, once the penalty scheme is implemented, the fine is very heavy. The real-world cases are in line with our finding in which governments basically always adopt a polarized strategy, i.e., either do not impose any penalty or impose a super heavy penalty on cyber-security issues.

As a remark, implementing the government's penalty scheme is not always preferred in all cases. Even if it is preferred, we have shown that the e-tailer still needs to suffer. Thus, in the extended analyses in Section 5, we consider some other measures (Section 5.1), forming alliances (Section 5.2 and E-Companion, etc.) which may help achieve all-win for all members of the supply chain, for both the cases with/without the government's penalty scheme.

5. Extensions

5.1 Using Blockchain-Based Systems Security Enhancing Technologies

In e-commerce and supply chain operations, a recent hot topic is about the implementation of innovative technologies such as blockchain (Choi et al. 2021; Pun et al. 2021; Shen et al. 2021; Wang et al. 2021). As mentioned in Section 1.2, for cyber-security, it is also widely reported that blockchain technologies can help provide the technological platform for operations with secure data. In real world, Danieli, one of the world's largest suppliers in the steel industry, is implementing blockchain technology to enhance cybersecurity for its networks[13]. Cyber Alliance Management (cm-alliance.com) recently even lists various application areas of blockchain for cybersecurity[14]. In this section, we analytically examine how systems security enhancing technologies (such as those blockchain-based systems) [15] can play a role for cyber-security. We extend the analysis to explore the impacts brought by the use of technologies by the e-tailer. We generate additional insights by exploring cases in which: (i) the e-tailer adopts technologies to defense cyber-attack without government penalty (Model NT); and (ii) the e-tailer makes use of technologies with government penalty (Model GT). We aim to see if adopting technologies can be an effective way to better deal with cyber-security. Before we conduct further analyses, we have Definition 5.1 which describes the "all-win" scenario.

Definition 5.1. *An all-win scenario is achieved under Model x if the supply chain, consumers and social welfare under Model x are all better off compared to the respective ones under Model NG.*

Note that for the cases with strategic alliance, Definition 5.1 treats the supply chain as a unit. If the all-win situation is achieved, it is just a matter of profit division between the e-tailer and supplier in sharing the "supply chain surplus", e.g., via a bargaining model.

5.1.1 Model NT

Before we conduct further analyses, we introduce the new demand function and profit functions which are shown as below:

$$D_{(NT)} = \int_{p+a\alpha-b}^{1} f(u)\,du = 1 + b - e + e\,\beta_{(NT)} - p_{(NT)}, \qquad (5.1)$$

where $b > 0$ is the benefit brought to consumers with the use of technologies (e.g., blockchain) as it fosters trust and may allow consumers to check more things with clean data. To be specific, if the right technologies are used, consumers will feel more secure towards the e-tailing operations and this increases their purchasing utility. Furthermore, with technologies such as blockchain-based platforms, transparency of the e-commerce supply chain will usually be enhanced and consumers can know more about the product (e.g., the product provenance information). This also creates value to the consumers.

$$\pi_{E(NT)} = \left(p_{(NT)} - w_{(NT)} - c\right)D_{(NT)} - K^{IT}\left(\beta_{(NT)}\right) - \ T^{IT}\,, \qquad (5.2)$$

[13] https://industryeurope.com/metals-giant-danieli-announces-move-towards-blockchain-based/ (accessed 26 March 2021)
[14] https://www.cm-alliance.com/cybersecurity-blog/the-future-use-cases-of-blockchain-for-cybersecurity (accessed 26 March 2021)

[15] In the remaining parts of this extended analysis, unless otherwise specified, the term "technologies" refer to the "systems security enhancing technologies" such as the use of blockchain.

$\pi_{S(NT)} = (w_{(NT)} - m)D_{(NT)}$, (5.3)

where $K^{IT}(\beta_{(NT)}) = k^{IT}\beta_{(NT)}^2/2$ and $k^{IT} < k$ which means improve cyber-defense is cheaper with technologies than without technologies; $c > 0$ is the per unit technologies operations cost; $T^{IT} > 0$ is the fixed technologies cost.

We try to explore and see if the use of technologies is an effective measure. By checking the Hessian matrix, we find that $\pi_{E(NT)}$ is jointly concave in $p_{(NT)}$ and $\beta_{(NT)}$,when $k^{IT} > e^2/2$. We solve this game by backward induction. Like the derivations and analyses conducted for Model NG, we can derive the respective equilibrium decisions for Model NT. There is a unique equilibrium with the wholesale price $w_{(NT)}^* = \frac{1}{2}(1 + b - c - e + m)$; the selling price $p_{(NT)}^* = \frac{e^3 - 3ek^{IT} - e^2(1+b+c+m) + k^{IT}(3+3b+c+m)}{2(2k^{IT} - e^2)}$, and the defense effort $\beta_{(NT)}^* = \frac{e(1+b-c-e-m)}{2(2k^{IT} - e^2)}$.

