Doctoral Dissertation

Human-Centered Cybersecurity Strategies and Behavioral Incentives for Secure Smart Homes

N'guessan Yves-Roland Douha
Program of Information Science and Engineering
Graduate School of Science and Technology
Nara Institute of Science and Technology

Supervisor: Professor Youki Kadobayashi
Laboratory for Cyber Resilience (Division of Information Science)

Submitted on September 15, 2023

A Doctoral Dissertation
submitted to Graduate School of Information Science,
Nara Institute of Science and Technology
in partial fulfillment of the requirements for the degree of
Doctor of Engineering

N'guessan Yves-Roland Douha

Thesis Committee:

Supervisor Youki Kadobayashi
(Professor, Division of Information Science)
Shoji Kasahara
(Professor, Division of Information Science)
Yuichi Hayashi
(Professor, Division of Information Science)
Yuzo Taenaka
(Associate Professor, Division of Information Science)
Masahiro Sasabe
(Professor, Graduate School of Informatics, Kansai University)

Human-Centered Cybersecurity Strategies and Behavioral Incentives for Secure Smart Homes*

N'guessan Yves-Roland Douha

Abstract

The proliferation of the Internet of Things (IoT) and smart homes has blurred the boundary between human and computer security, leading to an increase in cybersecurity threats. While previous research has primarily focused on technological vulnerabilities, the risks posed by context-based attacks that exploit user-related factors have been overlooked. This thesis adopts a human-centered approach to secure smart homes by investigating cybersecurity awareness among users and exploring the effectiveness of behavioral incentives. The research objectives include analyzing the costs and benefits of cybersecurity initiatives using game-theoretic models to identify the conditions for Nash equilibrium conducive to favoring investment in cybersecurity education, and investigating users' opinions on cybersecurity education and non-financial incentives. The theoretical investigation analyzes the costs and benefits of cybersecurity investment using static and evolutionary game-theoretic approaches. The empirical investigation collects and analyzes the perspectives of smart-home users on cybersecurity education and explores the influence of national cultures on their interests and motivations. The research contributes by providing insights into the costs, benefits, and implications of cybersecurity practices in smart homes. It identifies conditions for achieving Nash equilibria, emphasizes the importance of behavioral incentives and low-cost training, and highlights the need to consider cultural factors. The findings of this study underscore the crucial importance of investing in cybersecurity education and recognizing non-financial incentives to promote responsible

*Doctoral Dissertation, Graduate School of Information Science, Nara Institute of Science and Technology, September 15, 2023.

cybersecurity behaviors among smart-home users. These actions would play a pivotal role in empowering individuals to prevent and respond effectively to cyberattacks targeting smart homes. However, the study has limitations, including the assumption of rational actors in the theoretical investigation and the focus on a specific group of participants in the empirical investigation. Future research should explore more sophisticated game models that can capture the complexities of cybersecurity decision-making. Moreover, forthcoming endeavors should encompass a broader range of countries in cross-cultural studies and delve into participants' motivations to uncover deeper insights. This dissertation highlights the significance of human-centric approaches to address cybersecurity challenges in the realm of smart homes. It lays the foundation for further initiatives and policy development in securing smart homes, which is of utmost importance in our interconnected world.

Keywords:

cybersecurity awareness, behavioral incentives, smart homes, internet of things (IoT), context-based attacks, game-theoretic models, cultural factors

Contents

1. Introduction **1**
1.1 Background 1
1.2 Problem Statement 3
1.3 Research Objectives and Contributions 5
1.3.1 Research Objectives 6
1.3.2 Research Contributions 7
1.4 Dissertation Outline 9

2. Related Work **10**
2.1 Cybersecurity Awareness for Home Users 10
2.2 Survey Studies on Cybersecurity Literacy and Attitudes of Smart-Home Users 12
2.3 Game-Theoretic Approaches for Cybersecurity Investments 13
2.4 Cross-Cultural Studies for Cybersecurity Initiatives 15
2.5 Importance of Behavioral Incentives 16
2.6 Summary 17

3. Cybersecurity Investment Strategies for Smart-Home Users to Mitigate Cyberattacks: A Classical Game-Theoretic Approach **18**
3.1 Introduction 18
3.2 Proposed Game Model 19
3.2.1 System 20
3.2.2 Game Modeling 21
3.2.3 Normal-Form Game 24
3.3 Game Analysis 25
3.3.1 Pure Strategy Nash Equilibrium 25
3.3.2 Mixed Strategy Nash Equilibrium 29
3.4 Numerical Results 32
3.5 Discussion 35
3.5.1 Interpretation of the results 35
3.5.2 Limitations 35
3.5.3 Recommendations 36

3.6 Summary 37

4. An Evolutionary Game-Theoretic Analysis of Cybersecurity Investment Strategies for Smart-Home Users Against Cyberattacks 38

4.1 Introduction 38
4.2 Proposed Game Model 40
4.2.1 System 41
4.2.2 Game Modeling 42
4.2.3 Normal-Form Game 46
4.3 Game Analysis 47
4.3.1 Replicator Dynamics 48
4.3.2 Conditions for ESS 50
4.4 Numerical Results 53
4.4.1 Numerical Validation of the Stability of E_6 55
4.4.2 Analyzing the Effects of Cybersecurity and Cyberattack Costs on E_6 56
4.5 Discussion 59
4.5.1 Interpretation of the Results 60
4.5.2 Limitations and Recommendations 62
4.6 Summary 63

5. Examining Smart-Home Users' Interests in Cybersecurity Awareness Training and Behavioral Incentives 64

5.1 Introduction 64
5.2 Methodology 67
5.2.1 Survey Design 67
5.2.2 Preselection Criteria of Participants 68
5.2.3 Statistical Analysis 69
5.3 Results 70
5.3.1 Descriptive Statistics 70
5.3.2 Inferential Statistics 72
5.4 Discussion 81
5.4.1 Users' Cybersecurity Awareness for Smart-Home Security . 81

5.4.2 Non-Financial Reward for Cybersecurity 84
5.4.3 Implications 86
5.4.4 Limitations and Recommendations 86
5.5 Summary 87

6. Discussion **88**

7. Future Directions **90**
7.1 Simulation-Based Models 90
7.2 Exploring Punishments and Rewards 90
7.3 Cultural Factors and Personalized Solutions 90
7.4 Long-Term Sustainability of Cybersecurity Education 91
7.5 Quantifying the Financial Impact of Cyberattacks 91
7.6 AI-Assisted Network and Device Management 91
7.7 Friendly Security Dashboard 92
7.8 Collaborative Framework for Security Implementation 92

8. Conclusions **93**

Acknowledgements **95**

References **99**

Appendix **110**

A. Jacobian Matrix **110**

B. Survey Questionnaire **113**

Publication List **121**

List of Figures

1 An overview of the smart-home cyberattack landscape. 2
2 Flowchart of our approach using classical game theory. 19
3 Illustration of the proposed classical game system. 20
4 Players' payoffs are determined by users' rewards for adopting good cybersecurity practices under the condition $\varphi < min(c_{m1} + c_{t1}, c_{m2} + c_{t2}, c_{m3} + c_{t3})$. 33
5 Players' payoffs are determined by users' rewards for adopting good cybersecurity practices under the condition $\varphi > max(c_{m1} + c_{t1}, c_{m2} + c_{t2}, c_{m3} + c_{t3})$. 34
6 Flowchart of our approach using evolutionary game theory. 40
7 Illustration of the proposed evolutionary game system. 41
8 4-dimensional phase portraits by state combinations. 54
9 Population evolution of x, y, z_1, and z_2 over time. 56
10 The impact of cybersecurity costs on the ESS E_6. 57
11 The impact of rewards for cybersecurity commitment on the ESS E_6. 58
12 The impact of cyberattack costs on the ESS E_6. 59
13 The impact of operation costs of cyberattacks on the ESS E_6. . . 60
14 Cultural differences between Japan and the UK based on Hofstede's cultural dimensions. 65
15 Agreement on the necessity of cybersecurity awareness training for securing smart homes effectively. 74
16 Willingness to spend money on cybersecurity awareness training. . 74
17 Willingness to spend time on cybersecurity awareness training. . . 75
18 Cybersecurity awareness training for children. 76
19 Cybersecurity awareness training for senior citizens. 77
20 Level of satisfaction with non-financial rewards for promoting cybersecurity hygiene at home. 78
21 Non-financial rewards for secure behavior in smart homes. 81

