Combating Ransomware in Internet of Things: A Games-in-Games Approach for Cross-Layer Cyber Defense and Security Investment

Yuhan Zhao(✉), Yunfei Ge, and Quanyan Zhu

Department of Electrical and Computer Engineering, Tandon School of Engineering, New York University, Brooklyn, NY 11201, USA
{yhzhao,yg2047,qz494}@nyu.edu

Abstract. The recent surge in ransomware attacks has threatened many critical infrastructures such as oil pipeline systems, hospitals, and industrial Internet of Things (IoT). Ransomware is a cryptoviral extortion attack that involves two phases: the cyber infection of the malware and the financial transaction of the ransom payment. As the ransomware attackers are financially motivated, the protection of the infrastructure networked systems requires a cross-layer risk analysis that not only examines the vulnerability of the cyber system but also consolidates the economics of ransom payment. To this end, this paper establishes a two-player multi-phase and multi-stage game framework to model cyber and economic phases of a ransomware attack. We use a zero-sum Markov game to capture the multi-stage penetration of ransomware in the lateral movement. A sequential-move game is proposed to model the ransom payment interactions at the second phase. Two games are composed to form a multi-phase and multi-stage game-in-games (MPMS-GiG) that enables a holistic risk assessment of ransomware in networks and a cross-layer design of cyber defense and investment strategies to mitigate the attack. We provide a complete equilibrium characterization of ransomware game and design interdependent optimal strategies for cyber protection and ransom payment. We use prospect theory to analyze the impact of human factors on equilibrium strategies. Finally, we use a prototypical industrial IoT network as a case study to corroborate the results.

Keywords: Ransomware · Cybersecurity · Game theory · Security economics · Risk assessment · Prospect theory · Internet of Things

1 Introduction

Ransomware is a type of malware that infects particular network entities to demand ransom. It is in general classified into two categories: the locker ran-

This work is partially supported by grants SES-1541164, ECCS-1847056, CNS-2027884, and BCS-2122060 from National Science Foundation (NSF), DOE-NE grant 20-19829 and grant W911NF-19-1-0041 from Army Research Office (ARO).

B. Bošanský et al. (Eds.): GameSec 2021, LNCS 13061, pp. 208–228, 2021.
https://doi.org/10.1007/978-3-030-90370-1_12

somware and the crypto ransomware [23]. Once infected, the ransomware either locks the target device to deny any access or encrypts the target device data to disrupt normal functionality. [12,18]. Emerged in 1989 as a floppy disk Trojan, the ransomware has developed dramatically with time and has evolved into different families such as CryptoLocker [21], Petya [2], etc. It is becoming more prevalent nowadays with the fast advance of the Internet of Things (IoT) in various fields such as manufacturing and transportation [20,22]. The broad connections for IoT devices provide more security threats and vulnerabilities. Besides, the massive number of IoT devices increases the risk of getting infected by ransomware since any device could be the target. The consequence can be severe if critical devices such as medical equipment and generators are compromised. Indeed, the ransomware attack has caused significant economic losses in industrial domains. It is reported that there have been at least 150 ransomware attacks in manufacturing and 37 attacks in transportation industries in the third quarter of 2020 [7]. The estimated global damage from ransomware reaches $20 billion in 2021 [3]. A recent ransomware attack on the energy infrastructure company Colonial Pipeline this May alone has caused more than $2 million loss for the company [1]. The detriment of ransomware is no longer negligible.

A ransomware attack in general contains four stages: "code", "spread", "extract", and "monetize" [14], which can be summarized into cyber and economic phases. The cyber phase focuses on the multi-stage intrusion kill chain. An attacker first assembles the ransomware code and finds the initial entry point to deploy ransomware. Once entered, the ransomware penetrates over the network to compromise the target. After infecting the target, the ransomware extracts and processes the target's data to either lock it or encrypt important files. The economic phase refers to preliminary precautions and the "monetize" stage, which models the ransom payment interactions between the attacker and the victim.

As two indispensable components in the ransomware attack, the cyber and economic phases are naturally interdependent. A network defender can design effective cyber defense schemes by taking into account the risk of ransom payment. The defender's security investment and ransom payment strategy can benefit from the properly designed defense system. Therefore, a holistic and cross-layer defense-payment design framework can cost-effectively mitigate the cyber risks as well as reduce monetary losses. Traditional studies in ransomware treat the cyber and the economic phases separately. For the cyber phase, Intrusion Detection Systems (IDS) [6] have been widely studied in networks to detect malicious behaviors in cyberspace. However, they only provide monitoring information but no defense actions to mitigate the attack. Intrusion Response Systems (IRS) outperform IDS as they can conduct necessary actions to respond to malicious attacks [11], but the limited predefined actions confine their capability to cope with sophisticated attacks such as ransomware attacks. Practical methods, such as constantly updating the software and running network scans [24], fail to capture the complex behavior of the ransomware. Once compromised by ransomware, we may be discouraged by the fact that victims simply pay the ransom in many cases, and even the FBI once inadvertently mentioned paying

the ransom if the network device is infected [5]. It is not until recently that several studies have been conducted to understand the economics of ransomware [4,9,15]. These works mainly focus on the mitigation strategy after the target is compromised. A cost-effective strategy to combat ransomware requires not only a post-infection solution but also a proper cyber defense and security investment strategy to minimize the ransomware risk across multiple phases.

To this end, in this work, we propose a two-player multi-phase multi-stage ransomware game to capture both the cyber and economic phases of a ransomware attack and provide a holistic consideration and design for cyber defense and ransom payment. In the cyber phase, we use a zero-sum Markov game to characterize the sophisticated and dynamic features of ransomware. The attacker (i.e., the ransomware) explores the network edge vulnerabilities and moves laterally to infect the target, while the defender aims to prevent the penetration by hardening specific connection links. The cyber Markov game serves as a risk assessment measure to help make security decisions in the sequel. The economic phase depicts the ransom payment interactions between two players. Once the target is infected, we use a sequential-move ransom-payment game to analyze the defender's optimal payment strategy and the optimal ransom demanded by the attacker. The cyber Markov game is composed with the ransom-payment game to form a multi-phase multi-stage games-in-games (MPMS-GiG) framework that enables a holistic risk assessment of the ransomware in IoT networks and a cross-layer design of cyber defense and ransom payment strategies to mitigate the attack. The interdependency between the two phases is captured by ransom demand, security investment, and security budget. Specifically, the defender invests in IoT network security to better deter the penetration of ransomware, resulting in a lower infection probability. The infection probability and the remaining budget then influence the following ransom payment interactions. By considering the interdependency between the two phases, we analyze and provide a cross-layer defense-payment strategy to better combat ransomware and protect IoT network security.

Another special feature of ransomware attack is human factors. In ransomware attacks, the victims are humans, who hold biased recognition concerning losses and risks, which can lead to different defense strategies compared with the perfectly rational one. This phenomenon is explained by prospect theory, and it is necessary to investigate its impact on the decision-making within the ransomware attack. Our framework also provides an analysis of how human factors affect the optimal attack/defense strategies.

The contribution of this paper is as follows. First, we propose an MPMS-GiG framework to capture both the cyber and economic phases in the ransomware attack. Second, we provide a complete characterization and analysis of the equilibrium solution of the ransomware game and design interdependent optimal cyber protection and ransom payment strategies. Third, we use sensitivity analysis and prospect theory to investigate how human factors play a role in combating ransomware attacks. Finally, we use a case study with a prototypical industrial Internet of Things (IoT) network to corroborate the results.