The supplier's profit, the e-tailer's profit, consumer surplus ($CS_{(NT)}$), and social welfare ($SW_{(NT)}$) are given as follows (P.S.: See E-Companion A4 for the detailed derivations): $\pi_{S(NT)}^* = \frac{k^{IT}(1+b-c-e-m)^2}{4(2k^{IT} - e^2)}$, $\pi_{E(NT)}^* = \frac{k^{IT}(J+b-c)^2}{8(2k^{IT} - e^2)} - T^{IT}$, $CS_{(NT)}^* = \frac{k^{2IT}(1+b-c-e-m)^2}{8(2k^{IT} - e^2)^2}$, $SW_{(NT)}^* = \frac{k^{IT}(7k^{IT} - 3e^2)(1+b-c-e-m)^2}{8(2k^{IT} - e^2)^2} - T^{IT}$.

Define the technology benefit-to-cost ratio (*BCR*) as follows:

$BCR = b/c$,

which is a relative measure to represent whether the use of technologies is beneficial or not. It is crystal clear to see that using technologies is beneficial, "neutral", and harmful if *BCR* > 1, = 1, and < 1, respectively.

Note that BCR is a critical factor. To be specific, we find that the main difference between Model NG and Model NT is related to factors including *BCR* (i.e., b and c) and T^{IT}. For $w_{(NT)}^*$: If $BCR \geq 1$ then $w_{(NT)}^* \geq w_{(NG)}^*$. If $BCR < 1$, then $w_{(NT)}^* < w_{(NG)}^*$. Since $k^{IT} < k$, so we can get $0 < 2k^{IT} - e^2 < k - e^2$. For $\beta_{(NT)}^*$: The denominator for $\beta_{(NT)}^*$is smaller than $\beta_{(NG)}^*$; if $BCR \geq 1$, $\beta_{(NT)}^*$ is definitely greater when technologies are adopted. If b is slightly less than c, $\beta_{(NT)}^*$ increases. The magnitude depends on a tradeoff between the decrease of denominator and the increase of numerator. If $b \ll c$, then $\beta_{(NT)}^*$ decreases. The conditions are the same for the supplier's profit $\pi_{S(NT)}^*$ and consumer surplus $CS_{(NT)}^*$.

For the e-tailer: If $BCR \geq 1$ and $0 < T^{IT} < \frac{k^{IT}(J+b-c)^2}{8(2k^{IT} - e^2)} - \frac{kJ^2}{8(2k - e^2)}$, then $\pi_{E(NT)}^* > \pi_{E(NG)}^*$. If b is slightly less than c and T^{IT} is small enough, the e-tailer is still benefited from the adoption of technologies. Otherwise, the e-tailer will be hurt, i.e.,$\pi_{E(NT)}^* < \pi_{E(NG)}^*$. For *SW*, if $BCR \geq 1$ and $0 < T^{IT} < \frac{k^{IT}(7k^{IT} - 3e^2)(1+b-c-e-m)^2}{8(2k^{IT} - e^2)^2} - \frac{k(7k - 3e^2)J^2}{8(2k - e^2)^2}$, then $SW_{(NT)}^* > SW_{(NG)}^*$. If b is slightly less than c, and T^{IT} is small enough, *SW* will increase when technologies are present. Otherwise, $SW_{(NT)}^* < SW_{(NG)}^*$.

From the above analysis, we find that if $BCR \geq 1$ and $0 < T^{IT} \leq \frac{k^{IT}(b-c)(b-c+2J)}{8(2k^{IT} - e^2)}$, then $\pi_{E(NT)}^* > \pi_{E(NG)}^*$.

If $BCR \geq 1$ and $0 < T^{IT} \leq \frac{k^{IT}(7k^{IT}-3e^2)(b-c)(b-c+2J)}{8(2k^{IT}-e^2)^2}$, then $SW^*_{(NT)} > SW^*_{(NG)}$. When $BCR \geq 1$ and $\frac{k^{IT}(b-c)(b-c+2J)}{8(2k^{IT}-e^2)} < T^{IT} \leq \frac{k^{IT}(b-c)(b-c+2J)}{8(2k^{IT}-e^2)}$, the e-tailer's profit is hurt with the use of technologies, but the *SW* increases. Exploring $CS^*_{(NT)}$ and $\pi^*_{E(NT)}$, we can find that if $BCR \geq 1$, then $CS^*_{(NT)} > CS^*_{(NG)}$, which means using technologies is good for consumers. Moreover, using technologies is harmful to the e-tailer if T^{IT} is over $\frac{k^{IT}(b-c)(b-c+2J)}{8(2k^{IT}-e^2)}$.

We summarize the core insights from the above analysis in Theorem 5.1

Theorem 5.1. *Under the case without government penalty, if BCR* ≥ 1*, the e-tailer's use of technologies such as blockchain (i.e., comparing between Model NG and Model NT) will yield the following: (a) The cyber-security level is higher. (b) Both the supplier and consumers are benefited. (c) When* T^{IT} *is sufficiently small, the e-tailer is benefited and social welfare is improved. When* T^{IT} *is moderate, social welfare is improved but the e-tailer suffers a loss. When* T^{IT} *is sufficiently big, the e-tailer suffers a loss and social welfare drops.*

Theorem 5.1 points out that the adoption of technologies brings benefit to the cyber-security level. There exists an all-win situation for all participates including consumer, supplier and e-tailer, when the benefit brought to consumers with the use of technologies is greater than the per unit technology operations cost and the fixed technology cost is relatively small ($0 < T^{IT} < \frac{k^{IT}(J+b-c)^2}{8(2k^{IT}-e^2)} - \frac{kJ^2}{8(2k-e^2)}$). However, it may be harmful to the e-tailer when the fix cost is relatively high. As a result, for the case when using technologies is harmful to the e-tailer, the government may help by providing a financial support, such as sponsoring the e-tailer to cover a part of the fixed cost of using technologies. Note that having government's sponsor to support technological development is rather common[16] and hence providing this type of government sponsor should be feasible.