List of Tables

1	List of parameters used in the proposed classical game model.	23
2	Normal-form game with User 1 as the target of the attacker.	26
3	Normal-form game with User 2 as the target of the attacker.	27
4	Normal-form game with User 3 as the target of the attacker.	28
5	List of parameters used in the proposed evolutionary game model.	43
6	Normal-form game representation for the proposed evolutionary game.	47
7	Summary of equilibrium stability analysis.	52
8	List of parameter values used in the numerical results.	55
9	Descriptive statistics	71
10	Regression Results of the Logit and Ordered Logit Models	73
11	Marginal Effects of Citizenship for Ordered Logit Models CAT_1, CAT_4, CAT_5, NFR_1, NFR_2, and NFR_3	75
12	Marginal Effects of Logit Models CAT_2 and CAT_3	79

1. Introduction

1.1 Background

The frontier between human and computer security is becoming increasingly blurred, particularly with the widespread adoption of the Internet of Things (IoT) and its prominent application, the smart home. As part of this study, we define smart-home users (SHUs) as individuals who reside in and interact with IoT devices within smart homes. ITU-T J.1612 characterizes a smart home as a form of home automation system wherein an array of IoT devices cooperate to furnish home users with intelligent control and monitoring capabilities. These IoT devices include smart meters, smartwatches, and smart speakers, which offer a variety of functions such as energy management, healthcare, and entertainment. The smart home market is growing at an accelerated rate and is estimated to be worth US$222.90 billion by 2027, with 672.60 million active users [1]. The rapid adoption of smart homes has led to an exponential increase in IoT devices, which are unfortunately vulnerable to cyberattacks. These attacks can compromise the privacy and security of smart-home users, potentially exposing sensitive information or granting unauthorized access. The scale and frequency of cyberattacks targeting IoT devices is a significant cause for concern, with a recent report suggesting that over 1 billion attacks, including over 800 million IoT-related phishing attempts, occurred in 2021 [2].

Numerous cybersecurity threats currently pose a risk to smart homes. Yang and Sun classify cybersecurity attacks that target smart homes into distinct layers in their comprehensive study [3]. The perception layer encompasses actuators, sensors, and IoT devices, which are prone to attacks, such as side-channel attacks. The network/transport layer comprises networking devices such as routers, which are vulnerable to attacks such as Man-in-the-Middle (MITM), Denial of Service (DoS), or Distributed DoS (DDoS) attacks. Finally, the application layer includes software and web applications, which are susceptible to attacks, such as buffer overflows and phishing attacks. It is essential to note that the broad range of attacks on smart homes stems from inherent vulnerabilities in resource-constrained IoT devices, traditional network and application systems, and context-based attacks enabled in the smart-home environment.

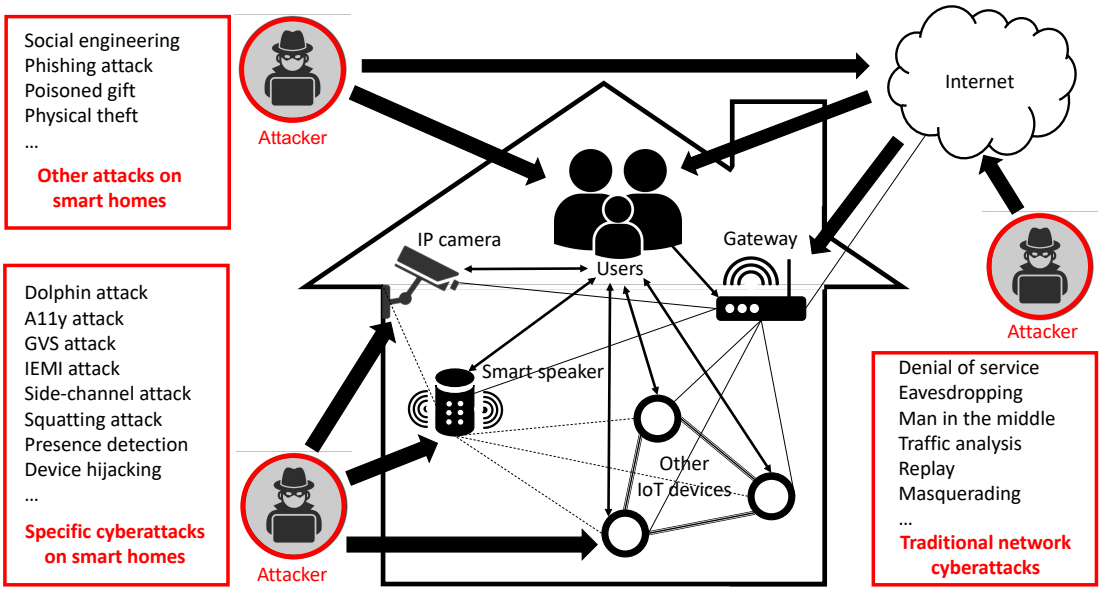


Figure 1: An overview of the smart-home cyberattack landscape.

In recent years, a significant amount of research papers have been dedicated to addressing cybersecurity concerns in smart homes [4, 5, 6, 7, 8, 9]. However, many of these studies have focused primarily on identifying and mitigating technological vulnerabilities while overlooking the threats posed by context-based attacks. This oversight is particularly problematic in the context of smart homes, where lay users, including children, adults, and senior citizens, are multiple and vulnerable to social engineering attacks. Consequently, research has emphasized the critical importance of recognizing users as a critical security issue in smart homes and has proposed an overview of the related cyberattack landscape [10].

Figure 1 [10] provides an overview of cyberattacks on smart homes, categorized into three groups. The first group consists of traditional network cyberattacks, such as DDoS attacks, MITM attacks, and eavesdropping. The second group comprises specific cyberattacks targeting smart home devices, such as exploiting vulnerabilities in motion sensors or Internet Protocol (IP) cameras to spy on users. The third group encompasses attacks that exploit the human factor, including social engineering and phishing attacks that aim to deceive users into revealing sensitive information or providing unauthorized access to the system.

With the ever-evolving and intricate cyberattack landscape, users' interaction

with IoT devices in smart homes is critical. Thus, it is imperative to consider how users could become valuable assets in achieving more dependable security for smart homes. This study investigates a human-centered approach to securing smart homes.

1.2 Problem Statement

Cybersecurity awareness is a critical factor in mitigating the success rate of cyberattacks and reducing information system misuse [11]. In the context of smart homes, cybersecurity awareness can enhance users' ability to prevent and respond to cyberattacks targeting their IoT devices and smart homes. Due to the rising frequency of IoT-related cyberattacks and the escalating adoption of smart homes, it is imperative to evaluate the extent of cybersecurity awareness among smart-home users. While previous studies have recognized the necessity of cybersecurity education for this group [12, 13], limited research has explored the cost-benefit analysis and effectiveness of cybersecurity awareness training for smart-home users.

Engaging in cybersecurity education programs can be challenging for individuals with limited resources due to the training costs [14]. While employer-sponsored training programs have demonstrated their effectiveness in increasing individuals' participation in cybersecurity training [15], relying solely on these initiatives to secure smart homes is impractical. This approach lacks cost-effectiveness for employers and overlooks individuals who are not part of the workforce and do not have the support of an employer. Thus, it is crucial to understand how to address the financial challenges of engaging smart-home users in cybersecurity awareness training. A cost-benefit analysis could provide valuable insights into whether the potential benefits of cybersecurity awareness training for individuals outweigh the associated costs.

