Cost-benefit Analysis Toward Designing Efficient Education Programs for Household Security

N'guessan Yves-Roland Douha[1], Bernard Ousmane Sane[2], Masahiro Sasabe[1],
Doudou Fall[1], Yuzo Taenaka[1], and Youki Kadobayashi[1]
[1]Division of Information Science, Nara Institute of Science and Technology, Ikoma, Japan
email: {douha.nguessan_yves-roland.dn6, sasabe, doudou-f, yuzo, youki-k}@is.naist.jp
[2]Faculty of Science and Technology, University Cheikh Anta Diop, Dakar, Senegal
email:bernardousmane.sane@ucad.edu.sn

***Abstract*—The human factor is still a crucial issue in the security chain. People who will live in a smart home might be exposed to many cyber threats due to the remaining lack of Internet of Things (IoT) device security. Cybersecurity awareness training could help households to become more resilient to face cyberattacks. However, the financial costs of training programs and the significant amount of time needed to notice security countermeasures could refrain many smart-home users from engaging in cybersecurity education. In this paper, we propose a game-theoretic approach to analyze the security investment cost-benefit of households. Our numerical results show that the increase of quality of services accessible in a smart home and the security rewards for noticing security countermeasures compared to the potential impacts of cyberattacks will increase the payoffs of households and reinforce the security behaviors. Our results also emphasize the urgent need to address human security toward a more resilient smart home.**

***Keywords*-Cost-benefit analysis; game theory; household security awareness; smart-home security.**

I. Introduction

Human factor is a recognized issue in information security and many researchers have proposed security awareness and training as a solution [1]–[3]. With the recent advancement of technologies such as ubiquitous systems and human-computer interaction, user security awareness issues are back on the table. Households, especially those who are interested in smart homes, a branch of ubiquitous computing that incorporates smartness into dwellings for a better quality of life [4], might face additional security challenges such as lack of device management, insecure software/firmware, and poor physical security [5]. A recent survey on cybersecurity education shows that adults are worried about cyber threats and the safety and security of children [6]. Given that user awareness of security countermeasures directly influence information systems misuses [7], cybersecurity awareness education could be an effective solution to empower households, including children [8] and senior citizens [9], with knowledge and skills to reduce the success rate of cyberattacks exploiting human vulnerabilities in homes.

However, a critical obstacle to adopting those cybersecurity education programs is the financial costs and resources [10]. For example, regarding employees' training, companies seek to minimize their budget regarding costs that are not tight to their operations. Furthermore, individuals are willing to take cybersecurity awareness training only if their employers sponsor them [6]. Similarly, we assume that the financial costs of cybersecurity training could be challenging for households.

Cost-benefit studies are important to understand the potential value of investing in cybersecurity education programs. Existing security cost-benefit analysis include the work of Zeng [11] who focuses on digital right management products. The author uses the stochastic Petri nets to simulate and predict the impact of the deployment of these digital systems on normal business processes. Furthermore, Zhang et al. [12] propose a new theoretical framework for conducting a cost-benefit analysis of cybersecurity awareness training programs to evaluate different costs and benefits on a company's optimal degree of security. Regarding household security awareness training, we need to identify the minimum investment of time and money that will encourage households to engage in cybersecurity education programs.

To the best of our knowledge, prior research have not addressed households' needs for cybersecurity training. The purpose of the present work is to address this research gap using a game-theoretic approach. We choose this approach to analyze the impacts of households' decision-making of investing in security training and identify the payoffs of each decision.

We summarize the research contributions below.

- We provide a game-theoretical approach to analyze the cost-effectiveness of households' investments in cybersecurity awareness education.
- We investigate the pure and mixed Nash equilibria of the proposed game.
- We propose graphical representations to analyze investment costs and households' payoffs.

We structure the remainder of this paper as follows. Section II presents the related work. Section III introduces the proposed game model, presents the normal-form game, and analyzes the pure and mixed equilibria. Section IV presents the numerical results. Section V discusses the findings of the paper. Section VI concludes the work.

II. Related Work

This section describes the related work that uses a game-theoretic approach to analyze security investment cost-benefits.

Generally speaking, IT security investment reflects decision-making resulting from an analysis of potential costs and

 ISBN: 978-1-61208-919-5

benefits. Thus one might consider decision theory as essential support for this purpose. However, Cavusoglu et al. [13] show that game-theoretic approaches are more suitable than traditional decision-theoretic risk management techniques regarding IT security investment, especially when considering that attackers are strategic. Furthermore, they find that in a game including two players: a firm and an attacker, the firm maximizes its payoff in a sequential game when the firm is the leader and the attacker is the follower. This result shows that it is possible to use a game-theoretic approach to address the research problem of our work. Sun et al. [14] propose a game model to address information security problems in the mobile electronic commerce industry chain. They introduce a penalty parameter that affects organizations that do not invest in IT security. The results indicate that reducing investment costs is essential to promote information security investments. Otherwise, the regulation of a penalty parameter might help to encourage those investments. In the present paper, we propose a reward parameter for users who take cybersecurity training and notice security countermeasures. Qian et al. [15] propose a game model based on information sharing and security investment between strategies for the two firms. The Nash equilibrium analysis shows that firms share no information when they make decisions individually. Furthermore, Zuo et al. [16] use a game-theoretic approach and Nash equilibrium to analyze information security cost investment to improve network security. The existing research and game models do not address security cost-benefits issues regarding households awareness education, which are the main focus of this paper.

In the literature, the studies on user cybersecurity awareness-based cost-benefit analysis are limited. Furthermore, the related work on security investment cost-benefit analysis only consider corporate areas, which are different from households' reality to some extent. In this new era of the Internet of Things (IoT), households' devices and data are valuable to attackers. We need to address issues, such as cost-benefit, related to households' cybersecurity education to avoid large-scale cyberattacks and ensure people's safety and security.

III. Proposed Game Model

This section introduces and analyzes our game model through four subsections. Subsection A describes the system. Subsection B defines the parameters of the game. Subsection C presents the normal-form game. Subsection D investigates the pure and mixed Nash equilibria of the proposed game.

A. System

We consider a smart home comprising three types of households: adults ($User_1$), children ($User_2$), and senior citizens ($User_3$). This house is composed of many IoT devices that are convenient for every household. For example, $User_1$ could use IP cameras and smart door locks to ensure the house's physical security. $User_2$ could use a smart TV and smart speakers for advertisement. $User_3$ could use a smart pill dispenser or smartwatch for healthcare.

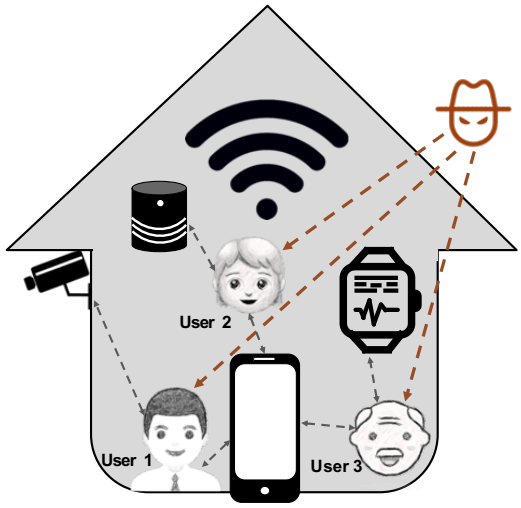

Fig. 1. Illustration of the proposed model.

As illustrated in Figure 1, an attacker could gain interests in compromising that house for various motives, such as accessing private information, using IoT-based home devices to execute Distributed Denial-of-Service (DDoS) attacks, the absence of resistance such as a dedicated cybersecurity team. Furthermore, attackers could discern that households might notice part of security countermeasures, such as changing default passwords, using multi-factor authentication, or recognizing and avoiding phishing links, which could give them various entry points. These attacks could be effective by targeting $User_1$, $User_2$, or $User_3$.

B. Game Modeling

Let T_i and $\bar{T}_i$, respectively, be the events $User_i$ has got cybersecurity awareness training, and $User_i$ has not got cybersecurity awareness training with $1 \leq i \leq 3$.

Let A be the event that an attacker compromises a user. We consider $P(A/T_i)$ the probability of an attacker to compromise $User_i$ given that $User_i$ has got cybersecurity awareness training, and $P(A/\bar{T}_i)$ the probability of an attacker to compromise $User_i$ given that $User_i$ has not got cybersecurity awareness training.

We assume that

$$P(A/T_1) = P(A/T_2) = P(A/T_3). \quad (1)$$

$$P(A/\bar{T}_1) = P(A/\bar{T}_2) = P(A/\bar{T}_3). \quad (2)$$

We have (1) and (2) because how users could react to an ongoing cyberattack depends more on their level of cybersecurity awareness than on their age.