As concluded, the adoption of technologies can increase the cybersecurity level and bring benefit to all members when the benefit brought to consumers with the use of technologies (b) is greater or slightly less than the per unit technology operations cost (c) and the fixed technology cost (T^{IT}) is not very high.

5.1.2 Model GT

In the above model analysis, we confirm that Model NT can improve the performance of every member and enhance the cyber-security level. In this section, we consider the presence of both government penalty scheme and technologies, represented by Model GT. Here, if consumers suffer a cyber-attack, the government will impose a penalty *F* on the technology-based e-commerce supply chain.

Like the derivations and analyses conducted for Model NT, we can derive the respective equilibrium decisions for Model GT. The equilibrium decisions under Model GT are very similar to those for Model G. Compared with Model G, each optimal decision has the new terms related to b and c. The fixed technology cost (T^{IT}) affects the profit of e-tailer and social welfare. Note that in our analysis, we only discuss the case

[16] https://medium.com/singulardtv/5-governments-that-actually-support-blockchain-innovation-d4b3c1e27119; and https://coindelite.com/news/u-k-government-is-ready-to-sponsor-blockchain-startups/ (accessed 8 January 2021).

when the e-tailer's profit is positive and the effort level is less than the upper bound. Thus, we find out that the penalty fee should be less than $\overline{F}_{IT} \equiv \frac{k^{IT}(4k^{IT}-e(1+e-m+b-c))}{(4k^{IT}-e^2)\gamma}$ and $4k^{IT} > e(1+e-m+b-c)$ under Model GT. Since the value of the penalty scheme for social welfare increases with the penalty fee, the optimal decision of F for government is $\overline{F}_{IT}$ under Model GT.

By comparing Model G and Model GT, we have Proposition 5.1.

Proposition 5.1. *If it is beneficial to impose the penalty, comparing between Model G and Model GT: When, $BCR > 1$, then the optimal penalty is smaller after adopting technologies (such as blockchain). Otherwise, if the $BCR < 1$ (BCR = 1), then the optimal penalty is larger (unchanged) after technology adoption.*

Proposition 5.1 indicates the importance of *BCR* in deciding whether the optimal penalty will be larger or smaller after the adoption of technologies. This finding is neat and also in line with the above discussions. The adoption of technologies with government intervention (by comparing Model GT and Model G) has the similar effect as the case without government intervention (comparing Model NT and Model NG). Compared Model GT to Model G, the adoption of technologies can also improve the cybersecurity level and bring benefit to supplier and consumer when $BCR \geq 1$. The profit of e-tailer and social welfare only increase when the use of technologies(b) is greater or slightly less than the per unit technologies operations cost (c) and the fixed technology cost (T^{IT}) is not very high. With the utilization of technologies, if the benefit brought to consumers with the use of technology is greater than the per unit technology operations cost (i.e., $BCR > 1$), then we can find that $\overline{F}_{IT} < \overline{F}$. This implies that for the government, the optimal penalty fee decreases after adopting technologies. Otherwise, if the $BCR < 1$, then $\overline{F}_{IT} > \overline{F}$, which indicates that the optimal penalty fee increases after technology adoption.

Similar to the analysis for Section 4, by comparing Model GT with Model NT, we can get the findings like Proposition 4.1. For given a, m, k and γ, we have: $w^*_{(GT)} > w^*_{(NT)}, p^*_{(GT)} > p^*_{(NT)}, \beta^*_{(GT)} > \beta^*_{(NT)}, {\pi_S}^*_{(GT)} > {\pi_S}^*_{(NT)}, CS^*_{(GT)} > CS^*_{(NT)}$. If we look at the impacts of having the penalty scheme under the case with technologies, we will find the government's use of penalty scheme will yield the following: (i) The cyber-security level is higher than the case without penalty scheme. (ii) Both the supplier and consumer are benefited from the scheme than without penalty scheme. (iii) The e-tailer's profit is hurt than without penalty scheme.

As $SW^*_{(GT)} - SW^*_{(NT)}$ increases with F, if the government has a sufficiently high emphasis on *CS*, then the optimal decision for government is to impose the highest penalty fee $\overline{F}_{IT}$. To be specific, with technologies, it is wise for the government to impose the penalty scheme if and only if $\vartheta_{IT} \geq T_{IT} \equiv \frac{(2k^{IT}-e^2)(2k^{IT}(8k^{IT}-e(3+3b-3c+e-3m))-F(8k^{IT}-e^2)\gamma)}{ek^{IT}(2k^{IT}(1+b-c-e-m)+eF\gamma)}$. If the government puts a sufficiently high emphasis on *CS* (i.e., $\vartheta_{IT} \geq T_{IT}$), social welfare increases. It shows the robustness of our core findings in our basic models.