Cost-benefit analysis provides a rational template for navigating complex decisions, and decision theory propels the advancement of cost-benefit analysis [16]. Decision theory can be categorized into two primary branches: normative decision theory and descriptive decision theory [17]. Normative theory aims to identify rational choices, with utility theory standing as a prominent example. This theory posits that individuals seek to maximize their expected utility. In

contrast, descriptive decision theory delves into actual decision-making processes, as illustrated by behavioral decision theory. This approach acknowledges the influence of heuristic strategies, biases, and decision-making under conditions of uncertainty. These theoretical frameworks offer distinct advantages across various contexts. However, for our specific investigation into cost-benefit analysis, we concentrate on utility theory to measure the satisfactions that individuals gain from evaluating costs and benefits.

According to a study conducted by Morrison, Coventry, and Briggs [18], the hesitance of individuals to actively participate in cybersecurity practices can frequently be ascribed to the perceived disparity between costs and benefits. Nevertheless, the accuracy of their perception remains ambiguous. Game theory, with its emphasis on strategic decision-making and equilibrium analysis, is highly suitable for delving into this issue.

Our investigation revolves around the interplay between two distinct groups: users and attackers. Recognizing the impact of one's choices on others, game theory emerges as a robust conceptual framework. Game theory provides a formal methodology for examining interactions among decision-makers facing strategic situations. It adeptly analyzes cases where gains are shaped not only by personal choices but also by the actions of others. In the context of cybersecurity awareness training and cyberattacks, game theory effectively captures the dynamic interplay between smart-home users and potential attackers, facilitating utility analysis for each individual. Furthermore, the adoption of game theory facilitates the development of mathematical models capable of addressing both static and dynamic scenarios. This becomes particularly pertinent when examining the evolution of strategies over time, a critical aspect in the context of cybersecurity education. As users become increasingly informed and attackers adapt their tactics accordingly. While alternative decision-making frameworks may provide insights into cost-benefit analysis, game theory allows for a closer examination of individuals' strategic decisions that impact these outcomes.

It is essential to acknowledge that merely understanding the costs and benefits of cybersecurity education for individuals through theoretical investigation is not sufficient to bring about effective changes in their behaviors. In this regard, the potential of incentives emerges as a powerful tool for encouraging positive

cybersecurity behavior. Previous research has suggested that rewards can positively influence users' intentions to adopt information system security policies [19]. However, the effectiveness of rewards as incentives may depend on users' environment, as environmental factors have been shown to impact cybersecurity behavior [20].

Non-financial incentives, particularly those related to social norms, could also have a significant impact on user behavior in the home [21]. Non-financial incentives offer compensation not tied to monetary rewards in exchange for changes in behavior or practices. In this study, non-financial rewards encompass direct non-monetary benefits such as recognition, awards, badges, and free services (e.g., virtual reality services), as well as indirect monetary rewards like virtual point reward systems and discount schemes. We consider these two aspects because the findings of Rehnen et al. [22] showed that monetary incentives tend to be more effective in promoting user engagement.

Despite the existing literature on the significance of incentives in cybersecurity behavior, there remains a lack of research on non-financial rewards for promoting cybersecurity best practices among smart-home users. To address this gap, our research adopts an empirical approach to gather and analyze real-world insights and preferences regarding non-financial incentives capable of fostering cybersecurity awareness and promoting sound cybersecurity behavior in smart homes.

The present thesis aims to address the previously highlighted research gaps.

1.3 Research Objectives and Contributions

The proposed research undergoes two directions: a theoretical investigation and an empirical investigation. The theoretical investigation will examine the costs and benefits of cybersecurity awareness training for smart-home users. The study aims to evaluate whether investing in cybersecurity education is valuable for smart-home users against cyberattacks targeting the smart-home environment. In this regard, the study will develop two game theory models to identify the conditions under which investing in cybersecurity education is beneficial for smart-home users. The first game model will examine a classical static game with smart-home users and an attacker. The second game model will study a dynamic game that focuses on the evolution of strategies among different populations of

smart-home users, stakeholders, and attackers over time, using evolutionary game theory.

In the empirical investigation, the study aims to collect and analyze the opinions of smart-home users regarding their interests in spending time and money on cybersecurity education against cyberattacks. The research will explore whether adult users agree that every age group, including children (defined as individuals under 18 years old) and senior citizens (defined as individuals aged 65 and older), should undergo cybersecurity education to avoid bad cyber behavior and IoT misuse leading to security breaches in the smart home. The study will also investigate non-financial rewards that would motivate users to adopt good cybersecurity practices in the smart home over time. Finally, the study aims to examine whether national cultural differences influence smart-home users' interests in cybersecurity awareness training and behavioral incentives.

1.3.1 Research Objectives

In this study, our research objectives are divided into two categories, which focus on both theoretical and empirical aspects of our investigation. The following are the research objectives related to the theoretical aspect of our investigation:

- To examine the cost-benefit payoffs of investing in cybersecurity awareness training for smart-home users in the context of cyberattacks.
- To develop a game model based on classical game theory and identify the Nash equilibrium conditions under which investing in cybersecurity education is advantageous for smart-home users.
- To develop a game model based on evolutionary game theory and analyze the stability of Nash equilibrium solutions over time and the conditions under which investing in cybersecurity education is advantageous for smart-home users.
- To discover whether investing in cybersecurity education is valuable for smart-home users to better equip them against cyberattacks targeting the smart-home environment.

The research objectives regarding the empirical aspect of our investigation are outlined as follows:

- To collect and analyze responses from adult smart-home users regarding their interest in investing time and money in cybersecurity education to mitigate cyberattacks.
- To investigate whether adult smart-home users acknowledge the importance of cybersecurity education for all age groups, including children and senior citizens, to prevent security breaches in the smart home.
- To identify non-financial rewards that can engage smart-home users in adopting good cybersecurity practices over time.
- To examine whether national cultural differences influence the level of interest among smart-home users in cybersecurity awareness training and behavioral incentives.

1.3.2 Research Contributions

We summarize the research contributions related to the theoretical investigation as follows:

- We model the competition between cybersecurity investments and cyberattacks as a non-cooperative game among three smart-home users (i.e., a child, an adult, and a senior citizen) and an attacker.
- We analyze the conditions that lead to pure and mixed strategy Nash equilibria, which represent stable outcomes of the game.
- We analyze and discuss the numerical results of the proposed game by investigating the impacts of costs and benefits of cybersecurity investments.
- We extend the game model to encompass three populations: smart-home users, smart-home stakeholders, and attackers, which provides a more realistic representation of the smart-home ecosystem.

- We derive the replicator dynamics of three populations using evolutionary game theory. We analyze the Nash equilibrium solutions of the proposed evolutionary game model and identify the conditions for asymptotic stability of equilibrium solutions.
- We validate our theoretical results by using 4-dimensional phase portraits by state combinations and plotting the evolution of population fractions to confirm the existence of a unique evolutionary stable strategy (ESS) in the proposed game. This validation provides evidence of the convergence of the system towards the ESS.
- We analyze and discuss the numerical results of the proposed game by investigating the impacts of costs and benefits of cybersecurity investments and cyberattack costs on the ESS.

The following are the research contributions related to our empirical investigation:

- We investigate the impact of national cultures on smart-home users' interests in cybersecurity awareness training.
- We propose non-financial rewards as a valuable incentive to encourage smart-home users to adopt good cybersecurity behavior at home.
- We conduct a survey questionnaire to collect and analyze the opinions of Japanese and British adult smart-home users regarding their potential interests in cybersecurity awareness training and desired non-financial rewards towards good cybersecurity behavior at home.
- We discover whether adult smart-home users intend to engage in cybersecurity awareness training, and are willing for children and senior citizens to get trained.
- We examine the influence of national cultures on smart-home users' interests in non-financial rewards.
- We identify the most prominent non-financial rewards that may motivate smart-home users to adopt good cybersecurity hygiene at home.