1.1 Related Work

The penetration process of ransomware in the cyber phase is commonly modeled by the lateral movement in Advanced Persistent Threats (APTs). Some works have adopted game theory to study the defense against lateral movement. Noureddine et al. in [17] have used a zero-sum game to model the lateral movement over enterprise networks, where the attacker seeks the shortest path to compromise the target and the defender responds by disconnecting available services of a potential victim node. Huang and Zhu in [10] have adopted a multi-stage Bayesian game to characterize the lateral movement with uncertainty in the infrastructure network. The equilibrium strategies are derived for network security enhancement. Although these works do not focus on ransomware, they share a similar penetration process as the cyber phase in ransomware attacks.

From the economic perspective, game theory has not been adopted to analyze ransomware until recently. Hernandez-Castro et al. in [9] provide an economic analysis of ransomware including the optimal pricing and bargaining strategies. They have also discussed several determinants of the victim's willingness to pay. Caporusso et al. in [4] have proposed a two-stage game to characterize the ransomware behavior after the target is compromised. Several cases are discussed based on the different parameters such as the attacker's cost. Laszka et al. in [15] have built a two-stage game-theoretic framework to study the ransomware ecosystem. They have studied the behavior of two target groups with different infection probabilities, including their optimal payment strategies and the attacker's optimal attack plan. Additionally, a backup strategy as a precaution to alleviate the ransomware attack has also been considered in their model. Cartwright et al. [5] have adapted two kidnapping game models and have applied them to the ransomware context. Theoretical results are discussed to understand the behavior of the attacker and the victim.

1.2 Organization of the Paper

The rest of the paper is organized as follows. Section 2 discusses the basic settings and formulates the ransomware problem. Section 3 analyzes the risk assessment outcome of the cyber Markov game and the equilibrium of the ransomware game. Section 4 studies the impact of the security budget and human factors on the equilibrium strategy with prospect theory. We use a case study in Sect. 5 to demonstrate the results and conclude the paper in Sect. 6.

2 Problem Formulation

In this section, we formulate the ransomware game as a two-player multi-phase multi-stage security game. The notations[1] are summarized in Table 1.

[1] The notations of the cyber Markov game are listed in Sect. 2.3 separately.

Table 1. List of notations in the ransomware game.

Symbol	Description
r_d, q_d	security investment and payment action
r_a, q_a	demanded ransom and attack action
U_d, U_a	defender's/attacker's payoff
c_f, c_s, δ	attack cost, overall and additional attack cost
θ	successful defense probability
λ	defender's untrusted level to the attacker
w	value of the target (defender's willingness to pay)
μ	defender's expected willingness to pay
B	defender's total security budget
$\hat{r}_d$	threshold investment to prevent the ransomware attack

2.1 Basic Settings

The ransomware game (RG) captures both cyber and economic phases in a ransomware attack and consists of two players, a defender (she) and an attacker (he). The defender operates a network with multiple connected entities and has a total security budget of $B > 0$. Her objective is to protect the target asset and to maximize the payoff by (a) investing the network security and (b) determining the payment strategy if the target is infected.

Let $w \in \mathbb{R}$ be the value of the target, which can also be interpreted as the defender's willingness to pay. We denote $\lambda \in [0, 1]$ as the defender's untrusted level to the attacker, which can be measured by the portion of people who choose not to pay the ransom in practice. Because of λ, we define the defender's expected willingness to pay as $\mu = (1 - \lambda)w$. We assume that $B > \mu$ so that the budget can cover the ransom if the target is infected by ransomware. Let $r_d \in [0, B]$ be the network security investment and $q_d \in \{0, 1\}$ be the defender's decision to pay ($q_d = 1$) or not to pay ($q_d = 0$) the ransom after infection. The objective of the attacker is to maximize the payoff using ransomware. He can either deploy ransomware ($q_a = 1$) or abandon the attack ($q_a = 0$). If the attacker decides to attack, he compromises some initial entry points to penetrate the network and searches for the target. The penetration process is modeled by the cyber Markov game in Sect. 2.3. Once the target is compromised, the attacker locks the target and determines the amount of ransom $r_a \in \mathbb{R}_+$. Note that the sum of the security investment and the ransom payment should not exceed the budget B, which we refer to as the budget constraint:

$$r_d + r_a \leq B. \tag{1}$$

2.2 Multi-phase Multi-stage Game Formulation

We formulate the RG as a two-phase three-stage game to capture the sequential interactions between the defender and the attacker, illustrated as follows.

Stage 1 *Initial Investment*: Defender invests r_d to improve the network security.
Stage 2 *Cyber Defense*: Two sub-stages due to attacker's binary action q_a.

Stage 2a The attacker decides whether to attack $q_a = 1$ or not $q_a = 0$. He receives a zero payoff if he abandons the attack and the game terminates. Otherwise, he enters Stage 2b.

Stage 2b The attacker deploys ransomware and starts the penetration, which is captured by the cyber Markov game. With probability θ, he fails to infect the target and receives a cost $c_f \in \mathbb{R}_+$; with probability $1 - \theta$, he compromises the target and demands the ransom r_a. The overall cost for a successful attack is $c_s = c_f + \delta$.

Stage 3 *Ransom Payment*: Two sub-stages due to defender's binary action q_d.

Stage 3a The defender decides whether to pay $q_d = 1$ or not $q_d = 0$. She receives a loss of $w + r_d$ if she does not pay and the game terminates. Otherwise, she enters Stage 3b. Note that the defender will not pay if the remaining budget is not sufficient to cover the ransom ($B - r_d < r_a$).

Stage 3b The defender pays the ransom but still faces the risk of target recovery failure: with probability λ, the attacker keeps locking the target and the defender loses both ransom and the target; with probability $1-\lambda$, the attacker releases the target.

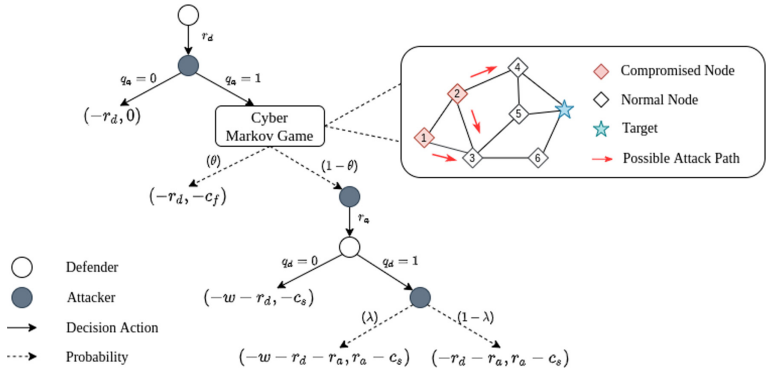


Fig. 1. Structure of the multi-phase and multi-stage game: A cyber Markov game is embedded in the ransom game.

2.3 Cyber Markov Game for Ransomware Penetration

In the cyber phase of the ransomware attack, the attacker penetrates the network and searches for attack paths to infect the target. The defender's security investment can increase the difficulty of ransomware penetration. We assume that after a maximum of K rounds search, if the attacker still cannot reach

the target, a security update will be applied to the system and the attack fails. We model the attack-defense interactions in the penetration process under the security investment r_d as a finite horizon zero-sum Markov game (MG).