Let S and $\bar{S}$, respectively, be the events that a user notices security countermeasures, and a user notices part of security countermeasures. We consider $P(A/T_i \cap S)$ the probability of an attacker compromising $User_i$ given that $User_i$ has got cybersecurity awareness training and notices security countermeasures, and $P(A/T_i \cap \bar{S})$ the probability of an attacker compromising $User_i$ given that $User_i$ has got cybersecurity

awareness training and notices part of security countermeasures. Like (1) and (2), we assume that

$$P(A/T_1 \cap S) = P(A/T_2 \cap S) = P(A/T_3 \cap S). \quad (3)$$

$$P(A/T_1 \cap \bar{S}) = P(A/T_2 \cap \bar{S}) = P(A/T_3 \cap \bar{S}). \quad (4)$$

We assume that, for a given $User_i$ with $1 \leq i \leq 3$,

$$P(A/T_i \cap S) < P(A/T_i \cap \bar{S}) < P(A/\bar{T}_i). \quad (5)$$

We have (5) because $User_i$ is more secure in the event $T_i \cap S$ than in $T_i \cap \bar{S}$ and more secure in the event $T_i \cap \bar{S}$ than in $\bar{T}_i$. We also assume that

$$0 < P(T_3 \cap S) \leq P(T_2 \cap S) \leq P(T_1 \cap S) \leq 1. \quad (6)$$

$$0 < P(T_1 \cap \bar{S}) \leq P(T_2 \cap \bar{S}) \leq P(T_3 \cap \bar{S}) \leq 1. \quad (7)$$

Furthermore, we have (6) and (7) because many challenges, such as those with cognitive or physical aspects, could regularly hinder senior citizens from noticing security countermeasures. Furthermore, we consider that the basis of knowledge of adults is greater than those of children. Considering every user faces the same potential threats, children might not notice various countermeasures out of ignorance because their cybersecurity-training content might be less intensive than those of adults.

Moreover, we consider the following $User_i$'s costs: c_{mi} the monetary costs related to the event T, c_{ti} the time costs related to the event S, and $c_{t'i}$ the time costs related to the event $\bar{S}$. We have

$$0 \leq c_{m1} \leq c_{m2} \leq c_{m3}. \quad (8)$$

$$0 \leq c_{t3} \leq c_{t2} \leq c_{t1}. \quad (9)$$

$$0 \leq c_{t'i} < c_{ti}. \quad (10)$$

We have (8) because $User_2$ and $User_3$ might require specific cybersecurity awareness training, which could be more expensive than the training of $User_1$. Furthermore, we consider that it is harder to provide training materials and resources to get $User_3$ than $User_2$ involved. Therefore, the training cost of $User_3$ is more than the training cost of $User_2$, which is more than that of $User_1$. We have (9) because we assume that $User_1$ might invest much more time than $User_2$ and $User_3$ to notice security countermeasures. Furthermore, the effect of age $User_3$'s on memory makes us consider that this user might spend less time noticing security countermeasures than $User_2$. We have (10) because $User_i$ spends much more time in the event S than in the event $\bar{S}$.

We also consider δ ($\delta > 0$) the costs of a cyberattack on a smart home which could involve interruption costs of smart-home services (e.g., home automation, electric power, healthcare, entertainment, the Internet). Note that δ applies to every user. Furthermore, we consider θ ($\theta > 0$) the costs associated with security breaches following an exploit through a user's device. This cost is assigned to the compromised user only. We assume that $\delta > \theta$. Note that $\theta = 0$ for a user who is not attacked and for a user who notices security countermeasures. We assume that

$$\theta P(A/T_i \cap \bar{S}) + \delta \geq c_{mi} + c_{ti} > c_{mi} + c_{t'i}. \quad (11)$$

θ is different from λ ($\lambda \geq 0$), which is the cost associated with privacy incidents related to households. λ depends on households' income and social status. We decide to assign this cost to $User_1$ only because being in charge of home safety and security. While θ could relate to the quality of life (e.g., unavailability of services, a decrease in the sense of privacy and self-esteem), λ could relate to money (e.g., ransom requests). Finally, we consider φ ($\varphi > 0$), the parameter that quantifies all the comforts and benefits a user could enjoy when living in a smart home. φ has the same value for every user. We also consider R the reward for noticing security countermeasures. Note that $R = 0$ for users who notice part of security countermeasures.

C. Normal-Form Game

We describe strategy sets of each player as matrices. Table I, Table II, and Table III, respectively, present the normal-form games of an attacker targeting $User_1$, $User_2$, and $User_3$. In these tables, each cell from Line 7 - Column 4 represents the payoffs of each player. In each cell, the first line shows $User_1$'s payoffs, the second line shows $User_2$'s payoffs, the third line shows $User_3$'s payoffs, and the fourth line shows the attacker's payoffs. As an illustration, we explain the payoffs of $User_1$ and the attacker described in Table I.

When $User_1$ chooses the events T and S, $User_1$'s payoff is $\varphi - c_{m1} - c_{t1} + R$ and the attacker's payoff is 0. Note that in our model the attack fails (attacker's payoff = 0) if the target is a user who takes cybersecurity awareness training and notices security countermeasures. When $User_1$ chooses the events T and $\bar{S}$, $User_1$'s payoff is $\varphi - c_{m1} - c_{t'1} - \theta P(A/T_1 \cap \bar{S}) - \delta - \lambda$ and the attacker's payoff is $\theta P(A/T_1 \cap \bar{S}) + \delta + \lambda$. When $User_1$ chooses the event $\bar{T}$, $User_1$'s payoff is $\varphi - \theta P(A/\bar{T}_1) - \delta - \lambda$ and the attacker's payoff is $\theta P(A/\bar{T}_1) + \delta + \lambda$. Note that when the targeted user chooses the events $\bar{S}$ or $\bar{T}$, the attack affects the other users through the parameter δ. For example in Table I, the payoffs of $User_2$ and $User_3$ are respectively $\varphi - c_{m2} - c_{t2} + R - \delta$ and $\varphi - c_{m3} - c_{t3} + R - \delta$ when both users choose the event S and $User_1$, the target of the attacker, chooses the event $\bar{S}$.

D. Game Analysis

We aim to understand the rational decision-making of every player: users and the attacker from the perspective of Nash equilibrium. We analyze the best actions of players based on their payoffs. According to the Nash equilibrium, every rational player chooses an action that maximizes his or her payoff.

1) Pure Strategy Nash Equilibrium: It refers to a game in which every player's mixed strategy in a mixed strategy Nash equilibrium assigns probability 1 to a single action [17]. In pure strategy Nash equilibrium, a player plays his or her best

TABLE I
NORMAL FORM: AN ATTACKER TARGETS USER 1.