We define $\overline{T}_{IT} \equiv \frac{(2k^{IT}-e^2)\left(8k^{IT}-e(3+3b-3c+e-3m)\right)}{ek^{IT}(1+b-c-e-m)}, \ddot{F}_{IT} = arg_F(T_{IT} = \vartheta_{IT})$, and $\underline{T}_{IT} \equiv \frac{(2k^{IT}-e^2)\left(e^4-12e^2k^{IT}+32k^{2IT}+5e^3(1+b-c-m)-16ek^{IT}(1+b-c-m)\right)}{ek^{IT}\left(e^3-4ek^{IT}+8k^{IT}(1+b-c-m)+3e^2(-1-b+c+m)\right)}$. Note that the subscript *IT* means the case with

technology adoption.

When $\underline{T}_{IT} < \vartheta_{IT} < \overline{T}_{IT}$, if the government chooses the penalty fee between $[\ddot{F}_{IT}, \overline{F}_{IT}]$, then imposing penalty is good for the social welfare and hence Model GT outperforms Model NT (P.S.: $\overline{F}_{IT}$ is the government's optimal decision). Otherwise, the penalty scheme should not be adopted as Model NT is better than Model GT. If $\vartheta_{IT} < \underline{T}_{IT}$, the penalty scheme should not be implemented.

With the present of the penalty scheme under the case with technologies, we will find that: (a) Social welfare increases if the government puts a sufficiently high emphasis on *CS* (i.e., $\vartheta_{IT} > \overline{T}_{IT}$), (b) It is wise for the government to impose the penalty scheme if and only if $\vartheta_{IT} > T_{IT}$. These findings are basically consistent with the ones in Theorem 4.1, and hence we can see that the respective findings in the basic model stay robust.

Furthermore, focusing on the thresholds (i.e., T for the case without technologies and T_{IT} for the case with technologies) which determine whether implementing the government's penalty scheme is beneficial to social welfare, we have the following findings: If F is relatively small and $BCR > 1$, then T_{IT} is smaller than T. It means that the penalty scheme more likely be preferred after the introduction of technologies. If F is relatively high and $BCR < 1$, then T_{IT} is greater than T. It presents that the penalty scheme is more likely be preferred under the case without technologies.

As a remark, we also explore a scenario in which the e-tailer outsources the cyber-security task to a third-party high-tech company by a paying lump-sum payment to acquire perfect security (i.e., $\beta = 1$). This extended analysis is in fact based on some industrial observations. For example, e-tailer can buy the cyber-security service from the outside platform like IBM Blockchain, Alibaba Cloud (Baas), etc. As claimed from the Alibaba[17], Blockchain as a Service (BaaS) is an enterprise-level platform service based on leading blockchain technologies, which would ensure companies could operate in a secure and stable environment. The platform also declares that BaaS "provides advanced security protection and creates a multi-dimensional blockchain security system". For IBM Platform, security is also guaranteed and many successful blockchain application cases are realized for various industries. Based on these cases, we build analytical models to identify the value of this outsourcing service by exploring the equilibrium profit of the e-tailer in the presence of government penalty scheme and outsourcing service. The details of this extended analysis are available upon request[18].

5.2. Other Extensions[19]

To show further robustness of our findings and generate more insights, we have conducted some more extended analyses. The detailed analyses can be found in the E-Companion (published online) and we present the core findings in the following.

Alliance*:* We consider the case in which the supplier and e-tailer form a strategic alliance and be integrated. For this case, we have shown that by forming the supply chain alliance, the cyber security level, the

[17] https://www.alibabacloud.com/products/baas?gclid=EAIaIQobChMI68r7woOY6gIVylVgCh2w-w0vEAAYAiAAEgKtzvD_BwE (accessed 23 June 2020)

[18] We sincerely thanks for reviewer's advice. The extension of outsourcing security with government supervision is available upon request.

[19] We just concisely present the core findings from these various extensions in the mainbody and relegate the details to the Online Appendix. We sincerely thank the comments by the senior editor and reviewers on restructuring the paper to make it cleaner and neat to read.

profit of the whole supply chain, consumer surplus, and social welfare will all be better. Forming an alliance, as an all-win strategy, is a very effective way for improving cybersecurity level. Thus, when it is unwise for the government to implement the penalty scheme, it will be a good idea for the government to encourage the e-tailer and supplier to form a strategic alliance and this will interestingly enhance the cyber security level. This is consistent with the observed industrial practices that major e-tailers like Amazon.com and JD.com all have formed strategic alliances with many of their suppliers. In addition to many benefits in supply chain operations (such as dampening the bullwhip effect and improving coordination), our findings show that this act is also helpful for cybersecurity.

Competition: In the market, competition commonly exists. We hence consider a stylized supply chain consisting of two competing e-tailers (called e-tailers 1 and 2) selling two substitutable products. (a) For the case without government's penalty, our findings interestingly show that a higher level of price competition benefits all members and enhances the cyber-security level. The larger degree of cyber-security competition also benefits all members when the cost coefficient for cyber-security is high enough. However, when the cost is not so high, members are hurt. (b) For the case with government's penalty, we find that the results of the basic models stay robust.

