Research Article

Information Security Decisions with Consideration of Hacker Intrusion Propagation

Liurong Zhao,1,2 Xinyu Zhou,2 and Jiao Li2

1School of Management and Engineering, Nanjing University, Nanjing 210008, China
2School of Economics and Management, Nanjing Tech University, Nanjing 211816, China

Correspondence should be addressed to Liurong Zhao; zhaolr_njtech@163.com

Received 7 January 2022; Revised 3 June 2022; Accepted 24 June 2022; Published 31 August 2022

Copyright © 2022 Liurong Zhao et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The spread of network attacks is extremely harmful, which poses a great threat to the assets and reputation of firms. Therefore, making a scientific information security strategy is an important task for the continued and stable development of the firms. This paper develops the SIR model of hacker intrusion propagation and then analyzes the evolution trend of hacker intrusion propagation and the conditions of strategy transfer. The research shows that when immune failure and strategy transfer are not considered, the threshold of hacker intrusion propagation is negatively correlated with the probability of invasion, whereas it is positively correlated with the probability of defense success and the externality during outsourcing. In the case of immune failure, there will always be infected firms in the network, where the threshold of hacker intrusion propagation is affected by the proportion of the infected state and the probability of immune failure. When immune failure and strategy transfer occur simultaneously if the externality is positive and high, information security outsourcing can improve firms’ security benefits; if the externality is negative, the firms should stop cooperating with the managed security service provider (MSSP).

1. Introduction

With the rapid development of economic globalization, collaboration between firms has become usual. However, cooperation improves the efficiency, it also brings potential risks to firms’ information security. The interdependence among different information systems is exploited by hackers to attack affiliated firms. For example, software of the firms’ information systems increasingly relies on the development tools or software modules of the third-party development platform. Once there are security vulnerabilities in these tools or modules (especially open-source software), hackers will successfully invade the third-party development platform and then attack the firms’ information system. Positive Technologies reported that hackers penetrated one firm’s network and used it as a gangplank that pointed to penetrate the other firms’ information systems [1]. To address the complex network security problems, firms usually enhance their security through two measures, i.e., autonomous defense and outsourcing information security services [2]. Compared with autonomous defense, although outsourcing information security services have certain advantages in more professional technology and lower management cost, the firms’ information systems security will rely on MSSP’s security protection system. Once the information systems of MSSP or firms are invaded, hackers will attack the affiliated organizations based on this interdependence, which will lead to security externalities [3]. For example, if MSSP prevents hackers from invading one customer firm, it has the successful preventing experience for such attacks so as to better serve other firms that purchase its outsourced services, which is a positive security externality from outsourcing information security strategy. Therefore, some firms are more willing to shift from autonomous defense to outsourcing strategy. However, if hackers successfully invade the firms or MSSP, the interdependence among different information systems will increase the security risk of affiliated organizations, which is a negative security externality from outsourcing information security strategy; thus, some firms may give up the corporations with MSSP.
Nowadays, studies on hacker intrusion behavior and firms’ information security strategies have recently become a research hotspot in complex network environments.

Hackers’ intrusion behavior includes embedding computer viruses [4], disseminating malware distribution [5], and launching DDoS attacks [6]. The influences of hacker intrusion on firms’ information sharing decision from the perspective of economics are studied recently. Gao and Zhong [7] explored the effect of attack level, firms’ information sharing and security technology investment on profits, and customer needs under hackers’ targeted attacks. Hausken [8] showed that the attack level is irrelevant with the efficiency of information sharing, but hackers’ information sharing level decreases with the increase of firm’s security investment [9]. On the basis, he also concluded that hackers improve their attack level by sharing vulnerability information of the firms’ information systems. In addition, there are some studies concentrated on the hackers’ intrusion behavior based on cellular automata. For example, Gagliardi and Alves [10] studied the influence of the small world on the effect of hacking behavior by structuring the CA model. The propagation behavior of network malware was studied based on the CA model as well [11, 12]. However, the CA model cannot reflect the average trend of hacker intrusion propagation and cannot make general predictions [13]. To sum up, the current research mainly focuses on analyzing hacker intrusion behavior by game model and CA model but lacks the mechanism of hacker intrusion diffusion. SIR model is a classical model to describe the mechanism of information diffusion. It can not only study the dynamics diffusion process but also position the key nodes and analyze the threshold of virus propagation [14–17]. The diffusion characteristics of computer network viruses are similar to those of biological viruses, which are latent, infectious, and destructive; thus, the evolution of virus infection among network nodes can be considered, and the SIR model is used to analyze the computer virus diffusion [18–22]. SIR model is introduced to study the mechanism of hacker intrusion diffusion, which has certain innovative significance.

Prior research on the information security strategy largely focuses on information security investment behavior, technology configuration, and security service outsourcing. For example, Qian et al. [23] developed an information security investment game model of affiliated firms considering the different probabilities of hacker intrusion. He also examined the optimal information security investment strategy based on security insurance [24]. Research in many domains has addressed information security technology configuration, such as IDS, firewall, and honeypot. For example, in economics, Smirnova and Smirnova [25] proposed the optimal configuration of intrusion detection systems when firms chose the strategy of autonomous defense and showed that the impact of IDS quality, cost structure, and strategic behavior of hackers are the main factors in the defense effect. Since security outsourcing is an emerging strategy in the field of information security management, there are few researches on this topic at present. Wu et al. [26], discussed the impact of positive and negative externalities on the information security effect and proposed an information security outsourcing contract. Some scholars concentrated on the incentive mechanism of security outsourcing and the risk of information disclosure, and discussed the security game between hackers, MSSP, and firms [27, 28]. The existing research on information security decision-making mainly focuses on the decision-making of information security within the firm and rarely considers the evolution of information security strategy between affiliated organizations due to the externality of information security outsourcing caused by interdependence. In fact, with the dynamic changes of hacker intrusion diffusion and security externality, the evolution of firms’ security status leads to adjust their security strategies. SIR model can effectively analyze the decision interaction of agents in network systems. Therefore, considering the conditions of hacker intrusion diffusion and security externalities, we develop an extended SIR model to analyze the evolution trend of hacker intrusion diffusion and the conditions of choosing strategy transfer, which is another innovation of this paper. Based on our results, it has theoretical supplementary value to the economics of information security.