1.4 Dissertation Outline

The subsequent sections of this doctoral thesis are structured as follows. Chapter 2 provides an overview of the relevant related work in the field. In Chapter 3, we use a classical game-theoretic approach to analyze cybersecurity investments in the face of cyberattacks. Building upon this, Chapter 4 utilizes an evolutionary game-theoretic approach to further explore cybersecurity investment strategies. Chapter 5 focuses on investigating the interests of smart-home users in cybersecurity awareness training and non-financial rewards. Chapter 6 discusses essential aspects of the research. The future directions of this research are outlined in Chapter 7. Finally, Chapter 8 concludes the thesis, summarizing the key findings, contributions, and implications of the study.

2. Related Work

This chapter provides a review of the related work in six subsections. Section 2.1 covers the topic of cybersecurity awareness for home users. Section 2.2 presents the existing survey studies on cybersecurity literacy and attitudes of smart-home users. Section 2.3 describes game-theoretic approaches for cybersecurity investments. Section 2.4 presents insights into cross-cultural cybersecurity awareness studies. Section 2.5 discusses the importance of non-financial rewards among behavioral incentives. Lastly, Section 2.6 summarizes the chapter.

2.1 Cybersecurity Awareness for Home Users

This study distinguishes between two types of users: home users and smart-home users. We consider home users as the conventional Internet users who access the Internet services through terminals (e.g., desktops, laptops, smartphones, and tablets) in the home. Smart-home users are the new-generation users who not only enjoy the Internet services but also utilize IoT devices (e.g., smart thermostats, smart speakers) through terminals and voice commands to improve their comfort and quality of life at home.

The importance of the human factor in cybersecurity cannot be overstated. Cybersecurity threats not only stem from technology but also from human error and ignorance. Therefore, cybersecurity awareness for home users is crucial in mitigating the risks posed by cyber threats.

Several studies have investigated the issue of cybersecurity awareness among home users, dating back to the early 2000s when home computers and Internet accessibility became widespread. In 2007, Furnell, Bryant, and Phippen [23] surveyed 415 home users and found that novice Internet users lacked the necessary knowledge to protect themselves and were unaware of initiatives that could help them. In 2008, Furnell, Tsaganidi, and Phippen [24] confirmed this finding in an additional investigation with 20 novice Internet users, and suggested that safeguards should be automatically provided for home users. In 2010, Kritzinger and von Solm [25] proposed an e-awareness model that requires home users to absorb the necessary awareness content before using the Internet, to improve their understanding of security risks and how to avoid threats.

In 2012, Howe et al. [26] analyzed the psychology of security for home users and found that users lacking understanding of security threats may be unwilling or unable to incur the costs to defend against these threats. In 2017, Alotaibi, Clarke, and Furnell [27] reviewed existing security awareness tools for home users and suggested that a holistic information security management system that is easy to understand and not time-consuming can improve information security awareness. However, several challenges persist in implementing cybersecurity awareness programs. In 2019, Aldawood and Skinner [14] studied the challenges associated with implementing training and awareness programs targeting cybersecurity social engineering and identified the economic aspect of cybersecurity training as a significant hurdle.

Various research investigations have explored cybersecurity awareness among parents and their children, shedding light on technical and economic concerns among adults. Ricci, Breitinger, and Baggili [15] conducted a survey involving 233 parents, revealing that despite their concerns about their children's vulnerability to cyberattacks, parents showed reluctance to spend money on cybersecurity education. Similarly, Ahmad et al. [28] surveyed 872 parents to assess their awareness of cybersecurity threats faced by children online, uncovering a significant lack of awareness among parents and emphasizing the urgent need for enhanced cybersecurity education and guidance. Quayyum, Cruzes, and Jaccheri [29] highlighted the need for cybersecurity education for children to foster safe and responsible online habits. Łukasz and Potyrała [30] examined the knowledge and literacy levels of 514 parents, finding that a majority of parents overestimated their digital literacy while having low cybersecurity skills. Blackwood-Brown, Levy, and D'Arcy [31] found that cybersecurity awareness training improved the cybersecurity skills of older adults, particularly senior citizens, enabling them to take proactive measures against cyberattacks. Furthermore, Morrison, Coventry, and Briggs [18] discovered that senior citizens perceived the costs associated with cybersecurity training as outweighing the benefits, resulting in a lack of interest in cybersecurity education.

2.2 Survey Studies on Cybersecurity Literacy and Attitudes of Smart-Home Users

The increasing popularity of smart home technology has raised concerns regarding the security and privacy of users. This subsection discusses relevant survey studies that investigate the cybersecurity literacy of smart-home users and their attitudes towards security.

Zeng, Mare, and Roesner [32] conducted interviews with 15 smart-home users through phone or Skype calls, uncovering limited personal concerns about security and privacy. The participants had a large variety of IoT devices (e.g., 10 out of 15 users owned at least six types of IoT devices). Participants' threat models often depended on the sophistication of their technical mental models, which demonstrated the importance of providing smart-home users with technical security skills. Furthermore, the study emphasized the unique security and privacy challenges faced in multi-user smart homes.

Zheng et al. [12] conducted interviews with eleven smart-home users in the United States through Skype video calls, revealing a prioritization of convenience and connectedness over security issues. The study participants displayed significant interest in emerging technologies. However, they showed limited awareness of privacy risks associated with non-audio/video IoT devices. In addition, the study highlighted participants' concerns regarding external actors, such as Internet Service Providers (ISPs), accessing their smart-home data.

Sun et al. [33] conducted interviews with 23 parents living in smart homes across Canada and the US via Zoom video calls, exploring their perceptions and mitigation strategies regarding their children's safety. The authors acknowledged that some parents may have exhibited social desirability bias during the interviews–as they attempted to portray themselves as responsible parents. Furthermore, it is noteworthy that the study encompassed participants from two Western countries that share similar national cultures, as indicated by Hofstede's cultural dimensions [34].

Li et al. [13] conducted a qualitative content analysis of 4,957 Reddit comments sourced from 180 discussion threads centered around security and privacy within the Reddit smart-home forum called "HomeAutomation" [35]. The authors demonstrated that active engagement of users in online discussions regard-

ing security and privacy can significantly contribute to the development of their individual and collective attitudes. Consequently, the study emphasized the critical significance of cybersecurity education for smart-home users.

Our research proposes a cross-cultural survey to address limitations in the literature and enhance our understanding of smart-home users' interest in cybersecurity education.

2.3 Game-Theoretic Approaches for Cybersecurity Investments

When making decisions about information technology (IT) security investments, it is necessary to consider the costs and benefits. While traditional decision-theoretic approaches may be helpful, Cavusoglu et al. [36] argue that game-theoretic approaches are more appropriate for IT security investment decisions, particularly in cases where attackers are strategic. Furthermore, in the context of smart homes, Douha et al. [10] have provided an overview of the various entry points that attackers can exploit to launch cyberattacks, including smart-home networks, IoT devices, mobile apps, and human vulnerabilities. Given the strategic nature of attackers in targeting smart homes, a game-theoretic approach may be particularly effective in addressing the research problem at hand, specifically in analyzing the costs and benefits of cybersecurity education for smart-home users.

Anna Nagurney and Ladimer Nagurney [37] present a game model that determines optimal product transactions and cybersecurity investments for sellers competing to maximize their expected profits. The model incorporates the preferences of buyers through demand price functions, which depend on product demand and the average level of security in the marketplace. Furthermore, Nagurney et al. [38, 39] propose game theory models to analyze supply chain networks, with a focus on retailers and demand markets. These models consider the potential threat of a cyberattack on retailers, who strategically choose their optimal product transactions and cybersecurity levels to maximize their expected profits. However, the authors do not account for attackers, a critical aspect in attack-defense models necessary for evaluating the cost and benefits of cyberse-

curity investments.

Tosh et al. [40] propose a sequential game model that involves three players: organization, attacker, and insurer. The authors use backward induction to determine the subgame perfect equilibrium and analyze the optimal self-defense investment strategy for organizations, the optimal attack rate for the adversary, and the optimal coverage level for insurers through numerical results. However, the proposed game assumes that each player is aware of the moves of other players, which may not be realistic in a real-world smart-home environment where users may not know if IoT devices available on the market are secure or if they are being targeted by attackers. This incomplete information can limit the effectiveness of the game model in capturing real-world scenarios. Therefore, in the present study, we use a simultaneous game model to address this limitation.