Attacker targets User 1			User 3						User 3		
			T						$\bar{T}$		
			S			$\bar{S}$					
			User 2			User 2			User 2		
			T		$\bar{T}$	T		$\bar{T}$	T		$\bar{T}$
			S	$\bar{S}$		S	$\bar{S}$		S	$\bar{S}$	
User 1	T	S	$\varphi - c_{m1} - c_{t1} + R;$ $\varphi - c_{m2} - c_{t2} + R;$ $\varphi - c_{m3} - c_{t3} + R;$ 0	$\varphi - c_{m1} - c_{t1} + R;$ $\varphi - c_{m2} - c_{t'2};$ $\varphi - c_{m3} - c_{t3} + R;$ 0	$\varphi - c_{m1} - c_{t1} + R;$ $\varphi;$ $\varphi - c_{m3} - c_{t3} + R;$ 0	$\varphi - c_{m1} - c_{t1} + R;$ $\varphi - c_{m2} - c_{t2} + R;$ $\varphi - c_{m3} - c_{t'3};$ 0	$\varphi - c_{m1} - c_{t1} + R;$ $\varphi - c_{m2} - c_{t'2};$ $\varphi - c_{m3} - c_{t'3};$ 0	$\varphi - c_{m1} - c_{t1} + R;$ $\varphi;$ $\varphi - c_{m3} - c_{t'3};$ 0	$\varphi - c_{m1} - c_{t1} + R;$ $\varphi - c_{m2} - c_{t2} + R;$ $\varphi;$ 0	$\varphi - c_{m1} - c_{t1} + R;$ $\varphi - c_{m2} - c_{t'2};$ $\varphi;$ 0	$\varphi - c_{m1} - c_{t1} + R;$ $\varphi;$ $\varphi;$ 0
		S	$\varphi - c_{m1} - c_{t1} - \theta P(A/T_1 \cap \bar{S}) - \delta - \lambda;$ $\varphi - c_{n2} - c_{t2} + R - \delta;$ $\varphi - c_{n3} - c_{t3} + R - \delta;$ $\theta P(A/T_1 \cap \bar{S}) + \delta + \lambda;$	$\varphi - c_{m1} - c_{t1} - \theta P(A/T_1 \cap \bar{S}) - \delta - \lambda;$ $\varphi - c_{n2} - c_{t2} - \delta;$ $\varphi - c_{n3} - c_{t3} + R - \delta;$ $\theta P(A/T_1 \cap \bar{S}) + \delta + \lambda;$	$\varphi - c_{m1} - c_{t1} - \theta P(A/T_1 \cap \bar{S}) - \delta - \lambda;$ $\varphi - \delta;$ $\varphi - c_{n3} - c_{t3} + R - \delta;$ $\theta P(A/T_1 \cap \bar{S}) + \delta + \lambda;$	$\varphi - c_{m1} - c_{t1} - \theta P(A/T_1 \cap \bar{S}) - \delta - \lambda;$ $\varphi - c_{n2} - c_{t2} + R - \delta;$ $\varphi - c_{n3} - c_{t3} - \delta;$ $\theta P(A/T_1 \cap \bar{S}) + \delta + \lambda;$	$\varphi - c_{m1} - c_{t1} - \theta P(A/T_1 \cap \bar{S}) - \delta - \lambda;$ $\varphi - c_{n2} - c_{t2} - \delta;$ $\varphi - c_{n3} - c_{t3} - \delta;$ $\theta P(A/T_1 \cap \bar{S}) + \delta + \lambda;$	$\varphi - c_{m1} - c_{t1} - \theta P(A/T_1 \cap \bar{S}) - \delta - \lambda;$ $\varphi - \delta;$ $\varphi - c_{n3} - c_{t3} - \delta;$ $\theta P(A/T_1 \cap \bar{S}) + \delta + \lambda;$	$\varphi - c_{m1} - c_{t1} - \theta P(A/T_1 \cap \bar{S}) - \delta - \lambda;$ $\varphi - c_{n2} - c_{t2} + R - \delta;$ $\varphi - \delta;$ $\theta P(A/T_1 \cap \bar{S}) + \delta + \lambda;$	$\varphi - c_{m1} - c_{t1} - \theta P(A/T_1 \cap \bar{S}) - \delta - \lambda;$ $\varphi - c_{n2} - c_{t2} - \delta;$ $\varphi - \delta;$ $\theta P(A/T_1 \cap \bar{S}) + \delta + \lambda;$	$\varphi - c_{m1} - c_{t1} - \theta P(A/T_1 \cap \bar{S}) - \delta - \lambda;$ $\varphi - \delta;$ $\varphi - \delta;$ $\theta P(A/T_1 \cap \bar{S}) + \delta + \lambda;$
	T		$\varphi - \theta P(A/\bar{T}_1) - \delta - \lambda;$ $\varphi - c_{n2} - c_{t2} + R - \delta;$ $\varphi - c_{n3} - c_{t3} + R - \delta;$ $\theta P(A/\bar{T}_1) + \delta + \lambda;$	$\varphi - \theta P(A/\bar{T}_1) - \delta - \lambda;$ $\varphi - c_{n2} - c_{t2} - \delta;$ $\varphi - c_{n3} - c_{t3} + R - \delta;$ $\theta P(A/\bar{T}_1) + \delta + \lambda;$	$\varphi - \theta P(A/\bar{T}_1) - \delta - \lambda;$ $\varphi - \delta;$ $\varphi - c_{n3} - c_{t3} + R - \delta;$ $\theta P(A/\bar{T}_1) + \delta + \lambda;$	$\varphi - \theta P(A/\bar{T}_1) - \delta - \lambda;$ $\varphi - c_{n2} - c_{t2} + R - \delta;$ $\varphi - c_{n3} - c_{t3} - \delta;$ $\theta P(A/\bar{T}_1) + \delta + \lambda;$	$\varphi - \theta P(A/\bar{T}_1) - \delta - \lambda;$ $\varphi - c_{n2} - c_{t2} - \delta;$ $\varphi - c_{n3} - c_{t3} - \delta;$ $\theta P(A/\bar{T}_1) + \delta + \lambda;$	$\varphi - \theta P(A/\bar{T}_1) - \delta - \lambda;$ $\varphi - \delta;$ $\varphi - c_{n3} - c_{t3} - \delta;$ $\theta P(A/\bar{T}_1) + \delta + \lambda;$	$\varphi - \theta P(A/\bar{T}_1) - \delta - \lambda;$ $\varphi - c_{n2} - c_{t2} + R - \delta;$ $\varphi - \delta;$ $\theta P(A/\bar{T}_1) + \delta + \lambda;$	$\varphi - \theta P(A/\bar{T}_1) - \delta - \lambda;$ $\varphi - c_{n2} - c_{t2} - \delta;$ $\varphi - \delta;$ $\theta P(A/\bar{T}_1) + \delta + \lambda;$	$\varphi - \theta P(A/\bar{T}_1) - \delta - \lambda;$ $\varphi - \delta;$ $\varphi - \delta;$ $\theta P(A/\bar{T}_1) + \delta + \lambda;$

TABLE II
NORMAL FORM: AN ATTACKER TARGETS USER 2.

Attacker targets User 2			User 3						User 3		
			T						$\bar{T}$		
			S			$\bar{S}$					
			User 2			User 2			User 2		
			T		$\bar{T}$	T		$\bar{T}$	T		$\bar{T}$
			S	$\bar{S}$		S	$\bar{S}$		S	$\bar{S}$	
User 1	T	S	$\varphi - c_{m1} - c_{t1} + R;$ $\varphi - c_{m2} - c_{t2} + R;$ $\varphi - c_{m3} - c_{t3} + R;$ 0	$\varphi - c_{m1} - c_{t1} + R - \delta - \lambda;$ $\varphi - c_{m2} - c_{t'2} - \theta P(A/T_2 \cap \bar{S}) - \delta;$ $\varphi - c_{m3} - c_{t3} + R - \delta;$ $\theta P(A/T_2 \cap \bar{S}) + \delta + \lambda$	$\varphi - c_{m1} - c_{t1} + R - \delta - \lambda;$ $\varphi - \theta P(A/\bar{T}_2) - \delta;$ $\varphi - c_{m3} - c_{t3} + R - \delta;$ $\theta P(A/\bar{T}_2) + \delta + \lambda$	$\varphi - c_{m1} - c_{t1} + R;$ $\varphi - c_{m2} - c_{t2} + R;$ $\varphi - c_{m3} - c_{t'3};$ 0	$\varphi - c_{m1} - c_{t1} + R - \delta - \lambda;$ $\varphi - c_{m2} - c_{t'2} - \theta P(A/T_2 \cap \bar{S}) - \delta;$ $\varphi - c_{m3} - c_{t'3} - \delta;$ $\theta P(A/T_2 \cap \bar{S}) + \delta + \lambda$	$\varphi - c_{m1} - c_{t1} + R - \delta - \lambda;$ $\varphi - \theta P(A/\bar{T}_2) - \delta;$ $\varphi - c_{m3} - c_{t'3} - \delta;$ $\theta P(A/\bar{T}_2) + \delta + \lambda$	$\varphi - c_{m1} - c_{t1} + R;$ $\varphi - c_{m2} - c_{t2} + R;$ $\varphi;$ 0	$\varphi - c_{m1} - c_{t1} + R - \delta - \lambda;$ $\varphi - c_{m2} - c_{t'2} - \theta P(A/T_2 \cap \bar{S}) - \delta;$ $\varphi - \delta;$ $\theta P(A/T_2 \cap \bar{S}) + \delta + \lambda$	$\varphi - c_{m1} - c_{t1} + R - \delta - \lambda;$ $\varphi - \theta P(A/\bar{T}_2) - \delta;$ $\varphi - \delta;$ $\theta P(A/\bar{T}_2) + \delta + \lambda$
		$\bar{S}$	$\varphi - c_{m1} - c_{t'1};$ $\varphi - c_{m2} - c_{t2} + R;$ $\varphi - c_{m3} - c_{t3} + R;$ $0;$	$\varphi - c_{m1} - c_{t'1} - \delta - \lambda;$ $\varphi - c_{m2} - c_{t'2} - \theta P(A/T_2 \cap \bar{S}) - \delta;$ $\varphi - c_{m3} - c_{t3} + R - \delta;$ $\theta P(A/T_2 \cap \bar{S}) + \delta + \lambda;$	$\varphi - c_{m1} - c_{t'1} - \delta - \lambda;$ $\varphi - \theta P(A/\bar{T}_2) - \delta;$ $\varphi - c_{m3} - c_{t3} + R - \delta;$ $\theta P(A/\bar{T}_2) + \delta + \lambda;$	$\varphi - c_{m1} - c_{t'1};$ $\varphi - c_{m2} - c_{t2} + R;$ $\varphi - c_{m3} - c_{t'3};$ $0;$	$\varphi - c_{m1} - c_{t'1} - \delta - \lambda;$ $\varphi - c_{m2} - c_{t'2} - \theta P(A/T_2 \cap \bar{S}) - \delta;$ $\varphi - c_{m3} - c_{t'3} - \delta;$ $\theta P(A/T_2 \cap \bar{S}) + \delta + \lambda;$	$\varphi - c_{m1} - c_{t'1} - \delta - \lambda;$ $\varphi - \theta P(A/\bar{T}_2) - \delta;$ $\varphi - c_{m3} - c_{t'3} - \delta;$ $\theta P(A/\bar{T}_2) + \delta + \lambda;$	$\varphi - c_{m1} - c_{t'1};$ $\varphi - c_{m2} - c_{t2} + R;$ $\varphi;$ $0;$	$\varphi - c_{m1} - c_{t'1} - \delta - \lambda;$ $\varphi - c_{m2} - c_{t'2} - \theta P(A/T_2 \cap \bar{S}) - \delta;$ $\varphi - \delta;$ $\theta P(A/T_2 \cap \bar{S}) + \delta + \lambda;$	$\varphi - c_{m1} - c_{t'1} - \delta - \lambda;$ $\varphi - \theta P(A/\bar{T}_2) - \delta;$ $\varphi - \delta;$ $\theta P(A/\bar{T}_2) + \delta + \lambda;$
	$\bar{T}$		$\varphi;$ $\varphi - c_{m2} - c_{t2} + R;$ $\varphi - c_{m3} - c_{t3} + R;$ $0;$	$\varphi - \delta - \lambda;$ $\varphi - c_{m2} - c_{t'2} - \theta P(A/T_2 \cap \bar{S}) - \delta;$ $\varphi - c_{m3} - c_{t3} + R - \delta;$ $\theta P(A/T_2 \cap \bar{S}) + \delta + \lambda;$	$\varphi - \delta - \lambda;$ $\varphi - \theta P(A/\bar{T}_2) - \delta;$ $\varphi - c_{m3} - c_{t3} + R - \delta;$ $\theta P(A/\bar{T}_2) + \delta + \lambda;$	$\varphi;$ $\varphi - c_{m2} - c_{t2} + R;$ $\varphi - c_{m3} - c_{t'3};$ $0;$	$\varphi - \delta - \lambda;$ $\varphi - c_{m2} - c_{t'2} - \theta P(A/T_2 \cap \bar{S}) - \delta;$ $\varphi - c_{m3} - c_{t'3} - \delta;$ $\theta P(A/T_2 \cap \bar{S}) + \delta + \lambda;$	$\varphi - \delta - \lambda;$ $\varphi - \theta P(A/\bar{T}_2) - \delta;$ $\varphi - c_{m3} - c_{t'3} - \delta;$ $\theta P(A/\bar{T}_2) + \delta + \lambda;$	$\varphi;$ $\varphi - c_{m2} - c_{t2} + R;$ $\varphi;$ $0;$	$\varphi - \delta - \lambda;$ $\varphi - c_{m2} - c_{t'2} - \theta P(A/T_2 \cap \bar{S}) - \delta;$ $\varphi - \delta;$ $\theta P(A/T_2 \cap \bar{S}) + \delta + \lambda;$	$\varphi - \theta - \lambda;$ $\varphi - \theta P(A/\bar{T}_2) - \delta;$ $\varphi - \delta;$ $\theta P(A/\bar{T}_2) + \delta + \lambda;$