Defense-level dependent penalty: To check if a change of penalty scheme may affect the findings, we consider in an extended model the case in which the government's penalty F is a function of β. In other words, we model the case in which the more effort the e-tailer makes, the lower the penalty fee it faces. Comparing to the findings under Model NG, we first uncover that the results of the basic models stay robust. After that, we compare the performance of the fixed penalty scheme (in basic models) and the defense-level dependent penalty scheme. Our analysis shows that when the cost for cyber-security is sufficiently low, when the consumers become more sensitive to cyber-security or the chance of being attacked increases, the government should choose the fixed penalty scheme. This finding shows that despite simple, the fixed penalty scheme is in fact a useful method which can outperform the defense-level dependent penalty scheme. Governments should hence consider it.

6. Conclusion

Cyber-security is a critical issue nowadays but it is under-explored in the OM literature. Motivated by observed real-world practices, we have built formal analytical models to explore the value of government cyber-security penalty schemes under different settings, e.g., including the use of systems security enhancing technologies (Section 5.1) and others (in Section 5.2, e.g., alliance, competing e-tailers, government's defense-level dependent penalty). In the basic models, we have considered the two situations of an e-commerce supply chain with and without the consideration of a government cyber-security penalty scheme (Model G and Model NG, respectively). We have found that the government's penalty scheme will always benefit the supplier and consumers but hurt the e-tailer. We have analytically proven (with the bounds derived) that when the government's emphasis on consumer surplus is sufficiently high, implementing the penalty scheme is beneficial

to social welfare. We have also found that once the government has decided to implement the penalty scheme, the optimal penalty should be a very heavy fine (which goes to the upper bound). Then we have extended the analysis to examine how adopting technologies such as blockchain will affect the government's choice of imposing penalty. We have revealed that when it is beneficial to have government's penalty scheme, if the unit technology operations cost is lower (higher) than the unit benefit brought to consumers, the optimal penalty will be lower (higher) after adopting technologies. To generate more insights, we have conducted further analyses for various extended modeling cases and found that our main results remain robust. Among other findings, we have proven that the formation of alliance is an effective way to increase cyber security. This is hence a good option in case governments find that imposing penalty as a way to increase cyber security is not beneficial to social welfare. Last but not least, we have found that the government penalty schemes may do more harm than good; while once it is beneficial to implement, the government should charge the heaviest fine. This finding may explain a common observation: In the real-world, governments basically always adopt a polarized strategy, i.e., either do not impose penalty or impose a super heavy penalty, on cyber-security issues.

Our findings have various practical implications and offer managerial insights, including some guidance for industrialists and governments on cyber-security issues.

When should the government impose the cyber-security penalty scheme: Our analytical results show that the government's implementation of cyber-security penalty scheme is beneficial to the supplier and consumers, but always hurts the e-tailer. We know that implementing the cyber-security penalty scheme is beneficial to improving social welfare only for the government which is characterized by having a sufficiently high emphasis on consumer surplus. This explains why some countries such as the UK and European Union implement cyber-security penalty schemes as they are well-known to have very high respects to consumer benefits. Just on the contrary, some governments of cities/countries (like China and New York) do not impose any penalty on cyber-security. Based on the analytical findings, we guess that one probable reason may be because compared to, e.g., economic benefits (i.e., profits of supply chain members), they don't pay much attention to consumer benefits in a relative sense. For example, maybe in New York, company profit is regarded relatively important, then there is no cybersecurity penalty. As of today (September 2021), one of the reasons why there is no cybersecurity penalty issue in China may be that the government focuses more on economic development and the interests of companies are relatively important. It is interesting to note that China is now talking about imposing heavy and strict cyber-security measures. According to our findings, this may mean that the government of China has changed to put more emphasis on consumers (than before) and hence the relevant legislations are now under way.

The optimal penalty scheme: From our analyses, if it is beneficial to implement the cyber-security penalty scheme, then the government should set the very heavy fine. This is in fact in line with the observed real world practices in which, e.g., European Union imposed a super high penalty on cyber-security problems. The same for the UK's case. Imposing a very heavy penalty on cyber-security problems is hence a scientifically sound practice.

What if it is not beneficial to have the cyber-security penalty scheme: From the above findings, we can

see that in the real-world, governments either do not impose penalty or impose a super heavy penalty on cyber-security issues. Then, for the situation in which it is not beneficial for the government to implement cyber-security penalty, then what will be some alternative measures? In our extended analyses, we have shown the importance of encouraging the e-tailer and suppler to form a strategic alliance. Our analysis (see Theorem A1.1 and A1.2 in E-Companion) has shown that establishing an alliance strategy is an essential measure in achieving an all-win situation and governments should not ignore its importance. This finding also supports the common observations that e-commerce supply chain members love to establish strategic alliance (as evidenced by the cases of Amazon.com and JD.com). This industrial practice is indeed wise and helpful in e-commerce environments with cyber-security considerations.