We consider a network (represented by a graph) $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the node set and $\mathcal{E} = \{(u, v)|u, v \in \mathcal{V}, u \neq v\}$ represents the edge set. Each node in $\mathcal{V}$ represents an entity such as a controller, database, etc. An edge in $\mathcal{E}$ means that two entities are connected and can perform service exchange. We attach a label function L^k: $\mathcal{V} \mapsto \{0, 1\}$ to each node in $\mathcal{V}$ at time k, representing their operation status. For all $v \in \mathcal{V}$ at time k,

$$L^k(v) = \begin{cases} 1 & \text{if } v \text{ is compromised,} \\ 0 & \text{if } v \text{ is normal.} \end{cases}$$

At time $k = 0$, the attacker compromises the initial node v_0 and searches for the target $\hat{v}$. Hence $L^0(v) = 0$, $\forall v \in \mathcal{V} \backslash v_0$ and $L^0(v_0) = 1$. We define the cyber MG by the tuple $\langle \mathcal{S}, \mathcal{A}_\mathcal{M}, \mathcal{D}_\mathcal{M}, P, C, K \rangle$. Each component is discussed as follows.

- *State space $\mathcal{S}$:* The finite set $\mathcal{S}$ constitutes all possible labeled graph in K steps, i.e., $\mathcal{S} = \{(\mathcal{G}, L^k)\}_{k=0}^K$, where $\mathcal{G}$ is the underlying network and L^k contains all possible labels for all nodes $v \in \mathcal{V}$ at time k. We denote $\mathcal{S}^k$ as the subset of $\mathcal{S}$ at time k and write $s^k \in \mathcal{S}^k$ as a specific state.
- *Attacker's action space $\mathcal{A}_\mathcal{M}$:* The attacker (minimizer) attempts to attack a normal node through edge vulnerabilities for the next step penetration. Given the game state s^k, the attacker's action set is defined as

$$\mathcal{A}_\mathcal{M}(s^k) = \{(u, v)|(u, v) \in \mathcal{E}, L^k(u) = 1, L^k(v) = 0\}.$$

  We write $a^k \in \mathcal{A}_\mathcal{M}(s^k)$ as a specific attacker's action at time k. In Fig. 1, the edges $\{(1, 3), (2, 3), (2, 4)\}$ form the attacker's action set $\mathcal{A}_\mathcal{M}$ in this example.
- *Defender's action space $\mathcal{D}_\mathcal{M}$:* The defender (maximizer) aims to mitigate the attack by hardening the service security over the selected edge. Thus, she shares the same action set as the attacker at time k, i.e., $\mathcal{D}_\mathcal{M}(s^k) = \mathcal{A}_\mathcal{M}(s^k)$.
- *Transition probability P:* We write the transition probability as $\Pr(s' \mid s, a, d)$ where s', s are current and future states and a, d are attacker's and defender's actions. If the attack $a^k = (u, v)$ succeeds, the label for node v is set to $L^{k+1}(v) = 1$ and the game state is updated accordingly. In our model, the defender combats the attacker by investing the edge security and increasing the attack cost of edge d^k. Thus, the defender's action will not influence the transition probability. Given s^k and a^k, we have

$$\Pr(s^{k+1} \mid s^k, a^k, d^k) = \Pr(s^{k+1} \mid s^k, a^k) = \begin{cases} \gamma(r_d, a^k) & s^{k+1} \neq s^k, \\ 1 - \gamma(r_d, a^k) & s^{k+1} = s^k, \end{cases}$$

  where $\gamma(r_d, e) \in [0, 1]$, $\forall e \in \mathcal{E}$ is the attack success probability through edge e, which captures the impact of the security investment r_d on that edge.

– *Immediate utility C:* Given the state s^k and the action pair (a^k, d^k), we have

$$C(s^k, a^k, d^k) = \begin{cases} C_d & \text{if } a^k = d^k, \\ C_e(a^k) - H(v) & \text{if } a^k \neq d^k, \end{cases}$$

where
- $C_d \in \mathbb{R}$ is cost for the attacker when the defender protect the same edge.
- $C_e(a^k) \in \mathbb{R}$ is cost of attacking through the chosen edge a^k without defense. Note that $C_d > C_e(e)$, $\forall e \in \mathcal{E}$.
- $H(v) \in \mathbb{R}$ is the attractiveness of the next node v, which is given by

$$H(v) = \frac{n}{(\text{distance to } \hat{v})} + q \cdot (\#\text{ of possible paths to } \hat{v}),$$

where n and q are positive weights.

The attacker receives an additional terminal reward $-w$ when he compromises the target $\hat{v}$. Then, he stays in $\hat{v}$ till the game terminates.

– *Game horizon K:* The horizon K represents the maximum time span for the ransomware to exist in the network. A successful defense prevents the attacker from reaching the target $\hat{v}$ within K steps.

2.4 Solution Concept

Ransomware can be viewed as a special case of APT attacks. In APT attacks, the attacker usually acquires sufficient knowledge about the system with preliminary reconnaissance. Therefore, we assume that both players have complete information in the RG. We adopt sub-game perfect Nash equilibrium (SPNE) as the solution concept in the RG. The cyber MG generates the successful defense probability and the attack cost, which serve as risk assessment parameters to develop the SPNE of the RG. The complete information assumption is crucial to characterize the interdependency between cyber and economic phases.

3 Ransomware Game Analysis

In this section, we first discuss the risk assessment outcome of the cyber MG and then provide a complete equilibrium analysis of the RG.

3.1 Risk Assessment Outcome of the Cyber Markov Game

In the cyber MG, at each state s^k, we denote the strategy of player i ={Attacker, Defender} as $\pi_i(s^k)$. To find the optimal strategies, we adopt the finite value iteration method [13] to solve the game computationally. Given the investment r_d, we denote the equilibria of the cyber MG $\pi_i^*(r_d)$. We mention that $\pi^*(r_d) = \{\pi_A^*(r_d), \pi_D^*(r_d)\}$ captures the successful defense probability $\theta \in [0, 1]$ and the attack cost $c_f \in \mathbb{R}_+$ given the investment $r_d \in [0, B]$. We define

$$\theta(r_d) = \frac{N_{\text{succ}}(r_d)}{N}, \quad c_f(r_d) = \mathbb{E}_{\pi^*(r_d)}\left[\sum_{k=1}^{K} C^k\right],$$

where N is the total simulated attacks and N_{succ} is the number of successful attacks[2], and C^k is the immediate utility he received at time k.

The average outcome in the cyber MG can serve as a risk assessment measure for the future security decision making. Although it is difficult to characterize $\theta(r_d)$ and $c_f(r_d)$ analytically, we can confirm their positive correlations with r_d. For the purpose of future analysis, we assume the differentiability and $\theta'(r_d) \geq 0$, $c_f'(r_d) \geq 0$. Indeed, these assumptions can be verified in our case study in Sect. 5. We also define the attacker's cost for a successful attack as $c_s(r_d) = c_f(r_d) + \delta$, where δ is the additional cost representing the cost of remote communication and manipulation to the target. Without causing confusions, we write θ and c_f for $\theta(r_d)$ and $c_f(r_d)$ in the rest of the paper.

3.2 Equilibria of the Ransomware Game

We use backward induction to analyze the SPNE of the RG. We use the subscript and the superscript to denote the players' payoffs under different actions and different stages respectively. For example, $U_d|^3_{q_d=1}$ represents the defender's payoff at stage 3 when she decides to pay the ransom.