 ISBN: 978-1-61208-919-5

TABLE III
NORMAL FORM: AN ATTACKER TARGETS USER 3.

Attacker targets User 3			User 3: T						User 3: $\bar{T}$		
			S			$\bar{S}$					
			User 2			User 2			User 2		
			T		$\bar{T}$	T		$\bar{T}$	T		$\bar{T}$
			S	$\bar{S}$		S	$\bar{S}$		S	$\bar{S}$	
User 1	T	S	$\varphi - c_{m1} - c_{t1} + R;$ $\varphi - c_{m2} - c_{t2} + R;$ $\varphi - c_{m3} - c_{t3} + R;$ 0	$\varphi - c_{m1} - c_{t1} + R;$ $\varphi - c_{m2} - c_{t'2};$ $\varphi - c_{m3} - c_{t3} + R;$ 0	$\varphi - c_{m1} - c_{t1} + R;$ $\varphi;$ $\varphi - c_{m3} - c_{t3} + R;$ 0	$\varphi - c_{m1} - c_{t1} + R - \delta - \lambda;$ $\varphi - c_{m2} - c_{t2} + R - \delta;$ $\varphi - c_{m3} - c_{t'3} - \theta P(A/T_3 \cap \bar{S}) - \delta;$ $\theta P(A/T_3 \cap \bar{S}) + \delta + \lambda$	$\varphi - c_{m1} - c_{t1} + R - \delta - \lambda;$ $\varphi - c_{m2} - c_{t'2} - \delta;$ $\varphi - c_{m3} - c_{t'3} - \theta P(A/T_3 \cap \bar{S}) - \delta;$ $\theta P(A/T_3 \cap \bar{S}) + \delta + \lambda$	$\varphi - c_{m1} - c_{t1} + R - \delta - \lambda;$ $\varphi - \delta;$ $\varphi - c_{m3} - c_{t'3} - \theta P(A/T_3 \cap \bar{S}) - \delta;$ $\theta P(A/T_3 \cap \bar{S}) + \delta + \lambda$	$\varphi - c_{m1} - c_{t1} + R - \delta - \lambda;$ $\varphi - c_{m2} - c_{t2} + R - \delta;$ $\varphi - \theta P(A/\bar{T}_3) - \delta;$ $\theta P(A/\bar{T}_3) + \delta + \lambda$	$\varphi - c_{m1} - c_{t1} + R - \delta - \lambda;$ $\varphi - c_{m2} - c_{t'2} - \delta;$ $\varphi - \theta P(A/\bar{T}_3) - \delta;$ $\theta P(A/\bar{T}_3) + \delta + \lambda$	$\varphi - c_{m1} - c_{t1} + R - \delta - \lambda;$ $\varphi - \delta;$ $\varphi - \theta P(A/\bar{T}_3) - \delta;$ $\theta P(A/\bar{T}_3) + \delta + \lambda$
		$\bar{S}$	$\varphi - c_{m1} - c_{t'1};$ $\varphi - c_{m2} - c_{t2} + R;$ $\varphi - c_{m3} - c_{t3} + R;$ 0;	$\varphi - c_{m1} - c_{t'1};$ $\varphi - c_{m2} - c_{t'2};$ $\varphi - c_{m3} - c_{t3} + R;$ 0;	$\varphi - c_{m1} - c_{t'1}\ ;$ $\varphi;$ $\varphi - c_{m3} - c_{t3} + R;$ 0;	$\varphi - c_{m1} - c_{t'1} - \delta - \lambda;$ $\varphi - c_{m2} - c_{t2} + R - \delta;$ $\varphi - c_{m3} - c_{t'3} - \theta P(A/T_3 \cap \bar{S}) - \delta;$ $\theta P(A/T_3 \cap \bar{S}) + \delta + \lambda;$	$\varphi - c_{m1} - c_{t'1} - \delta - \lambda;$ $\varphi - c_{m2} - c_{t'2} - \delta;$ $\varphi - c_{m3} - c_{t'3} - \theta P(A/T_3 \cap \bar{S}) - \delta;$ $\theta P(A/T_3 \cap \bar{S}) + \delta + \lambda;$	$\varphi - c_{m1} - c_{t'1} - \delta - \lambda;$ $\varphi - \delta;$ $\varphi - c_{m3} - c_{t'3} - \theta P(A/T_3 \cap \bar{S}) - \delta;$ $\theta P(A/T_3 \cap \bar{S}) + \delta + \lambda;$	$\varphi - c_{m1} - c_{t'1} - \delta - \lambda;$ $\varphi - c_{m2} - c_{t2} + R - \delta;$ $\varphi - \theta P(A/\bar{T}_3) - \delta;$ $\theta P(A/\bar{T}_3) + \delta + \lambda;$	$\varphi - c_{m1} - c_{t'1} - \delta - \lambda;$ $\varphi - c_{m2} - c_{t'2} - \delta;$ $\varphi - \theta P(A/\bar{T}_3) - \delta\ ;$ $\theta P(A/\bar{T}_3) + \delta + \lambda;$	$\varphi - c_{m1} - c_{t'1} - \delta - \lambda;$ $\varphi - \delta;$ $\varphi - \theta P(A/\bar{T}_3) - \delta;$ $\theta P(A/\bar{T}_3) + \delta + \lambda;$
	$\bar{T}$		$\varphi;$ $\varphi - c_{m2} - c_{t2} + R;$ $\varphi - c_{m3} - c_{t3} + R;$ 0;	$\varphi;$ $\varphi - c_{m2} - c_{t'2};$ $\varphi - c_{m3} - c_{t3} + R;$ 0;	$\varphi;$ $\varphi;$ $\varphi - c_{m3} - c_{t3} + R;$ 0;	$\varphi - \delta - \lambda;$ $\varphi - c_{m2} - c_{t2} + R - \delta;$ $\varphi - c_{m3} - c_{t'3} - \theta P(A/T_3 \cap \bar{S}) - \delta;$ $\theta P(A/T_3 \cap \bar{S}) + \delta + \lambda;$	$\varphi - \delta - \lambda;$ $\varphi - c_{m2} - c_{t'2} - \delta;$ $\varphi - c_{m3} - c_{t'3} - \theta P(A/T_3 \cap \bar{S}) - \delta;$ $\theta P(A/T_3 \cap \bar{S}) + \delta + \lambda;$	$\varphi - \delta - \lambda;$ $\varphi - \delta;$ $\varphi - c_{m3} - c_{t'3} - \theta P(A/T_3 \cap \bar{S}) - \delta;$ $\theta P(A/T_3 \cap \bar{S}) + \delta + \lambda;$	$\varphi - \delta - \lambda;$ $\varphi - c_{m2} - c_{t2} + R - \delta;$ $\varphi - \theta P(A/\bar{T}_3) - \delta;$ $\theta P(A/\bar{T}_3) + \delta + \lambda;$	$\varphi - \delta - \lambda;$ $\varphi - c_{m2} - c_{t'2} - \delta;$ $\varphi - \theta P(A/\bar{T}_3) - \delta;$ $\theta P(A/\bar{T}_3) + \delta + \lambda;$	$\varphi - \delta - \lambda;$ $\varphi - \delta;$ $\varphi - \theta P(A/\bar{T}_3) - \delta;$ $\theta P(A/\bar{T}_3) + \delta + \lambda;$

strategy; the rational player would never change his or her strategy to get a lower payoff than that of the best strategy.