Hyder and Govindarasu [41] propose a game-theoretic approach for optimizing cybersecurity investment strategies in the smart grid. Their system model focuses on the costs of both attackers and defenders, with attackers seeking to minimize their costs while maximizing the costs of defenders, and vice versa for defenders. However, the authors have not included benefit parameters in their model, which are critical in evaluating the significance of cybersecurity investment. Therefore, our proposed model builds upon their framework by studying a non-cooperative game that analyzes both the costs and benefits of attackers and defenders in the smart-home environment. Furthermore, we investigate the evolution of strategy choices of agents at a large scale and over time. This model extension contributes to a more comprehensive understanding of the strategic behavior of agents in cybersecurity investment decision-making.

Moreover, Sun et al. [42] utilize evolutionary game theory to investigate information security investments in the mobile electronic commerce industry chain. They introduce a penalty parameter to discourage organizations from not investing in IT security and show that regulating such a parameter could stimulate investments in information security. In contrast, our study proposes a different approach that imposes higher costs of cyberattacks on individuals who do not invest in cybersecurity while offering a reward parameter for those who do.

2.4 Cross-Cultural Studies for Cybersecurity Initiatives

In recent years, research has highlighted the role of cultural background in shaping users' cybersecurity awareness and behaviors. For instance, Harbach et al. [43] discovered variations in smartphone unlocking attitudes across different national cultures, with reasons ranging from convenience to perceived threats. Similarly, Sawaya et al. [44] observed differences in security behaviors between individuals in Asia and Western countries, emphasizing the need to consider cultural factors in security customization.

To address this important aspect, previous studies have explored the customization of security tools based on cultural differences [44]. Ndibwile et al. [45] found significant variations in security perception among Japanese and Tanzanian smartphone users, suggesting the redesign of security notifications to align with cultural norms. Argyris et al. [46] demonstrated the importance of tailoring picture passwords based on cultural backgrounds.

Further cross-national research is necessary to deepen our comprehension of users' intentions and behaviors regarding cybersecurity in smart homes. Prior studies have explored the impact of user knowledge on security intentions [47, 48], yet Sawaya et al. [44] suggested that users' self-confidence in their cybersecurity knowledge had a stronger positive influence on their security behaviors than their actual knowledge. Non-financial rewards, known to enhance users' intrinsic motivation [49], could prove valuable in building users' self-confidence and fostering secure behavior in smart homes. Lay users residing in smart homes may require a combination of educational initiatives and confidence-building measures to embrace cybersecurity practices within their homes.

Building upon this existing body of work, our study focuses on the influence of national culture on users' interest in cybersecurity education and non-financial incentives for good cybersecurity hygiene in smart homes. We aim to enhance our understanding of how tailored non-financial rewards can incentivize smart-home users and promote the adoption of secure behaviors in an increasingly digitalized world.

2.5 Importance of Behavioral Incentives

Behavioral incentives play a crucial role in promoting desirable actions and behaviors, including those related to cybersecurity. Traditionally, incentives have been categorized into two main types: financial and non-financial. Financial rewards, such as monetary compensation, have often been employed to motivate behavior change. However, recent research highlights the importance of non-financial rewards in achieving sustainable and long-term behavioral transformations.

Numerous studies have indicated that the use of extrinsic motivation, including financial rewards, can diminish individuals' perception of intrinsic motivation, subsequently reducing their actual intrinsic motivation levels [50]. From a neuroscience perspective, both extrinsic and intrinsic rewards activate similar chemical reactions in the brain, highlighting the potential for non-financial rewards to elicit similar motivational responses as their financial counterparts [51].

Despite these similarities, financial rewards present certain drawbacks from a cost perspective, as they involve substantial financial investments. In contrast, non-financial rewards, such as awards, recognition, and acknowledgements, offer a cost-effective alternative for promoting behavior change. Gneezy, Meier, and Rey-Biel [52] found that while financial incentives may drive short-term and intermediate behavioral changes, these effects tend to diminish once the incentives are removed. In contrast, non-financial rewards have demonstrated a significant impact on intrinsic motivation [49]. Consequently, non-financial rewards may prove more effective in fostering long-term behavior changes toward improved cybersecurity hygiene among smart-home users.

Through the utilization of non-financial rewards, such as public recognition or special awards, smart-home users can find the motivation to embrace and uphold cybersecurity practices. These rewards delve into individuals' inherent psychological needs for competence, autonomy, and relatedness, fostering a sense of accomplishment and self-determination in their cybersecurity efforts. Furthermore, non-financial rewards have the potential to establish a positive social norm and create a culture of cybersecurity consciousness within smart-home communities.

2.6 Summary

Chapter 2 reviews the literature on cybersecurity awareness among smart-home users. While existing studies have touched upon this crucial topic, they have largely overlooked the specific costs and benefits of cybersecurity investments tailored for smart-home users. Furthermore, prior research has overlooked the importance of behavioral incentives in promoting users' awareness of cybersecurity practices. The chapter emphasizes the need for further investigation into non-financial rewards and economic considerations to enhance user behaviors towards cybersecurity in the dynamic realm of smart homes.

3. Cybersecurity Investment Strategies for Smart-Home Users to Mitigate Cyberattacks: A Classical Game-Theoretic Approach

In this chapter, we use a classical game-theoretic approach to analyze the costs and benefits of cybersecurity investment of smart-home users against cyberattacks. The chapter begins with a description of classical game theory in Section 3.1. Section 3.2 introduces the proposed game model. Section 3.3 analyzes the pure and mixed equilibria. Section 3.4 presents the numerical results. Section 3.5 discusses the findings. Finally, Section 3.6 provides a summary of the chapter.

3.1 Introduction

The proliferation of smart homes and insecure IoT devices has led to increased cybersecurity risks and vulnerabilities that adversaries can exploit. In this chapter, we investigate cybersecurity investment strategies for smart-home users to mitigate cyberattacks using a classical game-theoretic approach.

Game theory is a branch of mathematics that studies the decision-making strategies and outcomes of strategic interactions among multiple individuals or groups, where each player's actions have consequences for the outcomes of others. It provides a framework for analyzing situations of conflict, cooperation, or mixed motives, in which the players' goals and preferences may not align.

Classical game theory, as formulated by John von Neumann and Oskar Morgenstern in their pioneering book "Theory of Games and Economic Behavior," focuses on strategic situations where rational players compete for resources or gains [53]. The theory assumes that each player seeks to maximize their own expected utility, given their beliefs about the other players' actions and preferences. By modeling the players' decision-making as a strategic game, classical game theory provides tools for predicting the likely outcomes of such games and identifying the optimal strategies for each player.

Our study uses classical game theory to analyze the strategic interactions between smart-home users and adversaries. We aim to identify the best cybersecurity investment strategies for smart-home users that can minimize their exposure