At stage 3, the defender decides whether to pay ($q_d = 1$) or not to pay ($q_d = 0$) the ransom. We have two possibilities: the remaining budget is either sufficient ($B - r_d \geq r_a$) for the ransom or not sufficient ($B - r_d < r_a$). In the latter case, the defender's only option is not to pay and her payoff is $-w - r_d$. In the former case, the defender can decide whether to pay or not to pay. The payoff of not to pay is still $-w - r_d$. Thus, we have $U_d|^3_{q_d=0} = -w - r_d$. If the defender decides to pay, then her expected payoff is

$$U_d|^3_{q_d=1} = \lambda(-w - r_a - r_d) + (1-\lambda)(-r_a - r_d) = -r_a - r_d - \lambda w.$$

Therefore, we conclude that the defender will choose to pay when the budget is sufficient and $U_d|^3_{q_d=1} \geq U_d|^3_{q_d=0}$, which indicates the optimal payment action is

$$q_d^* = \begin{cases} 1 & B - r_d \geq r_a, (1-\lambda)w \geq r_a, \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

Similarly, the attacker's payoffs at stage 3 for different cases are

$$U_a|^3_{q_d=0} = -c_s, \quad U_a|^3_{q_d=1} = r_a - c_s. \tag{3}$$

At stage 2, the attacker first decides whether to attack ($q_a = 1$) or not ($q_a = 0$) and then chooses the amount of ransom r_a if the attack is successful. The payoff of abandoning the attack is simply $U_a|^2_{q_a=0} = 0$. If the attacker decides

[2] An attack is successful if the attacker compromises the target within K steps.

to attack, his expected payoff is related to the successful defense probability θ in the following cyber MG:

$$U_a|^2_{q_a=1} = \theta(-c_f) + (1-\theta)U_a|^2_{q_a=1,\text{succ}}.$$

$U_a|^2_{q_a=1,\text{succ}}$ either equals $U_a|^3_{q_d=1}$ or $U_a|^3_{q_d=0}$, depending on the defender's payment action at stage 3. From (3) we always have $U_a|^3_{q_d=1} \geq U_a|^3_{q_d=0}$. In order to maximize the payoff, the attacker would set the ransom value to encourage ransom payment of the defender. Hence, by considering (1), we have

$$r_a \leq \min\{B - r_d, (1-\lambda)w\} = \min\{B - r_d, \mu\}. \tag{4}$$

In this case, the payoff of the attacker choosing to attack is

$$U_a|^2_{q_a=1} = \theta(-c_f) + (1-\theta)(r_a - c_s). \tag{5}$$

In addition, to ensure that starting the attack is indeed a better strategy, the attacker needs $U_a|^2_{q_a=1} \geq U_a|^2_{q_a=0} = 0$, which yields

$$r_a \geq \frac{\theta c_f + (1-\theta)c_s}{1-\theta}. \tag{6}$$

We note that (4) and (6) form a closed set of r_a, which we denote as $\Omega = \{r_a \,|\, (4) \text{ and } (6) \text{ hold}\} \subseteq \mathbb{R}$. As long as Ω is not empty, the optimal strategies for the attacker and the defender are to start the ransomware attack and to pay the ransom, respectively. The optimal amount of ransom is

$$r_a^* = \arg\max_{r_a \in \Omega} U_a|^2_{q_a=1} = \min\{B - r_d, \mu\} \tag{7}$$

provided $\Omega \neq \varnothing$. Thus, the optimal attack strategy at stage 2 is

$$q_a^* = \begin{cases} 1 & \Omega \neq \varnothing, \\ 0 & \text{otherwise.} \end{cases} \tag{8}$$

The defender's utility is simply the defense investment $-r_d$ if the attack abandons the attack, i.e., $U_d|^2_{q_a=0} = -r_d$. According to the aforementioned analysis, if the attacker decides to attack, he sets the amount of ransom to encourage ransom payment. Therefore, the defender pays the ransom and faces the risk that the attacker does not release the target even after receiving the payment. We can write the expected utility as

$$U_d|^2_{q_a=1} = \theta(-r_d) + (1-\theta)U_d|^3_{q_d=1} = -r_d - (1-\theta)(r_a + \lambda w). \tag{9}$$

At stage 1, the defender determines the security investment r_d to maximize her payoff. If the attacker implements the attack, the defender and the attacker play the cyber MG under the enhanced network with defense investment r_d. Since the outcomes of the cyber MG (θ and c_f) depend on the r_d, the set Ω is also parameterized by r_d and we denote it as $\Omega(r_d)$. To further analyze the optimal security investment, we first focus on the structure of $\Omega(r_d)$ and arrive at the following proposition.

Proposition 1. *There exists $r_d \geq 0$ such that $\Omega(r_d) \neq \varnothing$ if $c_s < \mu$. Furthermore, there exists a unique threshold $\hat{r}_d \in [0, B]$ such that $\Omega(r_d) = \varnothing$ when $r_d > \hat{r}_d$.*

Proof. Let $f(r_d) = \frac{\theta c_f + (1-\theta)c_s}{1-\theta}$. Further let $g(r_d) = \min\{B - r_d, \mu\} - f(r_d)$. Then, $g(r_d)$ denotes the length of $\Omega(r_d)$ when it is positive. Using the assumptions in Sect. 3.1, we show that $f'(r_d) > 0$. Therefore, $g'(r_d) < 0$ except for the point $r_d = B - \mu$, which does not affects the monotonicity of $g(r_d)$. So $g(r_d)$ is decreasing in $r_d \geq 0$. Since $B > w$ and $c_s < \mu$, we have $g(0) = \mu - c_s > 0$. Therefore, there exists $r_d \geq 0$ such that $\Omega(r_d) \neq \varnothing$. It is clear that $f(0) > 0$ and $g(B) < 0$. With the continuity assumption of θ and c_f, there exists a unique $\hat{r}_d$ such that $g(\hat{r}_d) = 0$ and $g(r_d) < 0$ when $r_d > \hat{r}_d$.

Remark 1. The condition $c_s < \mu$ implies that the attacker always has the incentive to attack. We assume the condition always holds in the sequel.

Remark 2. $f(r_d)$ and $\hat{r}_d$ have straightforward but critical interpretations. From (6), $f(r_d)$ is the minimum ransom that the attacker has to demand if he decides to attack. Otherwise, he receives a negative payoff, which is worse than abandoning the attack. The monotonic property $f'(r_d) > 0$ indicates that the minimum ransom increases along with the improvement of network security level. $\hat{r}_d$ is the *threshold investment* such that the attacker cannot make any profit by attacking. It refers to the scenario where the maximum possible ransom is not sufficient to offset the attack cost. Note that $\hat{r}_d$ is a critical value in the sense of economics, which does not indicate the network is fully secured with $\theta(\hat{r}_d) = 1$. In practice, rational attackers will not attack in the first place if they cannot profit from it.