Using systems security enhancing technologies (such as blockchain): From the supply chain perspective, if governments only implement penalty schemes, e-tailers and the profits of the whole supply chain will be affected. If the benefit brought to consumers with the use of systems security enhancing technologies (such as blockchain) is greater than the per unit technology operations cost and the fixed technology cost is relatively small, the adoption of technologies will be a good choice. It is also interesting to note that when it is beneficial to have the government penalty scheme, the presence of systems security enhancing technologies also affects the optimal penalty and the specific impact depends on the technology benefit-to-cost ratio (BCR). When $BCR > 1$, then the optimal penalty is smaller after adopting technologies. Otherwise, if $BCR < 1$, then the optimal penalty is larger after technology adoption. This implies that the implementation of systems security enhancing technologies like blockchain not only affects the optimal cyber-security level but also the optimal penalty that will be charged (if the government has decided to implement the penalty scheme).

A limitation of our study is that we do not consider a situation involving multiple competing e-tailers in the supply chain system with different substitutability coefficients. In future studies, applying the β-related government penalty scheme to e-tailers under competition (Ha et al. 2017) would thus be valuable. Investigating how the technology adoption may improve cyber-security in a competitive environment is also an interesting future research direction. In this paper, we consider the symmetry of information and postpone the asymmetry case in the future research. Last but not least, extending the analysis to reveal how the risk-averse attitudes of e-tailers may affect their investments in cyber-security would also be an interesting direction to explore.

Acknowledgments

The authors sincerely thank the editors and reviewers for their kind and helpful advice. They are indebted to Neil Feng, Jerry Shen, Yami Sun, Katy Wang, and Kelly Xu for their comments on the earlier drafts of this paper. Tsan-Ming Choi's research is supported by Yushan Fellow Program (NTU-110VV012). Suyuan Luo's research is partly supported by the National Natural Science Foundation of China under Grant 72101159 and in part by the Ministry of Education in China (MOE) Project of Humanities and Social Sciences under Grant 20YJC630092. Tsan-Ming Choi is the corresponding author of this paper.

References

Abhishek, V., K. Jerath, Z.J. Zhang. 2016. Agency selling or reselling? channel structures in electronic retailing. *Management Science* 62(8), 2259-2280.

Arya, A., B. Mittendorf. 2015. Supply chain consequences of subsidies for corporate social responsibility. *Production and Operations Management* 24(8), 1346-1357.

Babich, V., G. Hilary. 2019. Distributed ledgers and operations: What operations management researchers should know about blockchain technology. *Manufacturing & Service Operations Management* 22(2), 223-240.

Bensoussan, A., V. Mookerjee, W.T. Yue. 2020. Managing information system security under continuous and abrupt deterioration. *Production and Operations Management* 29(8), 1894-1917.

Berenguer, G., Q. Feng, J.G. Shanthikumar, L. Xu. 2017. The effects of subsidies on increasing consumption through for-profit and not-for-profit newsvendors. *Production and Operations Management* 26(6), 1191-1206.

Bier, V., A. Gutfraind. 2019. Risk analysis beyond vulnerability and resilience–characterizing the defensibility of critical systems. *European Journal of Operational Research* 276(2), 626-636.

Cai, G. 2010. Channel selection and coordination in dual-channel supply chains. *Journal of Retailing* 86(1), 22-36.

Cai, Y.J., T.M. Choi, J. Zhang. 2021. Platform supported supply chain operations in the blockchain era: Supply contracting and moral hazards. *Decision Sciences* 52(4), 866-892.

Carrillo, J.E., A.J. Vakharia, R. Wang. 2014. Environmental implications for online retailing. *European Journal of Operational Research* 239(3), 744-755.

Cheung, K. F., M.G. Bell. 2019. Attacker–defender model against quantal response adversaries for cyber security in logistics management: An introductory study. *European Journal of Operational Research* 291(2), 471-481.

Cheung, K. F., M. G. Bell. 2021. Improving connectivity of compromised digital networks via algebraic connectivity maximisation. *European Journal of Operational Research* 294(1), 353-364.

Choi, T.M., S. Guo, N. Liu, X. Shi. 2020. Optimal pricing in on-demand-service-platform-operations with hired agents and risk-sensitive customers in the blockchain era. *European Journal of Operational Research* 284(3), 1031-1042.

Choi, T.M., S. Kumar, X. Yue, H.L. Chan. 2021. Disruptive technologies and operations management in the Industry 4.0 era and beyond. *Production and Operations Management*, published online (DOI: 10.1111/poms.13622).

Choi, T.M., S. Luo. 2019. Data quality challenges for sustainable fashion supply chain operations in emerging markets: Roles of blockchain, government sponsors and environment taxes. *Transportation Research Part E* 131, 139-152.

Choi, T.M., X. Shi. 2021. On-demand-ride-hailing-service platforms with hired drivers during coronavirus (COVID-19) outbreak: Can blockchain help? *IEEE Transactions on Engineering Management*, in press.

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

Cohen, M. A., H.L. Lee. 2020. Designing the right global supply chain network. *Manufacturing & Service Operations Management* 22(1), 15-24.

Cohen, M.C. 2018. Big data and service operations. *Production and Operations Management* 27(9), 1709-1723.

Cui, R., M. Li, S. Zhang. 2021. AI and Procurement. *Manufacturing & Service Operations Management*, published online: https://doi.org/10.1287/msom.2021.0989

Doroudi, S., T. Avgerinos, M. Harchol-Balter. 2021. To clean or not to clean: Malware removal strategies for servers under load. *European Journal of Operational Research* 292(2), 596-609.