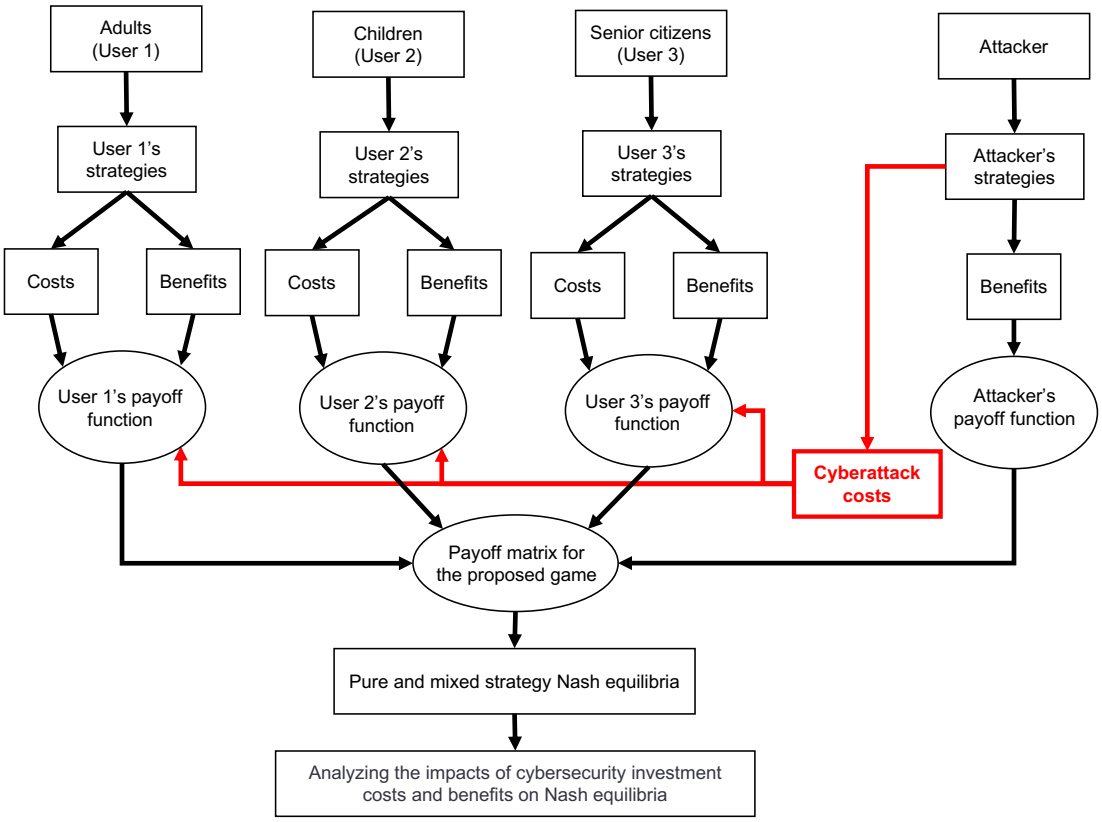


Figure 2: Flowchart of our approach using classical game theory.

to cyberattacks while maximizing their benefits. Figure 2 illustrates our proposed approach, which outlines how we investigate the pure and mixed strategy Nash equilibria. We will explore how changes in cybersecurity investment costs, benefits, and cyberattack costs can impact the equilibrium solutions of the game and outcomes for the players.

3.2 Proposed Game Model

This section begins by describing our proposed system. Next, we define the parameters of the game, followed by the presentation of the normal-form game.

3.2.1 System

Smart homes typically consist of various IoT devices that provide convenience to its users. As illustrated in Figure 3, we consider a smart home comprising three types of users: adults ($User_1$), children ($User_2$), and senior citizens ($User_3$), each with their own set of IoT devices. For example, adults can use IP cameras and smart door locks to enhance the physical security of the house, while children can use smart televisions (TVs) and smart speakers for entertainment. Senior citizens can benefit from health-related devices such as smart pill dispensers and smartwatches.

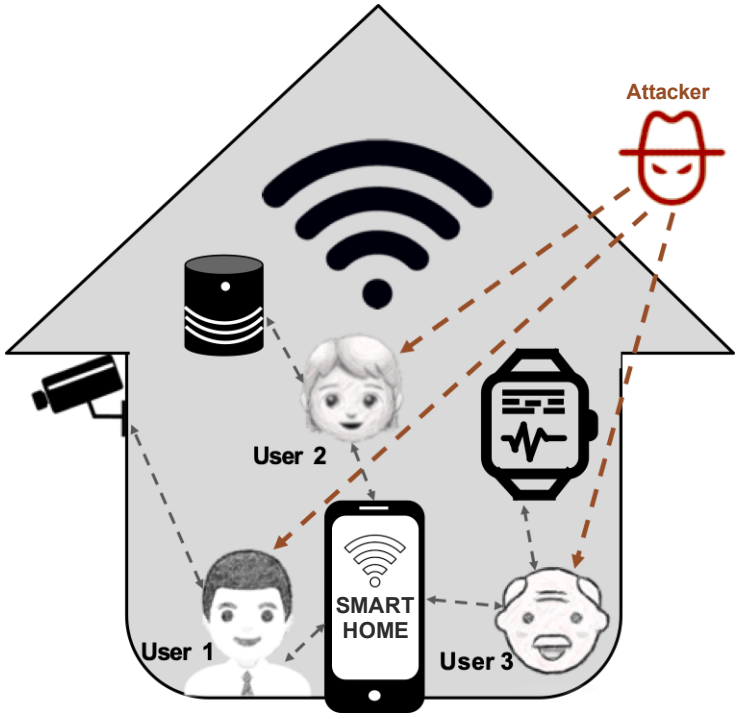


Figure 3: Illustration of the proposed classical game system.

Despite the numerous benefits associated with the use of IoT devices, smart-home users may not be fully aware of cybersecurity best practices, leaving them vulnerable to potential attacks. Attackers can take advantage of this vulnerability and use social engineering tactics, such as phishing, to trick users into revealing sensitive information or granting access to their IoT devices.

To address this issue and minimize the risks of potential security breaches, users can enhance their cybersecurity knowledge and skills by investing in cybersecurity awareness training. This study presents a game model that examines the strategic interactions between smart-home users and attackers. The proposed game model provides a framework for assessing the costs and benefits of different strategies. The following section presents the parameters used in the game model.

3.2.2 Game Modeling

This subsection presents the parameters used to describe the proposed game, as shown in Table 1.

Let T_i and $\bar{T}_i$, respectively, be the events $User_i$ has undergone cybersecurity awareness training, and $User_i$ has not undergone 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 compromising $User_i$ given that $User_i$ has undergone cybersecurity awareness training, and $P(A/\bar{T}_i)$ the probability of an attacker compromising $User_i$ given that $User_i$ has not undergone cybersecurity awareness training. We assume that

$$P(A/T_1) = P(A/T_2) = P(A/T_3). \tag{1}$$

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

We have (1) and (2) as evidence supporting the notion that the level of cybersecurity education has a stronger impact on users' responses to ongoing cyberattacks compared to their age group. Furthermore, all user groups are equally vulnerable to cyberattacks.

Let S denote the event where a user adopts good cybersecurity practices, while $\bar{S}$ corresponds to the event where a user partially adopts cybersecurity practices. We consider $P(A/T_i \cap S)$ the probability of an attacker compromising $User_i$ given that $User_i$ has undergone cybersecurity awareness training and adopts good cybersecurity practices, and $P(A/T_i \cap \bar{S})$ the probability of an attacker compromising $User_i$ given that $User_i$ has undergone cybersecurity awareness training and partially adopts good cybersecurity practices. Like (1) and (2), we assume that

$$P(A/T_1 \cap S) = P(A/T_2 \cap S) = P(A/T_3 \cap S). \tag{3}$$

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

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

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

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

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

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

We have (6) and (7) to take into consideration potential challenges that users may encounter in adopting good cybersecurity practices at home. For instance, senior citizens may experience cognitive or physical limitations that impede their ability to adopt good cybersecurity practices. Additionally, children may be less likely to adopt cybersecurity practices to some extent due to their lack of maturity or less intensive cybersecurity training content.

Moreover, we consider three types of costs that $User_i$ may incur: monetary costs associated with the event T denoted as c_{mi}, time costs associated with the event S denoted as c_{ti}, and time costs associated with the event $\bar{S}$ denoted as $c_{t'i}$. We have

$$0 \leq c_{m1} \leq c_{m2} \leq c_{m3}. \tag{8}$$

$$0 \leq c_{t3} \leq c_{t2} \leq c_{t1}. \tag{9}$$

$$0 \leq c_{t'i} < c_{ti}. \tag{10}$$

We have equation (8) because specialized training may be required for $User_2$ and $User_3$, which could potentially be more expensive than the training needed for $User_1$. In addition, providing training resources for $User_3$ may be more challenging than for $User_2$, potentially leading to a higher training cost for $User_3$. Equation (9) reflects our assumption that, as the person in charge of the smart home, $User_1$ may invest more time than $User_2$ and $User_3$ in adopting good cybersecurity practices. Furthermore, we assume that due to physical or cognitive limitations, $User_3$ may spend less time adopting good cybersecurity practices than $User_2$. Finally, we have equation (10) because $User_i$ may spend more time in the event S than in the event $\bar{S}$.