Theorem 1. *When every user notices security countermeasures, the proposed game admits a pure strategy Nash equilibrium related to the strategic profile (S, S, S, A).*

Proof. The proposed game generates nine strategic profiles when users choose the same actions and 72 otherwise. We study each of these two types of strategic profiles. Let $U_{att(User_i)}$ be the utility of the attacker when targeting $User_i$.

- Strategic profiles (Type 1): Users play the same actions.

Case 1.1: Every user has not got cybersecurity awareness training.

$$U_{att(User_i)}(\bar{T}, \bar{T}, \bar{T}, A) = \theta P(A/\bar{T}_i) + \delta + \lambda$$

From (2), there is equality between the attacker's payoffs. The attacker cannot increase his or her payoff. However, $User_i$ can increase his or her payoff from "$\varphi - \theta P(A/\bar{T}_i) - \delta - \lambda$" to "$\varphi - c_{mi} - c_{ti} + R$" by choosing to play S instead of $\bar{T}$ because (5) and (11) show that $-(\theta P(A/\bar{T}_i) + \delta) < -(c_{mi} + c_{ti})$. Therefore, the strategic profile ($\bar{T}, \bar{T}, \bar{T}$, A) is not a pure strategy Nash equilibrium.

Case 1.2: Every user notices part of security countermeasures.

$$U_{att(User_i)}(\bar{S}, \bar{S}, \bar{S}, A) = \theta P(A/T_i \cap \bar{S}) + \delta + \lambda$$

From (4), there is equality between the attacker's payoffs whoever his or her target is. The attacker cannot increase his or her payoff. However, $User_i$ can increase his or her payoff from "$\varphi - c_{mi} - c_{t'i} - \theta P(A/\bar{T}_i \cap \bar{S}) - \delta - \lambda$" to "$\varphi - c_{mi} - c_{ti} + R$" by choosing to play S instead of $\bar{S}$ because (11) shows that $-(\theta P(A/\bar{T}_i \cap \bar{S}) + \delta) < -(c_{mi} + c_{t'i})$. Therefore, the strategic profile ($\bar{S}, \bar{S}, \bar{S}$, A) is not a pure strategy Nash equilibrium.

Case 1.3: Every user notices security countermeasures.

$$U_{att(User_i)}(S, S, S, A) = 0$$

The attacker gets the same payoff whoever his or her target is. Furthermore, users get the maximum payoff (i.e., "$\varphi - c_{mi} - c_{ti} + R$") when they play "$S$". Therefore, the strategic profile (S, S, S, A) is a pure strategy Nash equilibrium.

- Strategic profiles (Type 2): Every user does not play the same action.

Case 2.1: One or two users notices security countermeasures.

The attacker's payoff is zero when targeting a user who notices security countermeasures. The attacker can increase his or her payoff by targeting a user who notices part of security countermeasures. Therefore, the related strategic profiles, such as (S, $\bar{S}$, $\bar{T}$, A), (S, S, $\bar{T}$, A), and (S, S, $\bar{S}$, A), are not pure strategy Nash equilibria.

Case 2.2: One or two users notices part of security countermeasures and the other user(s) has (have) not got cybersecurity awareness training.

The attacker's payoff is $\theta P(A/T_i \cap \bar{S}) + \delta + \lambda$ or $\theta P(A/\bar{T}_i) + \delta + \lambda$. From (5), $P(A/T_i \cap \bar{S}) < P(A/\bar{T}_i)$; then the attacker can increase his or her payoff by targeting a user who has not

 ISBN: 978-1-61208-919-5

got cybersecurity awareness training. Therefore, the related strategic profiles, such as $(\bar{S}, \bar{T}, \bar{T},$ A), $(\bar{T}, \bar{T}, \bar{S},$ A), and $(\bar{S}, \bar{S}, \bar{T},$ A), are not pure strategy Nash equilibria. □

2) Mixed Strategy Nash Equilibrium: It refers to a game in which every player plays a mixed strategy (i.e., a probability distribution over the pure strategies) and cannot improve his or her payoff under the mixed-strategy profile.

We consider the following parameters.

- u_i: The probability of $User_i$ taking cybersecurity awareness training, and $1 - u_i$ the probability of $User_i$ not taking the training.
- u_{si}: The probability of $User_i$ noticing security countermeasures, and $1 - u_{si}$ the probability of noticing part of security countermeasures.

$$0 \leq u_i, u_{si} \leq 1. \tag{12}$$

Note that u_i, $1 - u_i$, u_{si}, and $1 - u_{si}$, respectively, refer to as $P(T_i)$, $P(\bar{T}_i)$, $P(T_i \cap S)$, and $P(T_i \cap \bar{S})$ with $1 \leq i \leq 3$.

We consider a_1, a_2, and a_3, respectively, the probabilities associated with the attacker targeting $User_1$, $User_2$, and $User_3$.

$$0 \leq a_1, a_2, a_3 \leq 1. \tag{13}$$

$$a_1 + a_2 + a_3 = 1. \tag{14}$$

We assume that every player (i.e., attacker and users) randomizes his or her strategy.

2.1) User 1 plays a mixed strategy

The utility (U_1) of $User_1$ is the same when noticing security countermeasures (S), noticing part of security countermeasures ($\bar{S}$), or not taking cybersecurity awareness training ($\bar{T}$).

We have

$$U_1(S) = U_1(\bar{S}) = U_1(\bar{T}) \tag{15}$$

where

$$\begin{aligned}
U_1(S) =& (\delta + \lambda)(a_2 u_2 u_{s2} + a_3 u_3 u_{s3} - a_2 - a_3) + \\
& R + \varphi - c_{m1} - c_{t1} \\
U_1(\bar{S}) =& - a_1 \theta P(A/T_1 \cap \bar{S}) + (\delta + \lambda)(a_2 u_2 u_{s2} + a_3 u_3 u_{s3}) \\
& + \varphi - \delta - \lambda - c_{m1} - c_{t'1} \\
U_1(\bar{T}) =& - a_1 \theta P(A/\bar{T}_1) + (\delta + \lambda)(a_2 u_2 u_{s2} + a_3 u_3 u_{s3}) \\
& + \varphi - \delta - \lambda
\end{aligned}$$

From (14), we have $a_2 + a_3 = 1 - a_1$ then

If $U_1(S) = U_1(\bar{S})$ then

$$a_1 = \frac{-R + c_{t1} - c_{t'1}}{\theta P(A/T_1 \cap \bar{S}) + \delta + \lambda} \tag{16}$$

If $U_1(S) = U_1(\bar{T})$ then

$$a_1 = \frac{-R + c_{m1} + c_{t1}}{\theta P(A/\bar{T}_1) + \delta + \lambda} \tag{17}$$

If $U_1(\bar{S}) = U_1(\bar{T})$ then

$$a_1 = \frac{-(c_{m1} + c_{t'1})}{\theta(P(A/T_1 \cap \bar{S}) - P(A/\bar{T}_1))} \tag{18}$$

2.2) User j plays a mixed strategy

Similarly, regarding User j, with $2 \leq j \leq 3$, we obtain

If $U_j(S) = U_j(\bar{S})$ then

$$a_j = \frac{-R + c_{tj} - c_{t'j}}{\theta P(A/T_j \cap \bar{S}) + \delta} \tag{19}$$

If $U_j(S) = U_j(\bar{T})$ then

$$a_j = \frac{-R + c_{mj} + c_{tj}}{\theta P(A/\bar{T}_j) + \delta} \tag{20}$$

If $U_j(\bar{S}) = U_j(\bar{T})$ then

$$a_j = \frac{-(c_{mj} + c_{t'j})}{\theta(P(A/T_j \cap \bar{S}) - P(A/\bar{T}_j))} \tag{21}$$

2.3) The attacker plays a mixed strategy

The utility (U_{att}) of the attacker is the same when targeting $User_1$, $User_2$, or $User_3$.

$$U_{att(User_1)} = U_{att(User_2)} = U_{att(User_3)} \tag{22}$$

Using Equations (2) and (4), for $1 \leq i \leq 3$, we obtain

$$\begin{aligned}
U_{att(User_i)} =& u_i \theta P(A/T_i \cap \bar{S})(1 - u_{si}) + \theta P(A/\bar{T}_i)(1 - u_i) \\
& - u_i u_{si}(\delta + \lambda) + \delta + \lambda
\end{aligned}$$

The strategy profile at mixed strategy Nash equilibrium is $\{u_1 u_{s1} S + u_1(1-u_{s1})\bar{S} + (1-u_1)\bar{T}; u_2 u_{s2} S + u_2(1-u_{s2})\bar{S} + (1-u_2)\bar{T}; u_3 u_{s3} S + u_3(1-u_{s3})\bar{S} + (1-u_3)\bar{T}; a_1 A_1 + a_2 A_2 + a_3 A_3\}$.