Proposition 1 indicates a *threshold strategy* for investing the network security. If the defender invests any amount larger than $\hat{r}_d$, we have $\Omega = \varnothing$ and the attacker's optimal strategy is to abandon the attack and receives a zero payoff, i.e., $U_a|^1_{r_d \geq \hat{r}_d} = 0$. Then the defender successfully secure the target with this investment. However, we note that the defender has no incentive to invest more than $\hat{r}_d$ because the attacker will not attack anyway. Therefore, in this case, $r_d^* = \hat{r}_d$ and the optimal payoff $U_d^*|^1_{r_d \geq \hat{r}_d} = -\hat{r}_d$. On the other hand, if the defender invests $\widetilde{r}_d < \hat{r}_d$, the attacker has the incentive to attack. In this case, the defender's payoff is

$$\begin{aligned} U_d|^1_{r_d < \hat{r}_d} = U_d|^2_{q_a = 1} &= -r_d - (1-\theta)(r_a^* + \lambda w) \\ &= \begin{cases} -r_d - (1-\theta)w & 0 \leq r_d < B - \mu, \\ -\theta r_d - (1-\theta)(B + \lambda w) & B - \mu \leq r_d < \hat{r}_d, \end{cases} \end{aligned} \tag{10}$$

and the corresponding optimal security investment is

$$\widetilde{r}_d^* = \arg \max_{0 \leq r_d < \hat{r}_d} U_d|^1_{r_d < \hat{r}_d}, \tag{11}$$

which is related to the property of the successful defense probability $\theta(r_d)$. We summarize the optimal investment strategy as follows:

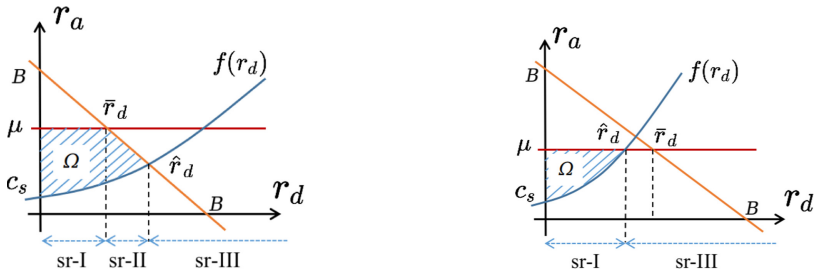
$$r_d^* = \begin{cases} \hat{r}_d & U_d|_{r_d<\hat{r}_d}^1(\widetilde{r}_d^*) < -\hat{r}_d, \\ \widetilde{r}_d^* & U_d|_{r_d<\hat{r}_d}^1(\widetilde{r}_d^*) \geq -\hat{r}_d. \end{cases} \tag{12}$$

Proposition 2. *The RG possesses one of the equilibrium solutions below based on the relationship between $-\hat{r}_d$ and $U_d|_{r_d<\hat{r}_d}^1(\widetilde{r}_d^*)$, where $\widetilde{r}_d^*$ is defined in (11):*

(Eq_1) If $-\hat{r}_d \geq U_d|_{r_d<\hat{r}_d}^1(\widetilde{r}_d^*)$: $\langle r_d^* = \hat{r}_d, q_d^* = 1, r_a^* = \min\{B - \hat{r}_d, \mu\}, q_a^* = 0\rangle$.
Optimal payoffs are $U_d^* = -\hat{r}_d$, $U_a^* = 0$.
(Eq_2) If $-\hat{r}_d < U_d|_{r_d<\hat{r}_d}^1(\widetilde{r}_d^*)$: $\langle r_d^* = \widetilde{r}_d^*, q_d^* = 1, r_a^* = \min\{B - r_d^*, \mu\}, q_a^* = 1\rangle$.
Optimal payoffs are $U_d^* = U_d|_{r_d<\hat{r}_d}^1(\widetilde{r}_d^*)$, $U_a^* = (1-\theta)r_a^* - \theta c_f - (1-\theta)c_s$.

4 Sensitivity Analysis and Impact of Human Factors

In this section, we study the impact of the security budget and human factors on the equilibrium attack/defense strategy by using sensitivity analysis and prospect theory. As shown in Sect. 3.2, the equilibrium is closely related to the structure of the set Ω, which can vary for different cases shown in Fig. 2. These cases can be distinguished by the relationship between $\bar{r}_d = B - \mu$ and $\hat{r}_d$. We split the region $r_d \geq 0$ into three sub-regions: sub-region I refers to the interval $[0, \bar{r}_d)$; sub-region II is equal to $[\bar{r}_d, \hat{r}_d)$; sub-region III refers to $[\hat{r}_d, \infty)$. Three sub-regions coexist in Fig. 2a, and sub-region II vanishes in Fig. 2b.



(a) Case 1: $\bar{r}_d < \hat{r}_d$. (b) Case 2: $\bar{r}_d > \hat{r}_d$.

Fig. 2. Ω in two cases. $f(r_d)$ is defined in Proposition 1. As $\bar{r}_d$ increases, sub-region II gradually vanishes till $\bar{r}_d = \hat{r}_d$. Sub-region I remains $[0, \hat{r}_d)$ when $\bar{r}_d > \hat{r}_d$.

4.1 Impact of the Security Budget

The security budget B affects both on the optimal investment r_d^* and the defender's optimal utility U_d^*. We first note that large budget B barely affects r_d^* and U_d^* as observed in Fig. 2b. This is because Ω is no longer determined by

B and $\mathrm{d}U_d|^1_{r_d<\hat{r}_d}/\mathrm{d}B = 0$. In this scenario, the defender compares $U_d|^1_{r_d<\hat{r}_d}(\widetilde{r}^*_d)$ in sub-region I and $-\hat{r}_d$ to determine which equilibrium strategy to use. To look into $\widetilde{r}^*_d$, since $U_d|^1_{r_d<\hat{r}_d} = -r_d - (1-\theta)w$, we have

$$\frac{\mathrm{d}U_d|^1_{r_d<\hat{r}_d}}{\mathrm{d}r_d} = 0 \quad \Rightarrow \quad \theta' = \frac{1}{w}.$$

We call this value $\frac{1}{w}$ the *critical sensitivity threshold* as it determines whether the increment of security investment helps improve the defender's payoff or not. If the network defense is not sensitive enough to the security investment, i.e., $\theta'(r_d) \leq \frac{1}{w}$, the defender will suffer more loss as she invests more. This is because the investment in security cannot provide strong enough defense to suppress attack threats. Conversely, if the investment can bring sufficient security improvement, i.e., $\theta'(r_d) > \frac{1}{w}$, the defender can benefit more from more investment.

If we lower the budget B, we arrive at the scenario shown in Fig. 2a. The payoff $U_d|^1_{r_d<\hat{r}_d}$ and the effective defense threshold in sub-region I remains the same as in the cases of large budget B. While in sub-region II, we have $U_d|^1_{\hat{r}_d\leq r_d<\bar{r}_d} = -\theta r_d - (1-\theta)(B+\lambda w)$, and

$$\frac{\mathrm{d}U_d|^1_{\hat{r}_d\leq r_d<\bar{r}_d}}{\mathrm{d}r_d} = 0 \quad \Rightarrow \quad \theta' = \frac{\theta}{B+\lambda w - r_d} < \frac{1}{w},$$

which implies that the critical sensitivity threshold is reduced. This result means that the network defense becomes less sensitive to the investment. With the assumption that θ grows slower as the investment increases (verified in Sect. 5), the defender would spend more on the security investment.

The decrease in the critical sensitivity threshold reflects the interdependency between cyber and economic phases. Since the attacker knows the defender's budget, when the budget is sufficient, the attacker can always demand μ as the ransom. As the budget reduces, the attacker may not make any profit if he keeps demanding μ, because the defender may not be able to afford it. The less budget remains at stage 3 in the RG, the less the attacker can profit, and the less incentive he has to start the attack. In short, as the defender's budget reduces, the network defense becomes less sensitive to the investment, which incentivizes the defender to invest more rather than nothing to secure the target.