Table 1: List of parameters used in the proposed classical game model.

Parameters	Descriptions
T_i	$User_i$ has undergone cybersecurity awareness training with $1 \leq i \leq 3$.
$\bar{T}_i$	$User_i$ has not undergone cybersecurity awareness training.
T	A user has undergone cybersecurity awareness training.
$\bar{T}$	A user has not undergone cybersecurity awareness training.
S	A user adopts good cybersecurity practices.
$\bar{S}$	A user partially adopts cybersecurity practices.
A	An attacker compromises a user.
$P(A/T_i)$	Probability of an attacker compromising $User_i$ given that $User_i$ has undergone cybersecurity awareness training.
$P(A/\bar{T}_i)$	Probability of an attacker compromising $User_i$ given that $User_i$ has not undergone cybersecurity awareness training.
$P(A/T_i \cap S)$	Probability of an attacker compromising $User_i$ given that $User_i$ has undergone cybersecurity awareness training and adopts good cybersecurity practices.
$P(A/T_i \cap \bar{S})$	Probability of an attacker compromising $User_i$ given that $User_i$ has undergone cybersecurity awareness training and partially adopts cybersecurity practices.
$P(T_i \cap S)$	Probability of $User_i$ undergoing cybersecurity awareness training and adopting good cybersecurity practices.
$P(T_i \cap \bar{S})$	Probability of $User_i$ undergoing cybersecurity awareness training and partially adopting cybersecurity practices.
c_{mi}	Monetary costs incurred by $User_i$ for undergoing cybersecurity awareness training (T).
c_{ti}	Time costs incurred by $User_i$ for adopting good cybersecurity practices (S).
$c_{t'i}$	Time costs incurred by $User_i$ for partially adopting cybersecurity practices ($\bar{S}$).
δ	Cost of a cyberattack on a smart home, encompassing potential interruptions to various smart-home services, including home automation and healthcare.
θ	Cost of data breaches and privacy incidents resulting from an exploit through a user's device.
λ	Cost of privacy incidents for smart-home users who have not adopted good cybersecurity practices.
φ	Measure of comforts and benefits in a smart home.
R	Reward for adopting good cybersecurity practices for a user who has undergone cybersecurity awareness training.

We introduce the parameter δ ($\delta > 0$) to account for the cost of a cyberattack on a smart home. This cost includes potential interruptions to various smart-home services, such as home automation, electric power, healthcare, entertainment, and the Internet. It is worth highlighting that δ applies uniformly to all users.

We also consider the costs related to security breaches by introducing θ ($\theta > 0$), which represents the expenses incurred from data breaches and privacy incidents resulting from an exploit through a user's device. This cost is specifically assigned to the user who owns the compromised device. Therefore, we set the cost to zero ($\theta = 0$) for users who have not been attacked or have

successfully adopted good cybersecurity practices. We assume that

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

We distinguish between θ and λ ($\lambda \geq 0$). λ represents the cost of privacy incidents for smart-home users who have not adopted good cybersecurity practices. This cost varies based on the income and social status of the smart-home users. In this study, we assign λ only to $User_1$ since they are responsible for home safety and security. While θ could relate to issues regarding the quality of life, such as the unavailability of services or a decrease in the sense of privacy and self-esteem, λ could relate to financial losses such as ransom requests.

Finally, we introduce φ ($\varphi > 0$) as the parameter that quantifies all the comforts and benefits a user could enjoy when living in a smart home. This value is constant across all users. We also consider R as the reward for users who successfully adopt good cybersecurity practices after undergoing cybersecurity awareness training. It is important to note that the reward is set to zero ($R = 0$) for users who partially adopt cybersecurity practices.

3.2.3 Normal-Form Game

We describe the strategy sets of each player as matrices. Table 2, Table 3, and Table 4, 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 2.

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 undergoes cybersecurity awareness training and adopts good cybersecurity practices at home. 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 2, 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 $\bar{S}$.

3.3 Game Analysis

This section investigates the pure and mixed Nash equilibria of the proposed game. 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.

3.3.1 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 [54]. In pure strategy Nash equilibrium, a player plays his or her best 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 adopts good cybersecurity practices, 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 undergone cybersecurity awareness training.

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

Table 2: Normal-form game with User 1 as the target of the attacker.

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

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

Table 3: Normal-form game with User 2 as the target of the attacker.

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

"$\varphi - \theta P(A/\bar{T}_i) - \delta - \lambda$" 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.

Table 4: Normal-form game with User 3 as the target of the attacker.

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

Case 1.2: Every user partially adopts good cybersecurity practices.

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

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 adopts good cybersecurity practices.

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

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 adopt good cybersecurity practices.
The attacker's payoff is zero when targeting a user who adopts good cybersecurity practices. The attacker can increase his or her payoff by targeting a user who partially adopts good cybersecurity practices or has not undergone cybersecurity awareness training. 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 partially adopt good cybersecurity practices and the other user(s) has (have) not undergone 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 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. □

3.3.2 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 $User_i$ undergoing cybersecurity awareness training, and $1-u_i$ the probability of $User_i$ not undergoing cybersecurity awareness training.

- u_{si}: The probability of $User_i$ adopting good cybersecurity practices, and $1-u_{si}$ the probability of partially adopting cybersecurity practices.

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

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.

User 1 plays a mixed strategy

The utility (U_1) of $User_1$ is the same when adopting good cybersecurity practices (S), partially adopting cybersecurity practices ($\bar{S}$), or not undergoing cybersecurity awareness training ($\bar{T}$).

We have

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

where

$$\begin{aligned}
U_1(S) =& (\delta+\lambda)(a_2u_2u_{s2} + a_3u_3u_{s3} - a_2 - a_3) + R + \varphi - c_{m1} - c_{t1} \\
U_1(\bar{S}) =& -a_1\theta P(A/T_1 \cap \bar{S}) + (\delta+\lambda)(a_2u_2u_{s2} + a_3u_3u_{s3}) + \varphi - \delta - \lambda - c_{m1} - c_{t'1} \\
U_1(\bar{T}) =& -a_1\theta P(A/\bar{T}_1) + (\delta+\lambda)(a_2u_2u_{s2} + a_3u_3u_{s3}) + \varphi - \delta - \lambda
\end{aligned}$$

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

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

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

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

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

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

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 $\bar{T}$.

□

3.4 Numerical Results

This section presents the numerical results of the proposed game. Considering that the mixed-strategy Nash equilibrium might increase the probability of successful cyberattacks, we will exclusively focus on the pure Nash equilibrium for our numerical analysis. This approach aligns with our objective of maximizing users' payoff while minimizing attackers' payoffs.

We analyze the payoffs for all players, including smart-home and attackers. This involves examining the monetary and time costs, along with the rewards, associated with users' adoption of effective cybersecurity practices. In addition, we account for a more realistic cost-sharing scenario in which $User_1$ covers the cybersecurity awareness training expenses for $User_2$ and $User_3$. To reflect this situation accurately, we will refer to $User_i$ as *Actual User i* ($1 \leq i \leq 3$).

Our results depend upon the following parameters: φ, R, c_{mi}, c_{ti}, $c_{t'i}$ ($1 \leq i \leq 3$). Within this framework, we introduce two distinct scenarios that examine costs and rewards.