Theorem 2. *The proposed game admits many mixed strategy Nash equilibria, especially when $\lambda = 0$, $User_i$ chooses to randomize to play S and $\bar{S}$ with $c_{ti} - c_{t'i} > R$, or chooses to play S and $\bar{T}$ with $c_{mi} + c_{ti} > R$, or chooses to randomize to play $\bar{S}$ and $\bar{T}$.*

Proof. Equations (16) and (19) show that, for $1 \leq i \leq 3$, $a_i > 0$ only if $c_{ti} - c_{t'i} > R$. Similarly, Equations (17) and (20) show that $a_i > 0$ only if $c_{mi} + c_{ti} > R$. Therefore, under these conditions, the proposed game may reach mixed strategy Nash equilibria when $User_i$ chooses randomly the events S and $\bar{S}$ or the events S and $\bar{T}$. Equations (18) and (21) show that $a_i > 0$ because (5) states that $P(A/T_i \cap \bar{S}) < P(A/\bar{T}_i)$. Therefore, the proposed game may reach a mixed strategy Nash equilibrium when $User_i$ plays randomly the events $\bar{S}$ and $\bar{T}$.

□

IV. Numerical Results

This section presents the numerical results of the proposed game using the equations obtained in Section III-D. We analyze the payoffs of households and attackers from the perspective of security costs and rewards for noticing security countermeasures. We further consider a more realistic cost covering scenario where $User_1$ pays the monetary cost of cybersecurity training of $User_2$ and $User_3$. In this scenario, we refer to $User_i$ as *Actual User* i ($1 \leq i \leq 3$).

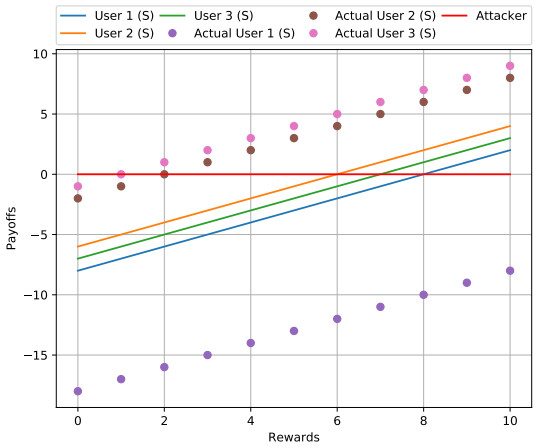

Fig. 2. Illustration of players' payoffs based on users' rewards for noticing security countermeasures with $\varphi < min(c_{m1}+c_{t1}, c_{m2}+c_{t2}, c_{m3}+c_{t3})$.

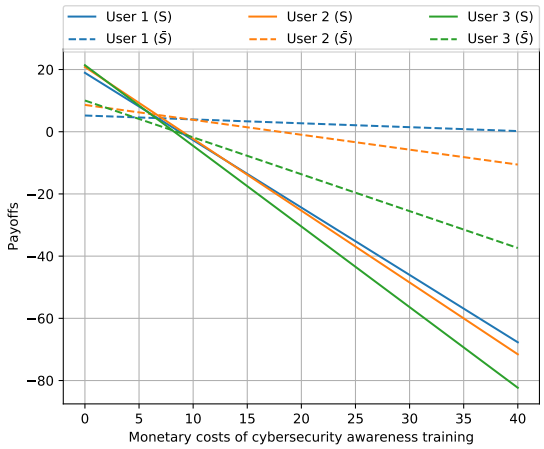

Fig. 4. Illustration of users' payoffs based on security investment costs when $\varphi > (\theta + \delta) > R$.

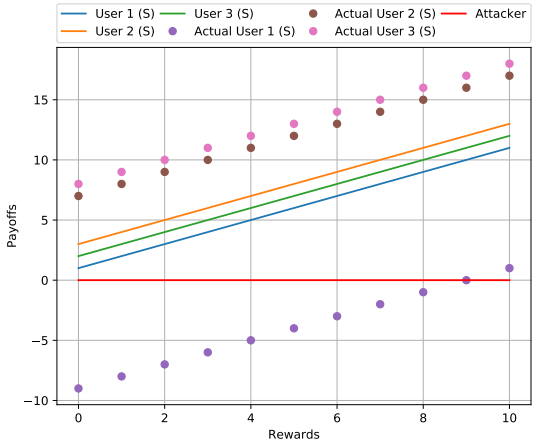

Fig. 3. Illustration of players' payoffs based on users' rewards for noticing security countermeasures with $\varphi > max(c_{m1}+c_{t1}, c_{m2}+c_{t2}, c_{m3}+c_{t3})$.

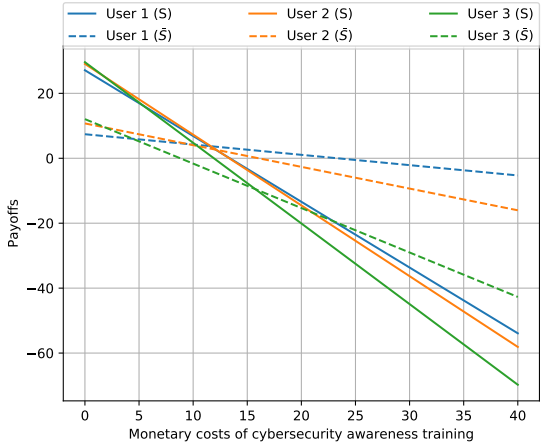

Fig. 5. Illustration of users' payoffs based on security investment costs when $\varphi > R > (\theta + \delta)$.

Our results are essentially based on the following parameters: φ, θ, R, c_{mi}, c_{ti}, $c_{t'i}$, $P(T_i)$, $P(T_i \cap S)$, $P(A/\bar{T}_i)$, and $P(A/T_i \cap \bar{S})$ $(1 \leq i \leq 3)$. We proposed, respectively, two scenarios related to the pure strategy Nash equilibrium and nine scenarios related to the mixed strategy Nash equilibria to examine the potential impacts of rewards for noticing security countermeasures, security costs, and the likelihood of the event $T_1 \cap S$ on the players' payoffs.

In the first two scenarios, the graph results are based on each player's payoff regarding the strategic profile (S, S, S, A). We set $c_{m1} = 3; c_{m2} = 4; c_{m3} = 6; c_{t1} = 6; c_{t2} = 3; c_{t3} = 2$. We choose $\varphi = 1$ in the first scenario and $\varphi = 10$ in the second. Figure 2 presents the results of the first scenario. We can see that when the comfort and benefit of living in a smart home are less considerable than security costs (money and time) to be invested, User 1, User 2, and User 3 will be satisfied with taking security training and noticing security countermeasures only if the security rewards are extremely significant and greater than the security costs invested $(R > 8)$. Furthermore "Actual User 2" and "Actual User 3" could be satisfied with a very few security reward $(R > 2)$ while "Actual User 1", will never be satisfied whatever the security rewards because his or her payoff remains negative. Figure 3 presents the results of the second scenario. It shows that when User 1, User 2, and User 3 estimate that the comfort and benefit of living in a smart home are more significant than the security costs to be spent, they are more likely to invest and notice security countermeasures whatever the reward. Same goes for "Actual User 2" and "Actual User 3" who are keen to notice security countermeasures. However, "Actual User 1" will be satisfied only if the security rewards are extremely significant $(R > 9)$. As it might be seen, in both scenarios, the results show a linear relationship between households' payoffs and the security rewards. Furthermore, the attacker's payoff is null, which reveals that the attacks would fail in such situations.

The graph results of the other scenarios are based on the players' payoffs in the mixed strategy Nash equilibria. We set $0 \leq c_{m1} < 40$; $c_{m2} = 1.25 * c_{m1}$; $c_{m3} = 1.75 * c_{m1}$; $c_{t1} = 6$;

 ISBN: 978-1-61208-919-5

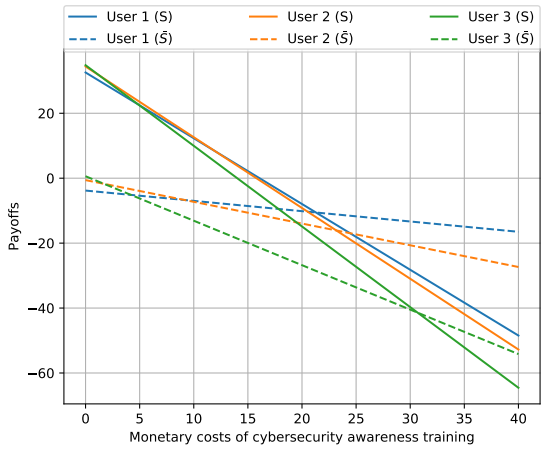

Fig. 6. Illustration of users' payoffs based on security investment costs when $R > \varphi > (\theta + \delta)$.