An interesting but counter-intuitive observation is that when the defender has a small budget, we have $\mathrm{d}U_d|^1_{\bar{r}_d\leq r_d<\hat{r}_d}/\mathrm{d}B = -(1-\theta) < 0$ and $\mathrm{d}(-\hat{r}_d)/\mathrm{d}B < 0$[3] in sub-region II and III, which implies that increasing the budget does not help improve the defender's payoff. This phenomenon has two reasons: the complete-information structure of the RG and the interdependency between the cyber and economic phases. The defender cannot invest much if she has a small budget, leading to a high probability of being compromised. Since the attacker knows the budget, he can always demand the remaining budget to make the most profit. For the defender, she either invests $\hat{r}_d$ to avoid the attack or invests some value less than $\hat{r}_d$ while facing the risk of being compromised. Her utility will go down

[3] See Appendix for the proof of $\mathrm{d}(-\hat{r}_d)/\mathrm{d}B < 0$.

in both ways if she increases her budget a bit. We name this phenomenon as the *budget dilemma*. We mention that the budget dilemma happens only when the budget is small. It disappears when the defender has a sufficient budget because her expected willingness to pay μ starts to dominate the attacker's ransom strategy.

To summarize, we arrive at the following insights. First, a sufficient budget corresponds to a fixed critical sensitivity threshold $\frac{1}{w}$. Conversely, a small budget reduces the threshold, which incentivizes the defender to invest more in network security. Second, the defender faces the budget dilemma for a small budget, but the dilemma disappears as the budget increases.

4.2 Impact of Human Factors and Prospect Theory

Humans have different cognitive preferences. In general, people are more averse to losses and less sensitive to gains; people inflate the belief for rare events and deflate for high-probability ones. Prospect theory captures human factors by

$$V(x) = \begin{cases} x^{\beta} & x \geq 0 \\ -\alpha(-x)^{\beta} & x < 0 \end{cases}, \qquad h(p) = \frac{p^{\zeta}}{p^{\zeta} + (1-p)^{\zeta}}, \tag{13}$$

where $V(x)$ and $h(p)$ are biased utility and weighted probability, respectively, and α, β, ζ are prospect parameters.

In the RG, we assume that the attacker is completely rational and the human factors are embodied in the defender's side (λ and w). Prospect theory provides a way to understand the impact of these human factors on the game equilibrium.

We denote the biased untrusted level λ and willingness to pay w as $\widetilde{\lambda}$ and $\widetilde{w}$. The biased expected willingness to pay becomes $\widetilde{\mu} = (1-\widetilde{\lambda})\widetilde{w}$. Note that $-w$ describes the defender's potential loss. From (13), the defender expects a larger loss $-\widetilde{w} < -w$ during decision-making. The biased $\widetilde{\mu}$ also depends on λ. For large λ (the defender barely trust the attacker), $\widetilde{\lambda}$ is deflated and thus $\widetilde{\mu} > \mu$. For small λ (the defender trusts the attacker), $\widetilde{\lambda}$ is inflated and $1-\widetilde{\lambda}$ is deflated. The value of $\widetilde{\mu}$ depends on specific values of $\widetilde{w}$ and $\widetilde{\lambda}$.

We first look into how human factors influence the critical investment $\hat{r}_d$. When the budget is sufficient (see Fig. 2b), an increased $\widetilde{\mu}$ leads to an increased $\hat{r}_d$. This means that the defender has to invest more in network security to eliminate the attack risk if she has a higher expected willingness to pay. When the budget is small (see Fig. 2a), $\hat{r}_d$ is no longer affected by $\widetilde{\mu}$ and thus remain unchanged. Therefore, human factors affect the critical investment $\hat{r}_d$ in a way such that $\hat{r}_d$ has a positive correlation in $\widetilde{\mu}$ for only for sufficient budget B.

For the optimal investment r_d^*, the defender either takes $\hat{r}_d$ or some value between $[0, \hat{r}_d)$ as r_d^*, depending on which strategy yields a larger payoff. Note that $\widetilde{w}$ reduces the critical sensitivity threshold, which implies that the defender's payoff can be further improved by more investment compared with the unbiased case. We conclude that if the defender's optimal investment $r_d^* \neq \hat{r}_d$ in the unbiased case, human factors will enhance r_d^*; if the defender takes $r_d^* = \hat{r}_d$ in the unbiased case, human factors affect r_d^* by following the variation trend of $\widetilde{\mu}$.

As for the defender's optimal payoff U_d^*, we focus on the case where the untrusted level λ is small (e.g., $\lambda = 0.3$). From (10) we see that the defender's payoff in sub-region I is always decreasing because $\widetilde{w} > w$. Besides, $\widetilde{\lambda}$ is inflated, causing a decrease in the defender's payoff in sub-region II. In sub-region III, the defender's payoff becomes $-\hat{r}_d$, and it is influenced by $\widetilde{\mu}$. To conclude, for small λ, if the defender's optimal investment $r_d^* \neq \hat{r}_d$ in the unbiased case, her optimal payoff is always worsened by the inflated $\widetilde{w}$; if the defender takes $r_d^* = \hat{r}_d$ in the unbiased case, human factors affect U_d^* by following the variation trend of $\widetilde{\mu}$.

The rational attacker may profit from the defender's bias. From (7), the attacker demands ransom $r_a = \min\{B - r_d^*, \mu\}$. Therefore, when the budget B is sufficient while the security investment r_d^* is small such that $B - r_d^* \geq \mu$, the attacker demands $r_a = \mu$ and he can receive more profit if $\widetilde{\mu} > \mu$. However, as r_d^* increases, the attacker can only demand $r_a = B - r_d^*$. So human factors influence his payoff in the exact opposite way as r_d^*. Specifically, if we have $\widetilde{\mu} > \mu$, the attacker in fact receives a worse payoff compared with the unbiased case.

5 Case Studies and Discussion

In this section, we use a case study over a prototypical industrial IoT network to analyze the impact of ransomware attacks. We conduct simulations to evaluate the performance of the cyber MG defense mechanism, which serves as the cyber risk assessment for future security decision-making. We analyze the equilibrium strategy in the RG and discuss the influences of limited budget and prospect theory on the equilibrium strategy.

5.1 Model Implementation

Typically, industrial networks are segregated into several interconnected sub-level networks based on the usage [16,25]. We consider the following network with four layers shown in Fig. 3, where the massively interconnected devices are grouped by their functions for simplicity. Each entity can represent a set of agents with similar functions. The target asset in our case is the production unit (e.g., a robotic arm) which can generate profit. We consider a locker ransomware attack, where the infected target will be locked and lose all its functionality. The target value can be assessed by the real loss in production if the target is locked. Since the value can vary dramatically for different applications, we use a normalized value $w = 10$ to denote the target value. Other money-related values can be converted to have the same magnitude as the w. We also set the untrusted level $\lambda = 0.3$ based on empirical results of the ransomware attack.

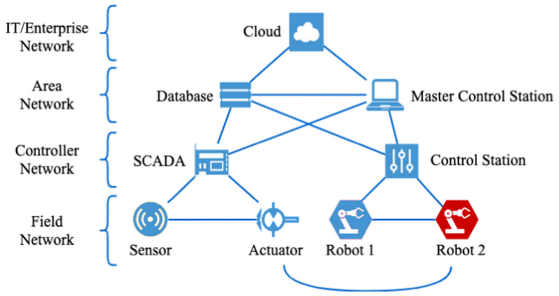


Fig. 3. A prototypical industrial IoT network consists of four network layers including IT/enterprise network, area network, controller network and field network. The target node of the attacker is Robot 2.