This study is presented as follows. Section 2 explains the assumptions of the SIR model and introduces hacker intrusion propagation. Section 3 studies three information security strategies: without considering immune failure and strategy transfer, only considering immune failure, and considering both immune failure and strategy transfer. Section 4 presents numerical simulations to extend the conclusions. Managerial implications are discussed in Section 5.

2. The Model

2.1. Description of the Model. Based on the SIR model, network security includes susceptible state (S), infected state (I), and recovered state (R), in which S indicates that firms have not been invaded but are at risk of being invaded, I indicates that firms have been invaded, and R indicates that firms have successfully defended against cyberattacks or recovered from attacks to a safe state. Firms choose one of two information security strategies, autonomous defense or outsourcing, to prevent the attacks. $S_1$, $I_1$, and $R_1$ denote the firms’ susceptible state, infected state, and recovered state, respectively, when they implement autonomous defense; $S_2$, $I_2$, and $R_2$ denote the firms’ susceptible state, infected state, and recovered state, respectively, when they choose information security outsourcing.

Suppose that there are $N$ nodes in the network, and each node represents a firm. If firms choose the strategy of autonomous defense, the probability of invasion is $\lambda_1$, where the firms’ security state changes from $S_1$ to $I_1$ after successful invasion. In this case, the probability of resisting invasion is $1 - \lambda_1$, where the firms’ security state changes from $S_1$ to $R_1$ after successful defense. After firms have been invaded, the probability of information systems recovery is $\beta_1$, where the firms’ security state changes from $I_1$ to $R_1$. After firms successfully defend against intrusion or recover their information systems, hackers can still target them and...
continue to attack. In this situation, the probability of reinvasion is \( \gamma_1 \), where the firms’ security state changes from \( R_1 \) to \( I_1 \). We define “firms’ immune failure” as the security state change from “immune” to “infection.” Likewise, if firms choose the strategy of information security outsourcing, there are similar explanations for parameters such as \( \lambda_2 \), \( \beta_2 \), and \( \gamma_2 \) and changes of security states. Furthermore, the security externality \( \theta (-1 \leq \theta \leq 1) \) is a phenomenon coming from the interdependence between information systems. To be specific, positive externality \( \theta > 0 \) or negative externality \( \theta < 0 \), respectively, has a positive or negative effect on information security levels. When the strategy of information security outsourcing is implemented, the probability of invasion under the condition of externality is \((1-\theta)\lambda_2\), where firms’ security state changes from \( S_2 \) to \( I_2 \). Similarly, the probability of state transfer from \( S_2 \) to \( R_2 \) is \((1+\theta)(1-\lambda_2)\), the probability of state transfer from \( I_2 \) to \( R_2 \) is \((1+\theta)\beta_2\), and the probability of state transfer from \( R_2 \) to \( I_2 \) is \((1-\theta)\gamma_2\). It is worth noting that the service ability of MSSP determines the quality of firms’ security products which affect the probability of invasion \( \lambda_2 \), the probability of information systems recovery \( \beta_2 \), the probability of re-invasion \( \gamma_2 \), and the security externality \( \theta \). After firms are invaded, they are dissatisfied with the existing security strategy and may change their information security strategy. We call this process of strategy change “strategy transfer.” \( \phi_1 \) is the proportion of firms transferring from autonomous defense to outsourcing strategy after hackers invade; \( \phi_2 \) is the proportion of firms transferring from the strategy of outsourcing to autonomous defense. Based on the above, Figure 1 shows the state evolution of process firms after hacker intrusion.

2.2. SIR Model of Hacker Intrusion Propagation. According to the model assumptions and the rules of state transfer, invaded firms and their affiliated firms constitute a social network. The SIR model of intrusion propagation can be expressed as follows:

\[
\frac{d(S_1)}{dt} = -\lambda_1 S_1(t) I_1(t) - (1-\lambda_1) S_1(t) I_1(t). \tag{1}
\]

\[
\frac{d(I_1)}{dt} = \lambda_1 S_1(t) I_1(t) - \phi_1 I_1(t) + \phi_2 I_2(t) - \beta_1 ((1-\phi_1) I_1(t) + \phi_2 I_2(t)) + \gamma_1 R_1(t). \tag{2}
\]

\[
\frac{d(R_1)}{dt} = (1-\lambda_1) S_1(t) I_1(t) + \beta_1 ((1-\phi_1) I_1(t) + \phi_2 I_2(t)) - \gamma_1 R_1(t). \tag{3}
\]

\[
\frac{d(S_2)}{dt} = -(1-\theta)\lambda_2 S_2(t) I_2(t) - (1+\theta)(1-\lambda_2) S_2(t) I_2(t). \tag{4}
\]

\[
\frac{d(I_2)}{dt} = \lambda_2 S_2(t) I_2(t) - \phi_1 I_2(t) + \phi_2 I_2(t) - \beta_2 ((1-\phi_1) I_2(t) + \phi_2 I_2(t)) + \gamma_2 R_2(t). \tag{5}
\]

\[
\frac{d(R_2)}{dt} = (1-\lambda_2) S_2(t) I_2(t) + \beta_1 ((1-\phi_1) I_2(t) + \phi_2 I_2(t)) - \gamma_2 R_2(t). \tag{6}
\]

where \( S_1(t) \), \( I_1(t) \), and \( R_1(t) \), respectively, represent the proportion of susceptible state, infected state, or recovered state relative to the total firms in the network when they implement the strategy of autonomous defense at the time \( t \); similarly, \( S_2(t) \), \( I_2(t) \), and \( R_2(t) \), respectively, represent that of when they implement the strategy of information security outsourcing at the time \( t \), where \( S_1(t) + I_1(t) + R_1(t) = S_2(t) + I_2(t) + R_2(t) = 1 \).