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

Guha, S., S. Kumar. 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.

Ha A.Y., Q. Tian, S. Tong. 2017. Information sharing in competing supply chains with production cost reduction. *Manufacturing & Service Operations Management* 19(2), 246-262.

Hagiu, A., J. Wright. 2015. Marketplace or reseller? *Management Science* 61(1), 184-203.

Hao, L., M. Fan. 2014. An analysis of pricing models in the electronic book market. *MIS Quarterly* 38(4), 1017-1032.

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

Hsu, V.N., G. Lai, G. Liang. 2019. Agricultural partnership for dairy farming. *Production and Operations Management* 28(12), 3042-3059.

Hua, Z., W. Chen, Z.G. Zhang. 2016. Competition and coordination in two-tier public service systems under government fiscal policy. *Production and Operations Management* 25(8), 1430-1448.

Ji, Y., S. Kumar, V. Mookerjee. 2016. When being hot is not cool: Monitoring hot lists for information security. *Information Systems Research* 27(4), 897-918.

Khouzani, M., Z. Liu, P.Malacaria. 2019. Scalable min-max multi-objective cyber-security optimisation over probabilistic attack graphs. *European Journal of Operational Research* 278(3), 894-903.

Kim, B. C., P. Y. Chen, T. Mukhopadhyay. 2011. The effect of liability and patch release on software security: The monopoly case. *Production and Operations Management* 20(4), 603-617.

Kuruzovich, J., H. Etzion. 2018. Online auctions and multichannel retailing. *Management Science* 64(6), 2734-2753.

Kwark, Y., J. Chen, S. Raghunathan. 2017. Platform or wholesale? A strategic tool for online retailers to benefit from third-party information. *MIS Quarterly* 41(3), 763-785.

Li, L. 2002. Information sharing in a supply chain with horizontal competition. *Management science 48*(9), 1196-1212.

Li, M., L. Zhu, X. Lin. 2018. Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing. *IEEE Internet of Things Journal* 6(3), 4573-4584.

Li T., S.P. Sethi. 2016. A review of dynamic Stackelberg game models. *Discrete & Continuous Dynamical Systems-B* 22(1), 125.

Liang, R., J. Wang, M. Huang, Z.Z. Jiang. 2020. Truthful auctions for e-market logistics services procurement with quantity discounts. *Transportation Research Part B: Methodological* 133, 165-180.

Lim, S.F.W.T., J.S. Srai. 2018. Examining the anatomy of last-mile distribution in e-commerce omnichannel retailing. *International Journal of Operations & Production Management* 38(9), 1735-1764.

Luo, S., T.M. Choi. 2021. Great partners: how deep learning and blockchain help improve business operations together. *Annals of Operations Research*, published online: https://doi.org/10.1007/s10479-021-04101-4.

Nagurney, A., S. Shukla. 2017. Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research* 260(2), 588-600.

Niu, B., F. Xie, L. Chen, X. Xu. 2019. Join logistics sharing alliance or not? Incentive analysis of competing e-commerce firms with promised-delivery-time. *International Journal of Production Economics*, 107553.

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

Pun, H., P. Hou. 2021. Combating copycatting from emerging market suppliers in global supply chains, working paper.

Paul, J. A., M. Zhang. 2021. Decision support model for cybersecurity risk planning: A two-stage stochastic programming framework featuring firms, government, and attacker. *European Journal of Operational Research* 291(1), 349-364.

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

Ru, J., R. Shi, J. Zhang. 2018. When does a supply chain member benefit from vendor‐managed inventory? *Production and Operations Management* 27(5), 807-821.

Scholz, M., V. Dorner, G. Schryen, A. Benlian. 2017. A configuration-based recommender system for supporting e-commerce decisions. *European Journal of Operational Research* 259(1), 205-215.

Shen, B., C. Dong, S. Minner. 2021. Combating copycats in the supply chain with permissioned blockchain technology. *Production and Operations Management*, published online: https://doi.org/10.1111/poms.13456

Shen, Y., S. P. Willems, Y. Dai. 2019. Channel selection and contracting in the presence of a retail platform. *Production and Operations Management* 28(5), 1173-1185.

Shetty, N., G. Schwartz, M. Felegyhazi, J. Walrand. 2010. Competitive cyber-insurance and internet security. In *Economics of Information Security and Privacy*. New York: Springer US, 229-247.

Simon, J., A. Omar. 2020. Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research* 282(1), 161-171.

Swaminathan, J.M. 2018. Big data analytics for rapid, impactful, sustained, and efficient (RISE) humanitarian operations. *Production and Operations Management* 27 (9), 1696-1700.

Tan, Y.R., J.E. Carrillo. 2017. Strategic analysis of the agency model for digital goods. *Production and Operations Management* 26(4), 724-741.

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

Tian, L., A.J. Vakharia, Y.R. Tan, Y. Xu. 2018. Marketplace, reseller, or hybrid: Strategic analysis of an emerging e-commerce model. *Production and Operations Management* 27(8), 1595-1610.

Tsay, A.A., N. Agrawal. 2004. Channel conflict and coordination in the e-commerce age. *Production and Operations Management* 13(1), 93-110.