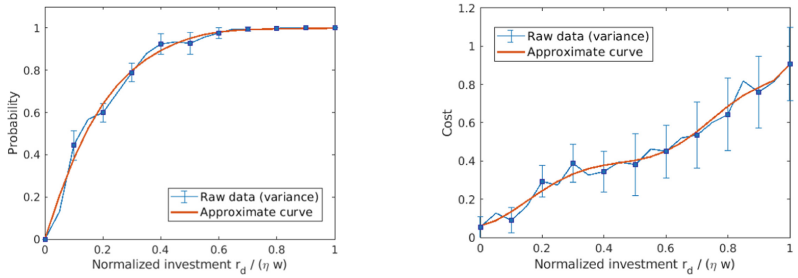
5.2 Outcome of Cyber Markov Game

In the cyber MG, we refer to the Common Vulnerability Scoring System (CVSS) [19] to describe the cost $C_e(e)$ of mounting an attack through edge $e \in \mathcal{E}$. CVSS provides a risk measurement of edge vulnerabilities. We convert the score into the same magnitude as w and simulates the MG under this setting.

The attacker establishes the initial foothold at the cloud in the IT network layer, penetrating through sub-level networks to infect the target. The defender invests $r_d \in [0, B]$ to change the transition probability $\gamma(r_d, e)$ in the cyber MG. In this case study, we assume that the influence of security investment is equivalent on each edge, i.e., $\gamma(r_d, e) = \widetilde{\gamma}(r_d)$, $\forall e \in \mathcal{E}$. In our case, we select

$$\widetilde{\gamma}(r_d) = 1 - \sqrt{\frac{r_d}{\eta w}},$$

where η is the scaling factor to measure the effectiveness of the investment. To obtain the average results of the cyber MG, we choose $\eta = 2$ and sample 40 points of $(r_d/\eta w)$ at equal intervals between 0 and 1. We simulate the cyber MG for $N = 5000$ times under each r_d to evaluate the empirical successful defense probability $\theta(r_d)$ and the attack cost $c_f(r_d)$, which are shown in Fig. 4. The additional attack cost for a successful attack is set to $\delta = 0.5$.



(a) Empirical defense probability $\theta(r_d)$. (b) Empirical attack cost $c_f(r_d)$.

Fig. 4. Simulation outcome with variance and approximations of the cyber MG

5.3 Impact of Budget

Under the parameter setting, we have $\mu = 7$. Thus, we vary B from 9 to 16 to study how the defense strategy changes under different budgets.

The derivative of approximated θ function in Fig. 5 shows that the network defense is highly sensitive to the investment at the very beginning and gradually losses its sensitivity as the investment increases. We observe that the critical sensitivity threshold in Fig. 5 splits the investment $r_d \geq 0$ into two regions, and the r_d on the left-hand side is always above the critical sensitivity threshold. This implies that the defender can always improve her payoff by investing some value rather than nothing. Therefore, the zero investment strategy is ruled out.

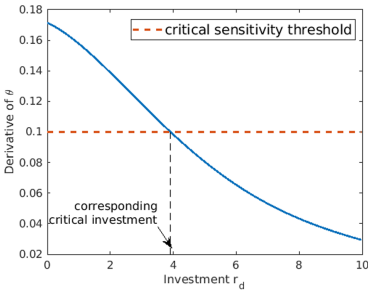
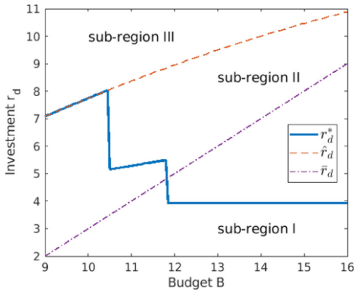


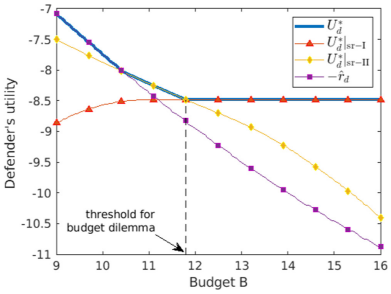
Fig. 5. Sensitivity of the network defense.

The optimal investment strategy r_d^* and the defender's optimal payoff in three sub-regions are shown in Fig. 6a and Fig. 6b respectively. The variation of $\hat{r}_d$ and $\bar{r}_d$ are also plotted in Fig. 6a. For a small budget of B, the length of sub-region I is short. The entire sub-region can be above the threshold. So the defender will not seek the optimal investment in this sub-region. For a better payoff, the defender will invest more. Thus, the optimal investment is $\hat{r}_d$ as shown in Fig. 6a.

As the budget improves, we see that the value of $\hat{r}_d$ also increases as discussed in Sect. 4.1. However, the network defense becomes less sensitive, which means that the defender may not be better off if she keeps investing $\hat{r}_d$. So she would consider the investment strategy in sub-region I and II instead of $\hat{r}_d$. As shown in Fig. 6a, the defender no longer invests $\hat{r}_d$ when the budget reaches $B = 10.5$. She starts to take some value in sub-region II as the optimal investment. Note that r_d^* is still not in sub-regions I because the size of sub-regions I is still small and the entire region is still above the critical sensitivity threshold. As we keep improving the budget, $\hat{r}_d$ keeps increasing and sub-region II gradually vanishes. As the budget reaches $B = 11.8$, the defender starts to take values in sub-region I as the optimal investment.



(a) Optimal investment strategy. Three sub-regions are split by $\hat{r}_d$ and $\bar{r}_d$.



(b) Defender's optimal payoff. We can also observe the udget dilemma.

Fig. 6. Defender's optimal investment strategy and optimal payoff.

We can observe the budget dilemma in Fig. 6b, where the defender's payoff is decreasing as the budget goes up when the budget is small. The decrements stop when $B = 11.8$ and remain unchanged with a larger budget, which coincides with the analysis that the budget dilemma disappears for a large budget. Note that in this case, we even do not need to arrive at the situation in Fig. 2b to suppress the budget dilemma, as the budget after $B = 11.8$ already stops influencing the optimal utility.

To conclude, when the defender has a small budget, she should invest $\hat{r}_d$ to eliminate the threat of attack. When the budget is sufficient, the defender can choose some other investment less than $\hat{r}_d$ to optimize her payoff. We note that the large budget offsets the defender's initiative to protect the target. This is because (a) network defense becomes less sensitive to the security investment and (b) paying the ransom becomes acceptable compared with the security expenditure. Therefore, the budget reflects the trade-off between the security investment and redeeming the target, which further implies the interdependency between cyber and economic phases in the ransomware attack.

5.4 Prospect Theory

To study the impact of human factors on $\hat{r}_d, r_d^*, U_d^*, r_a^*$, we discuss two cases with small budget $B = 14$ and large budget $B = 20$ respectively. We apply typical perspective parameters $\alpha = 2.25, \beta = 0.88, \zeta = 0.69$ in [8]. Under these parameters, the biased willingness to pay $\widetilde{\mu} = 12.47 > \mu$, which implies human factors increases the μ. We mention that $B = 14$ a small budget for the biased case in this subsection, although it is large enough for the unbiased case. The results are summarized in Table 2

Followed by the analysis in Sect. 4.2, we observe that $\hat{r}_d$ remains unchanged for small budget in Table 2a, but increases for large budget because of inflated $\widetilde{\mu}$, shown in Table 2b. Meanwhile, the biased $\widetilde{w}$ reduces the critical sensitivity threshold regardless of the budget, which requires the defender to invest more to be better off. Thus, the optimal investment r_d^* increases compared with the

unbiased case both in Table 2a–2b. Likewise, the inflated $\widetilde{w}$ and $\widetilde{\mu}$ can reduce the defender's optimal payoff U_d^* despite the budget. This shows that human factors in this case in fact worsen the defender's situation.