3. Steady-State Analysis

3.1. Steady-State Analysis without considering Immune Failure and Strategy Transfer. First, we assume that the strategy of autonomous defense can resist attacks successfully. In other words, the firms’ security state does not change from \( R \) to \( I \). Meanwhile, firms will not change their minds after adopting this strategy. In this case, there are \( \gamma_1 = \gamma_2 = 0 \) and \( \phi_1 = \phi_2 = 0 \), and substitute them into equations (1), (2), (4), and (5). We can yield

\[
\frac{dI_1}{dS_1} = \frac{\lambda_1 S_1(t) I_1(t) - \beta_1 I_1(t)}{-S_1(t) I_1(t)} = -\lambda_1 + \frac{\beta_1}{S_1(t)}. \tag{7}
\]

\[
\frac{dI_2}{dS_2} = \frac{\lambda_2 (1-\theta) S_2(t) I_2(t) - (1+\theta) \beta_2 I_2(t)}{-1 - 2\lambda_2 \theta + \theta} = \frac{\lambda_2 (1-\theta) I_2(t)}{1 - 2\lambda_2 \theta + \theta} S_2(t). \tag{8}
\]
\[
\begin{align*}
    f(S_1) &= -\lambda_1 S_1 + \beta_1 \ln \left( \frac{S_1}{S_0} \right) + (\lambda_1 S_0 + I_0). \\
    f(S_2) &= -\lambda_2 (1 - \theta) S_2 + (1 + \theta) \beta_2 \left( 1 - 2\lambda_2 \theta + \theta \right) \ln \left( \frac{S_2}{S_0} \right) \\
    &\quad + \left( \lambda_2 (1 - \theta) - (1 - 2\lambda_2 \theta + \theta) S_0 + I_0 \right).
\end{align*}
\]

where \( S_0 \) and \( I_0 \), respectively, represent the proportion of initial susceptible state and infected state relative to total firms in the network when they are at the beginning of the invasion. Then, the variation trend of \( S_1 \) with \( S_2 \) is studied, and the threshold of intrusion propagation is calculated subsequently. Next, it is necessary to analyze the monotonicity of \( f(S_1) \) and \( f(S_2) \).

Let \( f'(S_1) > 0 \) and \( f'(S_2) > 0 \), and the monotonicity of \( f(S_1) \) and \( f(S_2) \) are as follows: if \( S_1 \in (0, \beta_1 / \lambda_1) \), then \( f'(S_1) > 0 \); if \( S_1 \in (\beta_1 / \lambda_1, 1) \), then \( f'(S_1) < 0 \). If \( S_2 \in (0, (1 + \theta) \beta_2 / (1 - \theta) \lambda_2) \), then \( f'(S_2) > 0 \); if \( S_2 \in ((1 + \theta) \beta_2 / (1 - \theta) \lambda_2, 1) \), then \( f'(S_2) < 0 \).

Based on reality, the intrusion will propagate only when the proportion of infected firms increases. The threshold of intrusion propagation is \( \beta_1 / \lambda_1 \) when firms implement the strategy of autonomous defense; i.e., the intrusion will propagate only when \( S_0 > \beta_1 / \lambda_1 \). Similarly, the threshold of intrusion propagation is \( (1 + \theta) \beta_2 / (1 - \theta) \lambda_2 \) when firms implement the strategy of outsourcing; i.e., the intrusion will propagate only when \( S_0 > (1 + \theta) \beta_2 / (1 - \theta) \lambda_2 \). We can derive that \( f(S_1) \) and \( f(S_2) \) tend to be 0 with decreasing \( S_0 \). Furthermore, the firms’ ability to resist risk will increase with a higher threshold of intrusion propagation. Meanwhile, the threshold of intrusion propagation is positively correlated with both the probability of information systems recovery \( \beta_1 \) (or \( \beta_2 \)) and the externality \( \theta \), and negatively correlated with the probability of invasion \( \lambda_1 \) or \( \lambda_2 \). This means that if the MSSP has a high level of service ability to provide the firms high quality of security products, it can effectively reduce the probability of successful intrusion by hackers, improve the probability of successful repair after intrusion, and increase the positive security externality, so as to increase the threshold of intrusion propagation and enhance the ability of firms to resist risks.

Hereafter, we compare the thresholds of intrusion propagation with the two different security strategies. Let \( \lambda_1 = \lambda_2 = \lambda \), \( \beta_1 = \beta_2 = \beta \), and then \( (1 + \theta) \beta / (1 - \theta) \lambda - \beta / \lambda = 2 \theta \beta / (1 - \theta) \lambda \). We can obtain that \( 2 \theta \beta / (1 - \theta) \lambda > 0 \) if \( \theta > 0 \) and vice versa. In other words, when the externality is positive, the strategy of outsourcing will increase the threshold of intrusion propagation; otherwise, it will decrease the threshold of intrusion propagation.

To conclude this section, we came to the following conclusions without considering immune failure and strategy transfer.

**Conclusion 1.** If firms implement the strategy of autonomous defense, the threshold of intrusion propagation is \( \beta_1 / \lambda_1 \); if firms implement the strategy of outsourcing, the threshold of intrusion propagation is \( (1 + \theta) \beta_2 / (1 - \theta) \lambda_2 \). Only when the propagation of the initial susceptible state is beyond the threshold, the intrusion will propagate. Furthermore, regardless of whether the intrusion propagates or not, the final proportion of firms in the infected state is 0.