Wang, C., X. Fan, Z. Yin. 2019. Financing online retailers: Bank vs. electronic business platform, equilibrium, and coordinating strategy. *European Journal of Operational Research* 276(1), 343-356.

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

Wu, H., G. Cai, J. Chen, C. Sheu. 2015. Online manufacturer referral to heterogeneous retailers. *Production and Operations Management* 24(11), 1768-1782.

Wu, Y., G. Feng, R.Y.K. Fung. 2018. Comparison of information security decisions under different security and business environments. *Journal of the Operational Research Society* 69(5), 747-761.

Xiao, W., Y. Xu. 2018. Should an online retailer penalize its independent sellers for stockout? *Production and Operations Management* 27(6), 1124-1132.

Xu, J., V.N. Hsu, B. Niu. 2018. The impacts of markets and tax on a multinational firm's procurement strategy in China. *Production and Operations Management*, 27(2), 251-264.

Yan, Y., R. Zhao, T. Xing. 2019. Strategic introduction of the marketplace channel under dual upstream disadvantages in sales efficiency and demand information. *European Journal of Operational Research* 273(3), 968-982.

Yang, M., V. S. Jacob, S. Raghunathan. 2021. Cloud service model's role in provider and user security investment incentives. *Production and Operations Management* 30(2), 419-437.

Yu, J.J., C.S. Tang, Z.J.M. Shen. 2018. Improving consumer welfare and manufacturer profit via government subsidy programs: subsidizing consumers or manufacturers? *Manufacturing & Service Operations Management* 20(4), 752-766.

Zhang, F., R. Zhang. 2018. Trade-in remanufacturing, customer purchasing behavior, and government policy. *Manufacturing & Service Operations Management* 20(4), 601-616.

Zhang, S., J. Zhang. 2020. Agency selling or reselling: E-tailer information sharing with supplier offline entry. *European Journal of Operational Research 280*(1), 134-151.

Zhang, T., T.M. Choi. 2021. Optimal consumer sales tax policies for online-offline retail operations with consumer returns. *Naval Research Logistics* 68 (6), 701-720.

Zhang, X., Y. Yao. 2020. How much is too much? The effect of offline call intensity on online purchase of digital services. *Production and Operations Management* 29(3), 509-525.

Appendix:

Table 1.1b. Some real-world cases of cyber-security fines[20]

Real-world cases	Details of penalty
Equifax (2017 data breach)	$575 million.
British Airways (2018 data breach)	the UK Information Commissioner's Office ("ICO") fined BA $230 million.
Uber (2016 data breach)	Instead of quietly going away, the rideshare company was hit with a $148 million fine for violation of data breach notification laws.
Marriott International (2018 data breach)	On July 9, 2019, the ICO announce that the breach resulted in a fine of £99,200,396 (approximately $124 million).
Yahoo (2013 security breach)	This breach cost Yahoo $85 million.
Capital One (2019 data breach)	The bank suffered a fine of $80 million.
Google violated the GDPR in2019.	This cybersecurity issue cost Google the equivalent of $43 million.
Alibaba (Ant Group 2021)	Chinese regulators have fined Alibaba a record $2800 million. Ant agreed to strengthen the protection of personal information and effectively prevent the abuse of data.[21]
Didi Global Inc. (2021)	Bloomberg claims that Chinese regulators are considering serious, perhaps unprecedented, penalties for Didi, which is likely to impose harsher sanctions on Didi than on Alibaba.[22]

Table 1.2. Features of cyber-security of e-commerce platforms

Features	Details	Related Model Settings
Consumer's concerns for security	Online consumers provide their private information, including their names, addresses, and possibly their credit card details and other types of financial information. This exposes their information to serious dangers if the e-commerce platforms are not secure. They risk having their private information stolen. Cyber-security is hence critical.	This feature is reflected in the demand function in which consumers sensitivity to cyber-attacks is present.
Cyber-attack's impacts	Cyber-attacks can compromise users' privacy and may be disastrous for the companies involved as previous mentioned. It is critical and important to defend against cyber-attack.	β denotes the e-tailer's level of defense effort, and an associated cost $K_{DE}(\beta)$ is incurred.
Penalty measures	Unlike other "crimes", some governments have imposed very heavy penalty rules on cyber-security while some haven't. It is hence interesting to explore whether governments should impose penalty and play a role in cyber-security issues or not.	We take government penalty schemes into consideration and compare scenarios with and without governments.
Alliance	In e-commerce, it is widely reported that e-tailers form strategic alliance with their suppliers. Typical examples include Amazon.com and JD.com. Whether or not it is a wise measure to deal with cyber-security challenge deserves deep investigations	In our extended models, we compare the role played by alliance and show that it is critically important.

[20] https://www.statista.com/statistics/1170520/worldwide-data-breach-fines-settlements/ (accessed July 20, 2021)
[21] https://www.ft.com/content/bb251dcc-4bff-4883-9d81-061114fee87f (accessed August 1, 2021)
[22] https://www.bloomberg.com/news/articles/2021-07-22/china-is-said-to-weigh-unprecedented-penalty-for-didi-after-ipo (accessed August 1, 2021)