The attacker does not profit from the bias of the defender either. In both cases we study here, the defender selects r_d^* such that $B - r_d^* < \mu$. Therefore, the defender can only demand $r_a = B - r_d^*$. Since r_d^* is enlarged in both cases, the ransom r_a is also reduced, which is observed in Table 2a–2b.

Table 2. Impact of human factors under different budget scenarios.

	$\hat{r}_d$	r_d^*	U_d^*	r_a^*
unbiased	10	3.93	−8.48	10.08
biased	10	6.6	−9.84	7.4

(a) Small budget $B = 14$.

	$\hat{r}_d$	r_d^*	U_d^*	r_a^*
unbiased	11.9	3.93	−8.48	16.07
biased	12.3	6.55	−10.85	13.45

(b) Large $B = 20$.

6 Conclusion

In this paper, we have investigated the ransomware attack in networks by establishing an MPMS-GiG framework. The proposed framework captures both cyber and economic phases of the ransomware attack and provides a holistic analysis of the interdependency between them. The equilibrium characterizes the defense-payment strategy with budget constraints. The sensitivity analysis suggests that the network security investment is more effective to combat the ransomware attack when the defender has a small budget. It is also recommended to increase the investment to reduce the defender's overall loss under a small budget. We also observe the budget dilemma when the defender's budget is insufficient, which reflects the interdependency between cyber and economic phases in the ransomware attack. Human factors also contribute to the equilibrium attack/defense strategy. Being risk-averse can drop the defender's overall loss because she values the target more. It is also worth noting that the attacker gains less from a biased defender as she prefers to invest more in network security. Case studies show the equilibrium attack/defense strategy over a prototypical industrial IoT network and successfully corroborates the results in the paper.

For future work, we would consider the ransomware attack with incomplete information. For example, the attacker may not know exactly the defender's willingness to pay except for a prior distribution. Another direction would be to study cyber insurance and its impact on the equilibrium of ransomware attacks.

A Proof in the Budget Dilemma

Recall that $\hat{r}_d$ is the root of $g(r_d, B) = B - r_d - f(r_d)$ for small B. Assume the differentiability of θ and c_f, it is easy to show that $f'(r_d) > 0$. Using the implicit

function theorem, we can find a function $\hat{r}_d = h(B)$ in the neighborhood of $(B, \hat{r}_d)$ where $g(r_d, B) = 0$. Hence, we have $\frac{\mathrm{d}\hat{r}_d}{\mathrm{d}B} = -(-1 - f'(\hat{r}_d))^{-1} = \frac{1}{1+f'(\hat{r}_d)} > 0$. The defender's utility is $-\hat{r}_d$ if she chooses to invest $\hat{r}_d$. Thus, $\frac{\mathrm{d}(-\hat{r}_d)}{\mathrm{d}B} < 0$.

References

1. Colonial pipeline ransomware attack. Wikipedia. https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack. Accessed 20 July 2021
2. Aidan, J.S., Verma, H.K., Awasthi, L.K.: Comprehensive survey on petya ransomware attack. In: 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS), pp. 122–125. IEEE (2017)
3. Braue, D.: Global ransomware damage costs predicted to exceed $265 billion by 2031 (2021). https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/. Accessed 20 July 2021
4. Caporusso, N., Chea, S., Abukhaled, R.: A game-theoretical model of ransomware. In: Ahram, T.Z., Nicholson, D. (eds.) AHFE 2018. AISC, vol. 782, pp. 69–78. Springer, Cham (2019). https://doi.org/10.1007/978-3-319-94782-2_7
5. Cartwright, E., Hernandez Castro, J., Cartwright, A.: To pay or not: game theoretic models of ransomware. J. Cybersecur. **5**(1), tyz009 (2019)
6. Di Pietro, R., Mancini, L.V.: Intrusion Detection Systems, vol. 38. Springer Science & Business Media, Heidelberg (2008)
7. Flores, R.: The impact of modern ransomware on manufacturing networks (2020). https://www.trendmicro.com/en_us/research/20/l/the-impact-of-modern-ransomware-on-manufacturing-networks.html. Accessed 20 July 2021
8. Fox, C.R., Poldrack, R.A.: Prospect theory and the brain. In: Neuroeconomics, pp. 145–173. Elsevier (2009)
9. Hernandez-Castro, J., Cartwright, E., Stepanova, A.: Economic analysis of ransomware. Available at SSRN 2937641 (2017)
10. Huang, L., Zhu, Q.: Adaptive strategic cyber defense for advanced persistent threats in critical infrastructure networks. ACM SIGMETRICS Perform. Eval. Rev. **46**(2), 52–56 (2019)
11. Inayat, Z., Gani, A., Anuar, N.B., Khan, M.K., Anwar, S.: Intrusion response systems: foundations, design, and challenges. J. Netw. Comput. Appl. **62**, 53–74 (2016)
12. Kalaimannan, E., John, S.K., DuBose, T., Pinto, A.: Influences on ransomware's evolution and predictions for the future challenges. J. Cyber Secur. Technol. **1**(1), 23–31 (2017)
13. Kearns, M., Mansour, Y., Singh, S.: Fast planning in stochastic games. arXiv preprint arXiv:1301.3867 (2013)
14. Kivilevich, V.: Ransomware gangs are starting to look like ocean's 11 (2021). https://ke-la.com/ransomware-gangs-are-starting-to-look-like-oceans-11/. Accessed 20 July 2021
15. Laszka, A., Farhang, S., Grossklags, J.: On the economics of ransomware. In: Rass, S., An, B., Kiekintveld, C., Fang, F., Schauer, S. (eds.) Decision and Game Theory for Security. GameSec 2017. Lecture Notes in Computer Science, vol. 10575, pp. 397–417. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-68711-7_21
16. Mayoral-Vilches, V., Pinzger, M., Rass, S., Dieber, B., Gil-Uriarte, E.: Can ros be used securely in industry? red teaming ros-industrial. arXiv preprint arXiv:2009.08211 (2020)

17. Noureddine, M.A., Fawaz, A., Sanders, W.H., Başar, T.: A game-theoretic approach to respond to attacker lateral movement. In: Zhu, Q., Alpcan, T., Panaousis, E., Tambe, M., Casey, W. (eds.) GameSec 2016. LNCS, vol. 9996, pp. 294–313. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-47413-7_17
18. Richardson, R., North, M.M.: Ransomware: evolution, mitigation and prevention. Int. Manag. Rev. **13**(1), 10 (2017)
19. Scarfone, K., Mell, P.: An analysis of CVSS version 2 vulnerability scoring. In: 2009 3rd International Symposium on Empirical Software Engineering and Measurement, pp. 516–525. IEEE (2009)
20. Tonn, G., Kesan, J.P., Zhang, L., Czajkowski, J.: Cyber risk and insurance for transportation infrastructure. Transp. Policy **79**, 103–114 (2019)
21. Touchette, F.: The evolution of malware. Netw. Secur. **2016**(1), 11–14 (2016)
22. Tuptuk, N., Hailes, S.: Security of smart manufacturing systems. J. Manuf. Syst. **47**, 93–106 (2018)
23. Yaqoob, I., et al.: The rise of ransomware and emerging security challenges in the internet of things. Comput. Netw. **129**, 444–458 (2017)
24. Zahra, S.R., Chishti, M.A.: Ransomware and internet of things: a new security nightmare. In: 2019 9th International Conference on Cloud Computing, Data Science & Engineering (confluence), pp. 551–555. IEEE (2019)
25. Zhu, Q., Rass, S., Dieber, B., Vilches, V.M.: Cybersecurity in robotics: Challenges, quantitative modeling, and practice. arXiv preprint arXiv:2103.05789 (2021)