**Conclusion 2.** When the externality is positive, the strategy of outsourcing can better restrain hacker intrusion propagation. Compared with the strategy of autonomous defense, the threshold of intrusion propagation increases by \( 2 \theta \beta / (1 - \theta) \lambda \). On the other hand, when the externality is negative, the strategy of outsourcing hard attains to expect the result. Compared with the strategy of autonomous defense, the threshold of intrusion propagation decreases by \( 2 \theta \beta / (1 - \theta) \lambda \).

### 3.2. Steady-State Analysis considering Immune Failure

Based on the SIR model in Section 3.1, we consider the situation of immune failure; that is, the security state can change from “immune state” to “infected state.” However, it is still not considered of information security strategy transfer (\( \phi_1 = \phi_2 = 0 \)), \( \gamma_1 \) is the probability of immune failure, in which the security state may change from \( R_1 \) to \( I_1 \), and \( \gamma_2 \) is the probability of immune failure, in which the security state may change from \( R_2 \) to \( I_2 \). Then, the SIR model is

\[
\begin{align*}
    d(I_1) &= \lambda_1 S_1(I_1(t) - \beta_1 I_1(t) + \gamma_1 R_1(t)) \\
    d(S_1) &= -\lambda_1 S_1(t)I_1(t) - (1 - \lambda_1)S_1(t)I_1(t) \\
    d(I_2) &= \lambda_2 S_2(I_2(t) - (1 + \theta)\beta_2 I_2(t) + \gamma_2 (1 - \theta)R_2(t)) \\
    d(S_2) &= -(1 - \theta)\lambda_2 S_2(t)I_2(t) - (1 + \theta)(1 - \lambda_2)S_2(t)I_2(t).
\end{align*}
\]

Similarly, to analyze the threshold of intrusion propagation when immune failure occurs, it is necessary to discuss the monotonicity of equation (7). According to \( d(I_1)/d(S_1) > 0 \), we obtain that

\[
S_1(\lambda_1 I_1 - \gamma_1) < (\beta_1 + \gamma_1)I_1 - \gamma_1. \tag{12}
\]

The threshold of intrusion propagation is changing with the variation of \( \lambda_1 I_1 - \gamma_1 \), and \( \beta_1 + \gamma_1 \). Hence, we need to examine the following six situations, respectively.

**Situation 1.** If \( \lambda_1 I_1 < (\beta_1 + \gamma_1)I_1 < \gamma_1 \), formula (13) can be simplified to \( (\beta_1 + \gamma_1)I_1 - \gamma_1 / (\lambda_1 I_1 - \gamma_1) < S_1 < 1 \), and we have the threshold of intrusion propagation \( \eta = (\beta_1 + \gamma_1)I_0 - \gamma_1 / (\lambda_1 I_0 - \gamma_1) \). When \( S_0 > \eta \), the intrusion does not propagate.

**Situation 2.** If \( \lambda_1 I_1 < \gamma_1 < (\beta_1 + \gamma_1)I_1 \), formula (13) can be simplified to \( (\beta_1 + \gamma_1)I_1 - \gamma_1 / (\lambda_1 I_1 - \gamma_1) < S_1 < 1 \). In this situation, no matter what the value \( S_0 \) is, the intrusion will never propagate.

**Situation 3.** If \( \gamma_1 < \lambda_1 I_1 < (\beta_1 + \gamma_1)I_1 \), formula (13) can be simplified to \( \gamma_1 < (\beta_1 + \gamma_1)I_1 - \gamma_1 / (\lambda_1 I_1 - \gamma_1) < S_1 < 1 \), and we have the threshold of intrusion propagation \( \eta = (\beta_1 + \gamma_1)I_0 - \gamma_1 / (\lambda_1 I_0 - \gamma_1) > 1 \). In this situation, no matter what the value \( S_0 \) is, the intrusion will never propagate.
Situation 4. If $\gamma_1 < (\beta_1 + \gamma_1)I_1 < \lambda_1 I_1$, formula (13) can be simplified to $S_1 < (\beta_1 + \gamma_1)I_0 - \gamma_1 / (\lambda_1 - \gamma_1) < 1$, and we have the threshold of intrusion propagation $\eta = (\beta_1 + \gamma_1)I_0 - \gamma_1 / (\lambda_1 I_0 - \gamma_1) < 1$. When $S_0 < \eta$, the intrusion does not propagate.

Situation 5. If $(\beta_1 + \gamma_1)I_0 < \gamma_1 < \lambda_1 I_0$, formula (13) can be simplified to $S < (\beta_1 + \gamma_1)I_0 - \gamma_1 / (\lambda_1 I_0 - \gamma_1) < 0$, and we have the threshold of intrusion propagation $\eta = (\beta_1 + \gamma_1)I_0 - \gamma_1 / (\lambda_1 I_0 - \gamma_1) < 0$. In this situation, no matter what the value $S_0$ is, the intrusion will always propagate.

Situation 6. If $(\beta_1 + \gamma_1)I_0 < \lambda_1 I_0 < \gamma_1$, formula (13) can be simplified to $1 < (\beta_1 + \gamma_1)I_0 - \gamma_1 / (\lambda_1 I_0 - \gamma_1) < S_1$, and we have the threshold of intrusion propagation $\eta = (\beta_1 + \gamma_1)I_0 - \gamma_1 / (\lambda_1 I_0 - \gamma_1) > 1$. In this situation, no matter what the value $S_0$ is, the intrusion will always propagate.

Similarly, when firms choose the strategy of outsourcing, we can discuss the similar six situations, respectively.

Situation 1. If $(1 - \theta)\lambda_1 I_2 < ((1 + \theta)\beta_2 + (1 - \theta)\gamma_2) I_2 < (1 - \theta)\gamma_2$, the intrusion will always propagate.