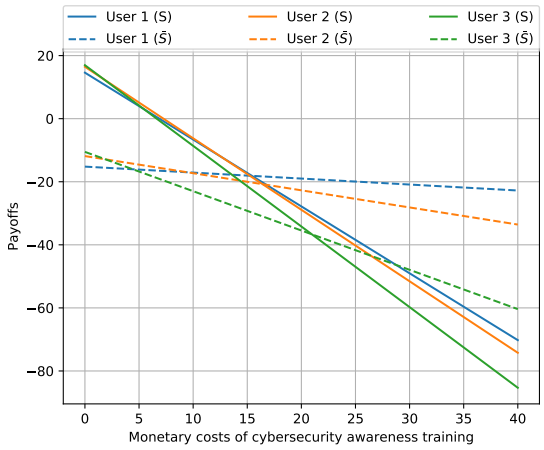

Fig. 8. Illustration of users' payoffs based on security investment costs when $(\theta + \delta) > R > \varphi$.

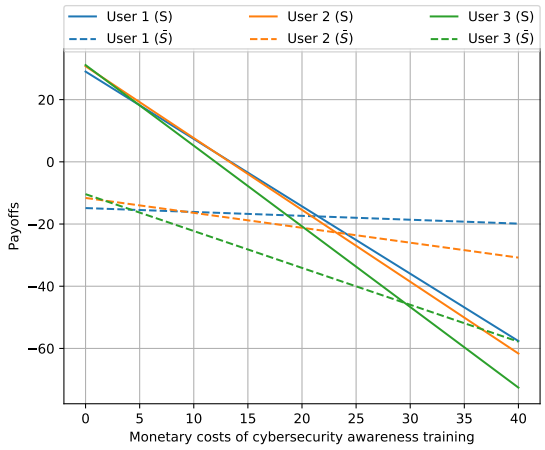

Fig. 7. Illustration of users' payoffs based on security investment costs when $R > (\theta + \delta) > \varphi$.

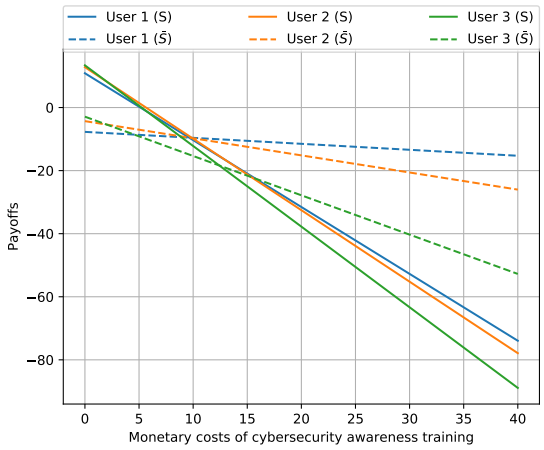

Fig. 9. Illustration of users' payoffs based on security investment costs when $(\theta + \delta) > \varphi > R$.

$c_{t2} = 3$; $c_{t3} = 2$; $c_{t'1} = 4$; $c_{t'2} = 2$; $c_{t'3} = 1$; $P(T_3 \cap S) = 0.5$; $P(T_2 \cap S) = 0.6$; $P(T_1 \cap S) = 0.7$; $P(A/T_i \cap \bar{S}) = 0.4$; $P(A/\bar{T_i}) = 0.9$ $(1 \leq i \leq 3)$.

Scenario 3 [$\varphi > (\theta + \delta) > R$]: We choose $\varphi = 18; \theta = 3; \delta = 7; R = 5$. Figure 4 presents the expected payoffs of households depending on the security costs in money of cybersecurity awareness training. We can see that the maximin strategy (the best of a set of worst possible security investment strategies) of households is reached when User 1 plays $\bar{S}$ and User 3 plays S with $c_{m1} = 6.56$ and *payoff* $= 4.39 > 0$.

Scenario 4 [$\varphi > R > (\theta + \delta)$]: We choose $\varphi = 18; \theta = 2; \delta = 3; R = 10$. Figure 5 shows that the maximin strategy of households is reached when User 1 plays $\bar{S}$ and User 3 plays S with $c_{m1} = 10.24$ and *payoff* $= 4.16 > 0$.

Scenario 5 [$R > \varphi > (\theta + \delta)$]: We choose $\varphi = 10; \theta = 2; \delta = 3; R = 18$. As presented in Figure 6, the maximin strategy of households is reached when User 1 plays $\bar{S}$ and User 3 plays S with $c_{m1} = 17.82$ and *payoff* $= -9.47$.

Scenario 6 [$R > (\theta + \delta) > \varphi$]: We choose $\varphi = 5; \theta = 3; \delta = 7; R = 18$. Figure 7 shows that the maximin strategy of households is reached when User 1 plays $\bar{S}$ and User 3 plays S with $c_{m1} = 18.63$ and *payoff* $= -17.19 < 0$.

Scenario 7 [$(\theta + \delta) > R > \varphi$]: We choose $\varphi = 5; \theta = 6; \delta = 12; R = 10$. Figure 8 shows that the maximin strategy of households is reached when User 1 and User 3 play $\bar{S}$ with $c_{m1} = 13.58$ and *payoff* $= -17.77 < 0$.

Scenario 8 [$(\theta + \delta) > \varphi > R$]: We choose $\varphi = 10; \theta = 6; \delta = 12; R = 5$. As presented in Figure 9, the maximin strategy of households is reached when User 1 plays $\bar{S}$ and User 3 plays S with $c_{m1} = 8.91$ and *payoff* $= -9.41 < 0$.

Scenario 9 [$\varphi > (\theta + \delta) > R$]: We choose $\varphi = 18; \theta = 3; \delta = 7; R = 5$. The previous results demonstrate that *Scenario 3* is the best option for households to minimize the monetary costs and get better payoffs. However, Figure 10 shows that *Scenario 3* may not suit actual users when only "Actual User 1" is accountable for the monetary costs. We can see that the maximin strategy of actual users is reached when "Actual User 1" plays $\bar{S}$ or S with $c_{m1} = 6.71$ and

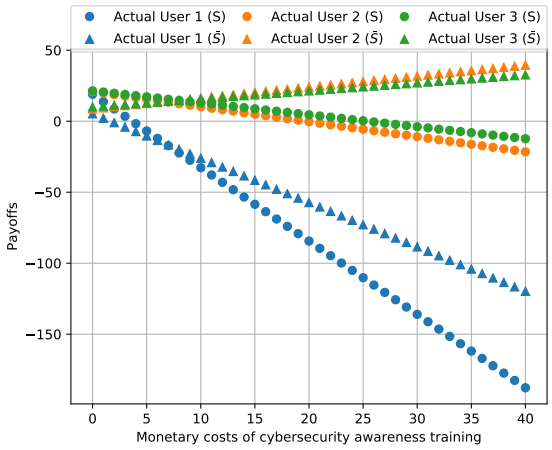

Fig. 10. Illustration of actual users' payoffs based on security investment costs when $\varphi > (\theta + \delta) > R$.

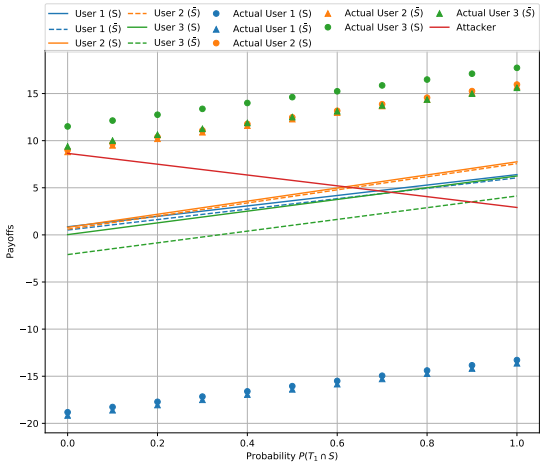

Fig. 11. Illustration of players' payoffs based on $P(T_1 \cap S)$ when $\varphi > (\theta + \delta) > R$ and $c_{m1} = 6.56$.

payoff $= -15.80 < 0$.