Situation 2. If $(1 - \theta)\lambda_2 I_2 < (1 - \theta)\gamma_2 < ((1 + \theta)\beta_2 + (1 - \theta)\gamma_2) I_2$, no matter what the value $S_0$ is, the intrusion will never propagate.

Situation 3. If $\lambda_1 I_2 < (1 - \theta)\lambda_1 I_2 < ((1 + \theta)\beta_2 + (1 - \theta)\gamma_2) I_2$, no matter what the value $S_0$ is, the intrusion will never propagate.

Situation 4. If $\gamma_2 < (1 + \theta)\beta_2 + (1 - \theta)\gamma_2 < (1 - \theta)\gamma_2$ or $I_2 < (1 - \theta)\lambda_2 I_2$, we have the threshold of intrusion propagation $\eta = (1 + \theta)\beta_2 + (1 - \theta)\gamma_2 / (1 - \theta)\lambda_2 I_2 - \gamma_2 < 1$. When $S_0 < \eta$, the intrusion does not propagate. When $S_0 > \eta$, the intrusion will first propagate at increasing speed and then slowly die out.

Situation 5. If $((1 + \theta)\beta_2 + (1 - \theta)\gamma_2) I_0 < (1 - \theta)\lambda_1 I_0$, no matter what the value $S_0$ is, the intrusion will always propagate.

Situation 6. If $((1 + \theta)\beta_2 + (1 - \theta)\gamma_2) I_0 < (1 - \theta)\lambda_2 I_0$, no matter what the value $S_0$ is, the intrusion will always propagate.

To conclude this section, we can drive the following conclusions when considering immune failure ($\gamma > 0$).

Conclusion 3. Infected firms always exist in the network when $\gamma > 0$.

Conclusion 4. When externality is positive, the overall trend of intrusion propagation is not changed, but if MSSP security ability prevents hackers from continuing attacks on affiliated organizations by the positive externality, it can reduce the proportion of infected firms and the scale of intrusion propagation.

Conclusion 5. If the strategy of autonomous defense is implemented, the intrusion will propagate when $(\beta_1 + \gamma_1)I_0 < \gamma_1 < \lambda_1 I_0$ or $(\beta_1 + \gamma_1)I_0 < \lambda_1 I_0$. On the contrary, the intrusion will not propagate when $\lambda_1 I_1 < \gamma_1 < (\beta_1 + \gamma_1)I_1 < \lambda_1 I_1$, or $\lambda_1 I_1 < (\beta_1 + \gamma_1)I_1 < \gamma_1$ and $S_0 > \eta$ or $\gamma_1 < (\beta_1 + \gamma_1)I_1 < \lambda_1 I_1$ and $S_0 < \eta$.

Conclusion 6. If the strategy of outsourcing is implemented, the intrusion will propagate when $((1 + \theta)\beta_2 + (1 - \theta)\gamma_2) I_0 < (1 - \theta)\lambda_2 I_2$, or $((1 + \theta)\beta_2 + (1 - \theta)\gamma_2) I_0 < (1 - \theta)\beta_2 + (1 - \theta)\gamma_2) I_2 < (1 - \theta)\gamma_2$. On the contrary, the intrusion will not propagate when $((1 - \theta)\lambda_2 I_2 < (1 - \theta)\gamma_2 < (1 + \theta)\beta_2 + (1 - \theta)\gamma_2) I_2$, or $((1 - \theta)\gamma_2 < (1 - \theta)\beta_2 + (1 - \theta)\gamma_2) I_2 < (1 - \theta)\gamma_2$ or $((1 + \theta)\beta_2 + (1 - \theta)\gamma_2) I_2 < (1 - \theta)\lambda_2 I_2$ and $S_0 < \eta$.

3.3. Steady-State Analysis considering Immune Failure and Strategy Transfer. Based on the SIR model in Section 3.2, we consider the situation of both immune failure and strategy transfer. In reality, firms compare the strategy advantages of autonomous defense and outsourcing combining the situation of intrusion propagation and then dynamically adjust the information security strategy to ensure information system security. For example, if intrusion propagation occurs, the externality is positive ($\theta > 0$), and firms may change their strategy from autonomous defense to outsourcing, which achieves the positive effects of externality. Alternatively, the externality is negative ($\theta < 0$), and firms may stop cooperating with MSSP to avoid the negative effects of externality.

3.3.1. Steady-State Analysis When the Externality Is Positive. Let $\varphi_2 = 0, \theta > 0$, the other parameters are unequal zero, and we can yield

\[
\frac{d(I_1)}{d(S_1)} = \frac{\lambda_1 S_1 (t) I_1 (t) - \varphi_1 I_1 (t) - \beta_1 (1 - \varphi_1) I_1 (t) + \varphi_1 R_1 (t)}{-\lambda_1 S_1 (t) I_1 (t) - (1 - \lambda_1) S_1 (t) I_1 (t)},
\]

\[
\frac{d(I_2)}{d(S_2)} = \frac{\lambda_2 S_2 (1 - \theta) I_2 (t) + \varphi_1 I_1 (t) - (1 + \theta) \beta_2 (1 - \varphi_1) I_1 (t) + \varphi_1 R_2 (t)}{- (1 - \theta) \lambda_2 S_2 (t) I_2 (t) - (1 + \theta) (1 - \lambda_2) S_2 (t) I_2 (t)}.
\]

\[
\eta_1 = \frac{(\varphi_1 (1 - \beta_1 - \gamma_1) + \varphi_1 + \gamma_1) I_1 - \eta_1}{(\lambda_1 I_1 - \gamma_1)}.
\]
When firms choose the strategy of outsourcing, the threshold of intrusion propagation is

$$\eta_2 = \frac{(1 + \theta)\beta_2 + (1 - \theta)\gamma_2 I_2 - (1 - \theta)\gamma_2 + ((1 + \theta)\beta_2 + (1 - \theta)\gamma_2 - 1)\phi_1 I_1}{(1 - \theta)(\lambda_1 I_2 - \gamma_2)}$$  \hspace{1cm} (15)$$

Suppose that all parameters are equal except $\theta$, the security level increases after the strategy transfer, and it should be satisfied $\eta_2 > \eta_1$, that is, $\eta_2 - \eta_1 = 2(\phi_1 + \theta)\beta I + 2\phi_1(1 - \theta)\gamma I - (2 - \theta)\phi I > 0$. It can be simplified to $\theta > 2\phi_1(1 - \gamma - \beta)/2\beta - 2\phi_1\gamma + \phi_1$. Then, the strategy transfer from autonomous defense to outsourcing will improve the security level of the firms.

### 3.3.2. Steady-State Analysis When the Externality Is Negative.

Let $\phi_1 = 0$, $\theta < 0$, the other parameters are unequal zero, and when firms choose the strategy of autonomous defense, the threshold of intrusion propagation is

$$\eta_1 = \frac{(\phi_2(\beta_1 - \gamma_1 - 1) + \beta_2 + \gamma_1)I_1 - \gamma_1}{(\lambda_1 I_1 - \gamma_1)}$$  \hspace{1cm} (16)$$

When firms choose the outsourcing strategy, the threshold of intrusion propagation is

$$\eta_2 = \frac{(1 + \theta)(1 - \phi_2)\beta_2 + (1 - \theta)(1 - \phi_2)\gamma_2)I_2 - (1 - \theta)\gamma_2 + \phi_2 I_2}{(1 - \theta)(\lambda_1 I_2 - \gamma_2)}$$  \hspace{1cm} (17)$$

Suppose that all parameters are equal except $\theta$, the security level increases after the strategy transfer, and it should be satisfied $\eta_1 > \eta_2$. We can examine that $\eta_1 > \eta_2$ is always true, which shows that when the externality is negative, firms should stop information security outsourcing.

To conclude this section, we can derive the following conclusions when considering immune failure and strategy transfer simultaneously:

**Conclusion 7.** When the externality is positive and $\theta > 2\phi_1(1 - \gamma - \beta)/2\beta - 2\phi_1\gamma + \phi_1$, the invaded firms should choose the strategy of outsourcing to protect their information security.

**Conclusion 8.** When the externality is negative, the decision factors of the information security strategy are not correlated with $\phi$ and $\theta$. In other words, invaded firms should choose the strategy of outsourcing for better security level.

According to the above conclusions, we summarize the conditions of hacker intrusion propagation or non-propagation under different information security strategies (Table 1), in which Case I indicates that immune failure and strategy transfer are not considered, Case II indicates that only immune failure is considered, and Case III indicates that immune failure and strategy transfer are considered at the same time. Firms and MSSP could adjust their own information security strategy or network security level due to the conditions of hacker intrusion propagation or non-propagation in the case of autonomous defense or outsourcing information security.

For example, we discuss the situations when firms choose autonomous defense strategy. In Case I, hacker intrusion propagation is related to the probability that the firm is invaded and the probability that the systems are successfully repaired after being invaded, while in Case II, hacker intrusion propagation is also affected by the probability of immune failure and the proportion of infected states in network nodes. Besides in Case III, hacker intrusion propagation is restricted by the probability of immune failure, the proportion of infected states in network nodes together with the proportion of strategy transfer.

To sum up, firms will choose the security technology according to the above influencing factors and improve their security levels. In addition, the proportion of susceptible states should be controlled in the range of hacker intrusion non-propagation. For instance, in Case I, compared with the firms choosing autonomous defense, if the information security outsourcing strategy is implemented, hacker intrusion propagation is affected by the security externalities. Similarly, MSSP should also adjust its own security service level according to the network environment to control the proportion of susceptible state in the range of hacker intrusion non-propagation.

### 4. Numerical Analysis

To better understand the conclusions of steady-state analysis, numerical simulation is a valid means to clarify the analytical process of the overall and local details. We set simulation parameters which accord with the numerical range in Section 2.1.

#### 4.1. Numerical Simulation without considering Immune Failure and Strategy Transfer.

Let $\lambda_1 = \lambda_2 = 0.5$, $\beta_1 = \beta_2 = 0.2$, $S_0 = 0.6$, and the externalities are $\theta = -0.1$ and $\theta = 0.1$, the phase trajectory of $I_2$ with $S_2$ when firms choose the strategy of outsourcing, and the phase trajectory of $I_1$ with $S_1$ when firms choose the strategy of autonomous defense.