Scenario 10 [$\varphi > (\theta + \delta) > R$]: We choose $\varphi = 18; \theta = 3; \delta = 7; R = 5$. We analyze the payoffs of users and the attacker based on the probability $P(T_1 \cap S)$ regarding to the best maximin strategy ($c_{m1} = 6.56$). Figure 11 shows that the attacker payoff decreases linearly from 8.65 to 2.91. The payoffs of User 1, User 2, and User 3 increase linearly in the range of -2.09 to 7.75. Furthermore, the payoff of "Actual User 2" and "Actual User 3" increase linearly in the range of 7.49 to 17.29. We note that the payoffs of "Actual User 1" increases linearly from -19.16 to -13.28. Even with $P(T_1 \cap S) = 1$, the payoffs of "Actual User 1" remain negative.

Scenario 11 [$\varphi > (\theta + \delta) > R$]: We choose $\varphi = 18; \theta = 3; \delta = 7; R = 5; c_{m1} = 0$. Figure 12 shows that the attacker payoff decreases linearly from 8.65 to 2.91. Users' payoffs are all positive even though they decrease linearly. Furthermore, User 1 payoff $\geq$ attacker payoff when $P(T_1 \cap S) \geq 0.55$. We can also notice that the payoffs of User i and "Actual User i" are similar (with $1 \leq i \leq 3$).

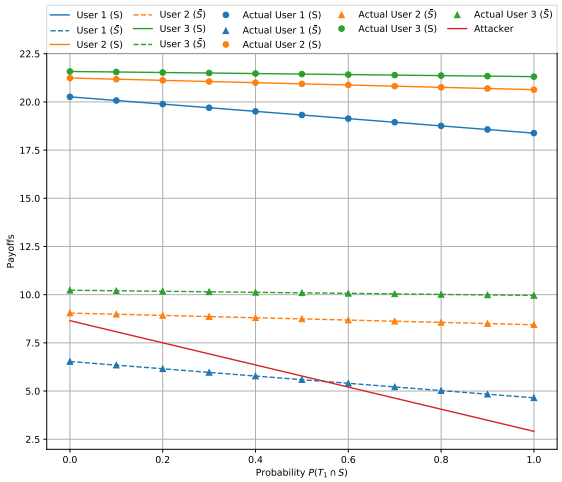

Fig. 12. Illustration of players' payoffs based on $P(T_1 \cap S)$ when $\varphi > (\theta + \delta) > R$ and $c_{m1} = 0$.

V. Discussion

The analysis of the numerical results indicates that security investments and the reward for noticing security countermeasures may influence households to engage in cybersecurity awareness education. The numerical results related to the pure strategy Nash equilibrium show that households would take the cybersecurity awareness training and notice security countermeasures under two conditions. First, the smart home should provide original values and vital comfort, and the other is that the security rewards should be very significant. Thus, investigating and providing new frameworks for security rewards in smart homes is a research area that needs to be explored and addressed.

Regarding the results of mixed strategies, we can see that *Scenario 3* is the best option for households because they can minimize the security investment costs and get a positive payoff. However, as shown in Figure 10, if a rational adult (e.g., "Actual User 1") has to pay the monetary costs for every user, then minimizing the security investment costs would provide a negative payoff. Furthermore, Figure 11 shows that even though a rational adult notices security countermeasures (with $P(T_1 \cap S) = 1$), his payoff will remain negative. Therefore "Actual User 1" will not be satisfied with the security investment done, which may impact his decision to keep noticing security countermeasures and affect the security behaviors of the other users. To address this issue, we encourage government to support households by subsidizing the cybersecurity training costs. As presented in Figure 12, when the training costs are zero, the payoff of every user is positive. Thus, households will be more likely to notice security countermeasures. Note that the decrease of users' payoff could shed light on the need to encourage households constantly on the importance of noticing security behaviors.

 ISBN: 978-1-61208-919-5

It is worth noting that the results of this paper rely on the effectiveness of cybersecurity awareness programs. We have assumed that those programs provide the required information to households to be aware of and deal with most known cyberattacks. Therefore, one limitation of this study is due to the existence of unknown cyberattacks that will not be teaching in the cybersecurity awareness programs. Furthermore, we have made some assumptions such as those of Equations (1), (2), (3), and (4) which may not be realistic. Additional research on this matter is recommended. Moreover, this study provides many insights regarding the future of cybersecurity education programs. The numerical results show the importance of the parameters φ and R. It would be highly appropriate for households to access tailored-service in smart homes. Thus, the comfort and benefit of living in such houses will encourage users to invest in cybersecurity to preserve their quality of life at home. Furthermore, providing households with tangible security rewards could also engage them in cybersecurity education programs. Our work also highlights the importance of developing specific and efficient programs for each category of households: children, adults, and senior citizens. Finally, we encourage public cybersecurity policy towards households security to provide free cybersecurity awareness training. Once the monetary costs are addressed, another challenge will be to reduce the time costs and make cybersecurity easier to learn and more intuitive for households.

VI. Conclusion and Future Work

In this paper, we proposed a game-theoretic approach to analyze cybersecurity awareness cost-benefit toward designing efficient education programs for households security. The goal is to encourage home users to engage in cybersecurity awareness education by identifying the minimum security investment cost that satisfies households and compare households' payoffs and the attacker's payoffs given a cyberattack. We provide a normal-form game with four players: three home users, including a senior citizen, an adult, and a child, and one attacker. We determine the conditions to reach the pure and mixed Nash equilibria of the proposed game. The numerical results show that the quality of services provided in a smart home, the security rewards of taking cybersecurity awareness training and noticing security countermeasures, and the potential impacts of cyberattacks may affect the payoffs of households and the attacker. Our research finds that the increase of quality of services accessible in a smart home may motivate households to engage in cybersecurity awareness education. Furthermore, providing security rewards to households may help them raise and maintain a high level of security awareness.

Future work may extend the present study to more than three users and many attackers. More importantly, we will propose an evolutionary game-theoretic approach to study the evolution of real users' behaviors in the proposed game and provide more realistic results. We will also seek to provide a survey research to confirm the findings of this paper. This work may also encourage a deeper investigation into cybersecurity education programs to provide more efficient frameworks for households, including children, adults, and senior citizens. Furthermore, our work may inspire smart-home providers to develop high-quality, tailored services for households. Finally, future work may also investigate the reduction of time costs and the design of security rewards in smart homes.

Acknowledgment

Part of this study was funded by the ICS-CoE Core Human Resources Development Program.

References

[1] S. Hansche, "Designing a security awareness program: Part 1," *Information systems security*, vol. 9, no. 6, pp. 1–9, 2001.

[2] S. Furnell, M. Gennatou, and P. Haskell-Dowland, "A prototype tool for information security awareness and training," *Logistics Information Management*, vol. 15, pp. 352–357, 12 2002.

[3] D. Ki-Aries and S. Faily, "Persona-centred information security awareness," *Computers & Security*, vol. 70, pp. 663–674, 2017.

[4] M. R. Alam, M. B. I. Reaz, and M. A. M. Ali, "A review of smart homes—past, present, and future," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 42, no. 6, pp. 1190–1203, 2012.

[5] OWASP, "Internet of Things Top Ten," 2014.

[6] J. Ricci, F. Breitinger, and I. Baggili, "Survey results on adults and cybersecurity education," *Education and Information Technologies*, vol. 24, no. 1, pp. 231–249, 2019.

[7] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Information systems research*, vol. 20, no. 1, pp. 79–98, 2009.

[8] A. A. Al Shamsi, "Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE," *International Journal of Information Technology and Language Studies*, vol. 3, no. 2, 2019.

[9] C. G. Blackwood-Brown, "An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills," Ph.D. dissertation, Nova Southeastern University, 2018.

[10] H. Aldawood and G. Skinner, "Challenges of implementing training and awareness programs targeting cyber security social engineering," in *2019 Cybersecurity and Cyberforensics Conference (CCC)*. IEEE, 2019, pp. 111–117.

[11] W. Zeng, "A methodology for cost-benefit analysis of information security technologies," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 7, p. e5004, 2019.

[12] Z. J. Zhang, W. He, W. Li, and M. Abdous, "Cybersecurity awareness training programs: a cost–benefit analysis framework," *Industrial Management & Data Systems*, vol. 121, pp. 613–636, 2021.

[13] H. Cavusoglu, S. Raghunathan, and W. T. Yue, "Decision-theoretic and game-theoretic approaches to it security investment," *Journal of Management Information Systems*, vol. 25, no. 2, pp. 281–304, 2008.

[14] W. Sun, X. Kong, D. He, and X. You, "Information security problem research based on game theory," in *2008 International Symposium on Electronic Commerce and Security*, 2008, pp. 554–557.

[15] X. Qian, X. Liu, J. Pei, and P. M. Pardalos, "A new game of information sharing and security investment between two allied firms," *International Journal of Production Research*, vol. 56, no. 12, pp. 4069–4086, 2018.

[16] Z. Zuo, Y. Fang, L. Liu, F. Fang, and X. Hu, "Research on information security cost based on game-theory," in *2013 IEEE 8th Conference on Industrial Electronics and Applications (ICIEA)*. IEEE, 2013, pp. 1435–1436.

[17] M. J. Osborne, *An introduction to game theory*. Oxford university press New York, 2004, vol. 3, no. 3.

 ISBN: 978-1-61208-919-5