Firms in the susceptible state tend to turn into $I$ or $R$, and the proportion of the susceptible state decreases. Figure 2 shows that with the decline of the proportion of susceptible firms, the proportion of infected firms first increases, then decreases, and eventually tends to be 0. Due to hackers having invaded certain firms and copied successful experiences to invade the affiliated firms, the proportion of infected firms is increased. However, firms will develop...
<table>
<thead>
<tr>
<th>Situation</th>
<th>Autonomous defense</th>
<th>Outsourcing information security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Conditions of hacker intrusion propagation</td>
<td>Conditions of hacker intrusion nonpropagation</td>
</tr>
<tr>
<td>I</td>
<td>$S_0 &gt; \phi_0/\beta_1$</td>
<td>$S_0 &lt; \phi_0/\beta_1$</td>
</tr>
<tr>
<td>II</td>
<td>$(\phi_1 + \gamma)/\beta_1 &lt; \lambda_1/\lambda_1$</td>
<td>$\lambda_1 &lt; \phi_1 + \gamma/\lambda_1$</td>
</tr>
<tr>
<td></td>
<td>$\gamma &lt; (\phi_1 + \gamma)/\lambda_1 &lt; \lambda_1/\lambda_1$</td>
<td>$(1 - \theta)\phi_0 &lt; (1 - \theta)_I$</td>
</tr>
<tr>
<td>III</td>
<td>$(\phi_1 + \gamma)/\beta_1 &lt; \lambda_1/\lambda_1$</td>
<td>$(1 - \theta)\phi_0 &lt; (1 - \theta)_I$</td>
</tr>
<tr>
<td>$\theta &gt; 0$</td>
<td>$S_0 &gt; (\phi_1 - \beta_1 - \gamma)/\lambda_1/(\lambda_1/\lambda_1 - \gamma)$</td>
<td>$S_0 &lt; (\phi_1 - \beta_1 - \gamma)/\lambda_1/(\lambda_1/\lambda_1 - \gamma)$</td>
</tr>
<tr>
<td></td>
<td>$(\phi_1 + \gamma)/\beta_1 &lt; \lambda_1/\lambda_1$</td>
<td>$(1 - \theta)\phi_0 &lt; (1 - \theta)_I$</td>
</tr>
<tr>
<td>$\theta &lt; 0$</td>
<td>$S_0 &gt; (\phi_2 - \phi_1 - \beta_1 - \gamma)/\lambda_1/(\lambda_1/\lambda_1 - \gamma)$</td>
<td>$S_0 &lt; (\phi_2 - \phi_1 - \beta_1 - \gamma)/\lambda_1/(\lambda_1/\lambda_1 - \gamma)$</td>
</tr>
<tr>
<td></td>
<td>$(\phi_1 + \gamma)/\beta_1 &lt; \lambda_1/\lambda_1$</td>
<td>$(1 - \theta)\phi_0 &lt; (1 - \theta)_I$</td>
</tr>
</tbody>
</table>

Table 1: Conditions of hacker intrusion propagation or nonpropagation.
effective security defense strategies that increase the number of immunized firms in the network. In addition, the above discussion is an ideal case, in which the negative impact of the immune failure on the security level is not considered. Therefore, firms in the infected state will eventually change to the recovered state as long as the defense is successful. Figure 2 also shows that if the proportion of susceptible firms is less than the threshold, the proportion of infected firms will decrease, which is consistent with Conclusion 1.

Next, we study the impact of externality on the security state of firms. Let $\lambda_1 = \lambda_2 = 0.5$, $\beta_1 = \beta_2 = 0.2$, $S_0 = 0.4$, and $I_1 = I_2 = 0.1$. Figures 3 and 4 show the security transfer if firms choose different security strategies, when positive externality or negative externality occurs during outsourcing, in which $S_1$, $I_1$, $R_1$ is the security state when firms choose the strategy of autonomous defense; in this situation, the externality is 0. Figure 3 shows $S_2$, $I_2$, $R_2$ is the security state curve when firms choose the strategy of information outsourcing with the positive externality ($\theta = 0.3$). Figure 4 shows $S_2$, $I_2$, $R_2$ is the security state curve when firms choose the strategy of outsourcing with negative externality ($\theta = -0.3$).

When $\theta = 0.3$, we obtain that $\beta_1/\lambda_2 = 0.2/0.5 = 0.4 = S_0$, $1 + \theta)/\lambda_2/(1 - \theta)\lambda_2 = 1.3 \times 0.2/0.7 \times 0.5 = 0.74 > S_0$, and satisfy the condition that the intrusion does not propagate in Conclusion 1, which is consistent with the declining trend of $I_1$ and $I_2$ in Figure 3. When $\theta = -0.3$, we obtain that $(1 + \theta)/\lambda_2/(1 - \theta)\lambda_2 = 0.21 < S_0$ and satisfy the condition that the intrusion propagates in Conclusion 1, which is consistent with the trend of $I_2$ that first increases and then declines in Figure 4. In addition, Figure 3 shows that when the externality is positive, the declining trend of $I_2(t)$ is faster than that of $I_1(t)$. On the other hand, Figure 4 shows that when the externality is negative, the declining trend of $I_1(t)$ is faster than that of $I_2(t)$, which is consistent with Conclusion 2.

4.2. Numerical Simulation considering Immune Failure. In this section, we first consider the case of immune failure when firms choose the strategy of autonomous defense. For situation 1, let $\gamma_1 = 0.5$, $\lambda_1 = 0.2$, and $\beta_1 = 0.2$, $I_0 = 0.4$. For situation 2, let $\gamma_1 = 0.5$, $\beta_1 = 0.8$, and $I_0 = 0.4$. For situation 3, let $\gamma_1 = 0.1$, $\lambda_1 = 0.3$, $\beta_1 = 0.8$, and $I_0 = 0.4$. For situation 4, let $\gamma_1 = 0.1$, $\lambda_1 = 0.8$, $\beta_1 = 0.2$, and $I_0 = 0.4$. For situation 5, let $\gamma_1 = 0.3$, $\lambda_1 = 0.8$, $\beta_1 = 0.2$, and $I_0 = 0.4$. Figure 5 shows the variation curves of the proportion of infected firms with $t$ when the firms choose the strategy of autonomous defense.

Secondly, we consider the case of immune failure when firms choose the strategy of outsourcing. For situation 1, let $\gamma_2 = 0.5$, $\lambda_2 = 0.2$, $\beta_2 = 0.2$, $I_0 = 0.4$, and $\theta = 0.2$. For situation 2, let $\gamma_2 = 0.5$, $\lambda_2 = 0.2$, $\beta_2 = 0.8$, and $I_0 = 0.4$. For situation 3, let $\gamma_2 = 0.1$, $\lambda_2 = 0.3$, $\beta_2 = 0.8$, and $I_0 = 0.4$. For situation 4, let $\gamma_2 = 0.1$, $\lambda_2 = 0.8$, $\beta_2 = 0.5$, and $I_0 = 0.4$. For situation 5, let $\gamma_2 = 0.3$, $\lambda_2 = 0.8$, $\beta_2 = 0.2$, and $I_0 = 0.4$. For situation 6,
\( \gamma_2 = 0.5, \lambda_2 = 0.8, \beta_2 = 0.2, \) and \( I_0 = 0.4. \) Figure 6 shows the variation curves of the proportion of infected firms with \( t \) when the firms choose the strategy of outsourcing if the externality is 0.2.

Figures 5 and 6, respectively, show the variation curves of the proportion of infected firms when they choose the strategy of autonomous defense and outsourcing. When immune failure occurs, whichever security strategy firms choose, there are always invaded firms, and the variation trend of the proportion of infected firms is the same. Specifically, the proportion of infected firms in situation 1, situation 5, and situation 6 shows an increasing trend, while the proportion of infected firms in situation 2, situation 3, and situation 4 shows a declining trend. In addition, comparing Figures 5 and 6, we derive when firms choose the strategy of outsourcing and the externality is positive, the proportion of infected firms as well as the scale of intrusion propagation can be decreased in the network.

### 4.3. Numerical Simulation considering Immune Failure and Strategy Transfer.

In this section, regardless of whether externality is positive or negative, let \( \lambda_1 = \lambda_2 = 0.5, \beta_1 = \beta_2 = 0.3, \gamma_1 \approx \gamma_2 = 0.5, \) and \( \phi_2 = 0.2. \) Figures 7 and 8(a) show that \( I_1(t) \) is the variation curve of infected firms when the strategy of autonomous defense is chosen. The remaining four curves \( I_2(t) \), respectively, correspond to the variation curves of infected firms when they transfer the strategy from autonomous defense to that of outsourcing with gradually increasing externality.

In addition, to clarify how the strategy transfer affects the information security strategy, we compare the trends of \( I_1(t) \) and \( I_2(t) \) under a certain negative externality in Figure 8(b) (i.e., let \( \theta = -0.4).\)

Figure 7 shows that the strategy of outsourcing is inferior to that of autonomous defense when \( 2\phi_1(1 - \gamma - \beta) / 2\beta - 2\phi_1\gamma + \phi_1 = 0.13, \) which implies that \( \theta = 0.1 < 0.13. \) With the continuous increase of positive externality (i.e., \( \theta = 0.2, \theta = 0.3, \theta = 0.4), \) the scale of invaded firms in the network decreases after implementing the strategy of outsourcing. And the greater impact of positive externality leads to a lower proportion of infected firms. This demonstrates that if the MSSP plays an active role through positive externality, strategy transfer can better ensure the firms’ security. Therefore, firms have more motivation to transfer from the strategy of autonomous defense to that of outsourcing, which is consistent with Conclusion 7.
Figures 8(a) and 8(b) show that in the case of negative externality, no matter how the externality influences and the proportion of strategy transfer varies, the proportion of infected firms when choosing the strategy of autonomous defense is always less than that of outsourcing. This demonstrates that the strategy of autonomous defense can better protect the firms’ security.

5. Conclusion

In this paper, the SIR model of intrusion propagation in complex networks is established under different information security states. The threshold conditions of intrusion propagation are studied by steady-state analysis when firms choose different security strategies. The influences of externalities on the scale of intrusion propagation and strategy transfer are also discussed. We showed that (i) without considering immune failure and strategy transfer, the intrusion will propagate if the initial proportion of susceptible firms is greater than the threshold of intrusion propagation; firms can effectively resist the intrusion propagation only if the externality is positive. (ii) Considering immune failure, there are always infected firms in the network. When the externality is positive, it will not change the fact of intrusion propagation if firms choose the strategy of outsourcing; however, it can reduce the propagation speed. The probability of intrusion propagation is influenced by the proportion of the initial infected state, the probability of invasion, and the probability of immune failure. (iii) Considering both immune failure and strategy transfer, if the externality is positive and greater than a certain threshold, invaded firms can seek the help of outsourcing; otherwise, firms should stop outsourcing information security as soon as possible.

In addition, the conclusions of this paper also provide guidance when firms encounter hacker intrusion.

First, if the hacking damage is not serious or the firms’ defense is successful and can resist the same type of attack again, the ratio between the effect of recovering information systems and the probability of invasion should be comprehensively considered. And the probability of intrusion propagation can be judged by the proportion of firms that have not been invaded relative to the total firms in the network. If firms choose the strategy of outsourcing, the MSSP must play an active role in ensuring information systems security by positive externality of intrusion event associative processing.

Secondly, if the hacking methods are upgraded, which probably leads to the immune failure, firms need to be prepared for a long battle with hackers. And the probability of intrusion propagation can be comprehensively judged by the proportion of infected firms in total and the probability of immune failure. If the quality of the MSSP’s security service is relatively high, the strategy of outsourcing can slow down the speed of hacker intrusion propagation, which reduces the scale of invaded firms.

Finally, when the firms transfer their information security strategy after they are invaded, then collaborating with the MSSP is a better choice only if the MSSP may collect hackers’ information by analysis tools to develop personalized defense measures, dynamically respond to security threats, and maximize security benefits. On the contrary, if the MSSP cannot effectively detect system vulnerabilities and ignore the potential risk of the threat to affiliated firms, which reduces the hackers’ cost of copying intrusion experience, leading to a poor outsourcing service quality, firms should stop outsourcing security service as soon as possible.
Data Availability
The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest
The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments
This research was funded by the National Natural Science Foundation of China (71801125 and 71701093), China Postdoctoral Science Foundation funded project (2018M630544), and Jiangsu Postdoctoral Science Foundation funded project (1701080C).

References