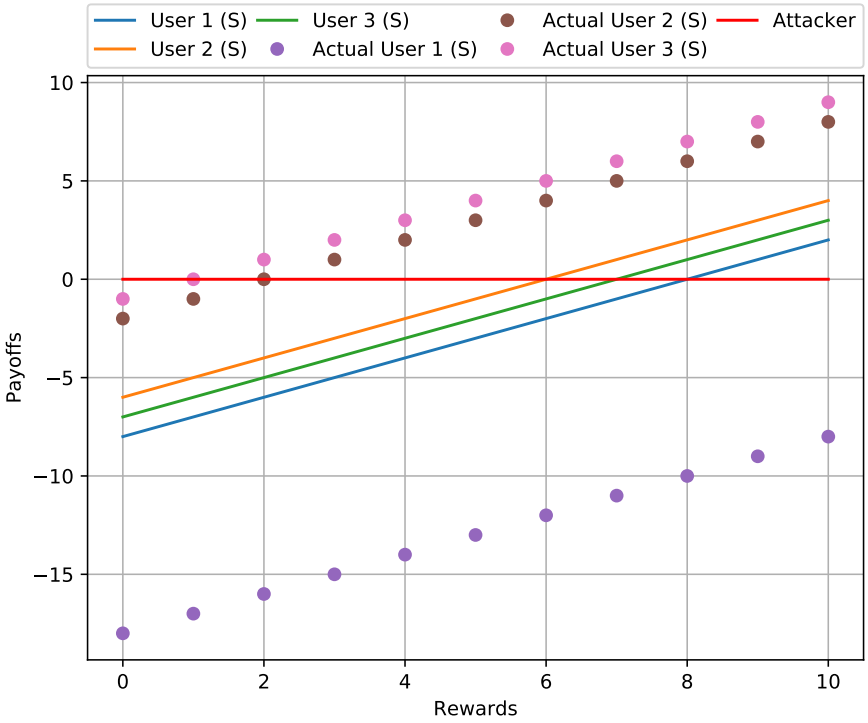


Figure 4: Players' payoffs are determined by users' rewards for adopting good cybersecurity practices under the condition $\varphi < min(c_{m1}+c_{t1}, c_{m2}+c_{t2}, c_{m3}+c_{t3})$.

The 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.

In scenario 1, where φ is smaller than the minimum of the combined costs $c_{m1} + c_{t1}$, $c_{m2} + c_{t2}$, and $c_{m3} + c_{t3}$, the findings presented in Figure 4 indicate that when the costs associated with investing in cybersecurity awareness training and good cybersecurity practices in terms of both monetary and temporal resources outweigh the advantages of residing in a smart home, Users 1, 2, and 3 will only contemplate engaging in cybersecurity awareness training and adopting good cybersecurity practices if the incentives for adopting good cybersecurity practices substantially surpass the incurred cybersecurity costs ($R > 8$). Furthermore, our analysis reveals that "Actual User 2" and "Actual User 3" might find modest rewards acceptable ($R > 2$). However, "Actual User 1" is less likely to attain satisfaction, given that their payoff remains negative even at $R = 10$, which

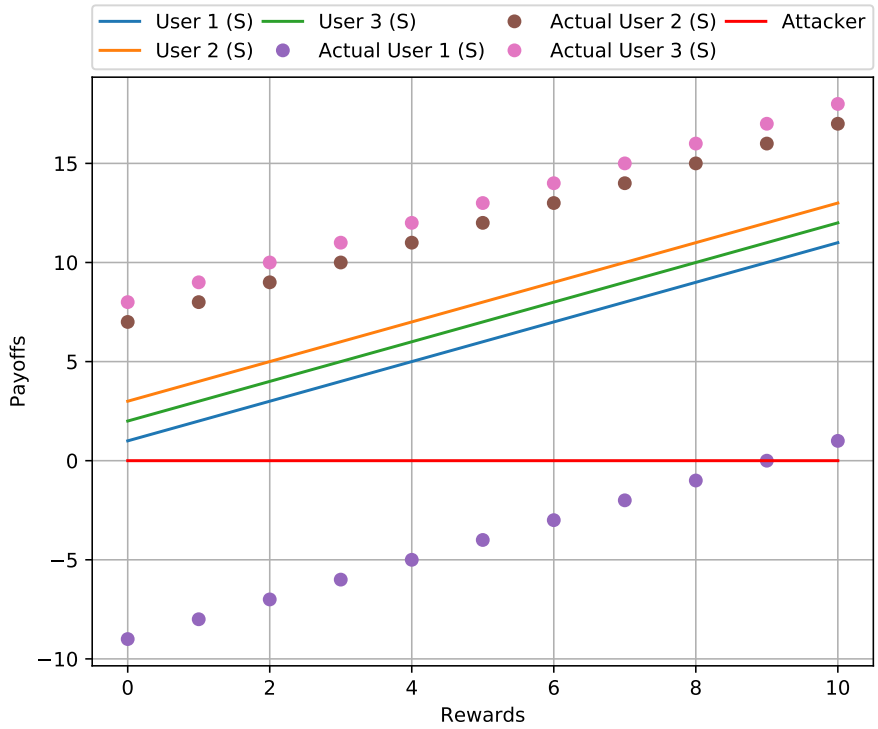


Figure 5: Players' payoffs are determined by users' rewards for adopting good cybersecurity practices under the condition $\varphi > max(c_{m1}+c_{t1}, c_{m2}+c_{t2}, c_{m3}+c_{t3})$.

suggests a need for a substantial reward to achieve a positive payoff.

In scenario 2, where φ is larger than the maximum of the combined costs $c_{m1} + c_{t1}$, $c_{m2} + c_{t2}$, and $c_{m3} + c_{t3}$, the findings presented in Figure 5 suggest that Users 1, 2, and 3 display a greater inclination to invest in cybersecurity awareness training and good cybersecurity practices when the benefits of residing in a smart home outweigh the associated cybersecurity costs, regardless of the rewards offered. The findings also indicate that within these given conditions, "Actual User 2" and "Actual User 3" are more predisposed to adopting good cybersecurity practices. However, satisfying the requirements of "Actual User 1" would necessitate substantially higher rewards, specifically with $R > 9$.

Across both scenarios, we notice a linear correlation between users' payoffs and rewards for adopting good cybersecurity practices. It is noteworthy that the attacker's payoff is zero, signaling unsuccessful attacks in these contexts.

3.5 Discussion

This section presents the findings of the study and discusses their implications. In addition, it identifies the limitations of the research and suggests potential avenues for future research.

3.5.1 Interpretation of the results

Our research highlights the crucial role of cybersecurity costs and rewards in motivating smart-home users to prioritize to improve their cybersecurity attitude.

Our findings show that smart-home users are more inclined to engage in cybersecurity awareness training and embrace good cybersecurity practices under specific conditions. Firstly, the smart home must have valuable assets and ensure user comfort. Manufacturers should prioritize offering innovative and user-friendly services to encourage users to invest in cybersecurity measures that protect their valuable smart-home assets. Secondly, users need to perceive significant benefits associated with good cybersecurity practices. However, creating an optimal incentive scheme remains a challenge. Lastly, user participation in cybersecurity initiatives relies on a strategy set that aligns with the requirements of a pure strategy Nash equilibrium, ultimately minimizing the potential gains for potential attackers. Therefore, it is essential to consider a comprehensive and strategic approach to cybersecurity engagement.

3.5.2 Limitations

While our study provides valuable insights, it is essential to acknowledge its inherent limitations.

One limitation lies in utilizing a classical game-theoretic approach in modeling interactions between smart-home users and attackers. This approach presupposes that all players possess complete information about the game and consequently make rational decisions based on this information. However, this simplified framework may fail to precisely encapsulate the intricacies of the real-world context, where players' decision-making processes can evolve in response to their experiences or feedback from their environment. Furthermore, our model does not incorporate pertinent stakeholders, including manufacturers, cyber insurance com-

panies, or regulatory bodies. These factors have the potential to exert substantial influence on the strategies adopted by both smart-home users and attackers. In addition, our numerical findings are confined to a delimited scope of scenarios and strategies, leaving room for the possibility that alternatives could yield additional outcomes. Lastly, we must emphasize that our study is predicated upon specific assumptions. These assumptions necessitate further validation through empirical investigation to affirm their robustness and applicability.

3.5.3 Recommendations

This study has limitations that could be addressed by future research. One avenue for enhancement involves an expansion of the scope pertaining to the scenarios and strategies under analysis. This expansion could encompass a wider array of stakeholders and strategies, consequently yielding potentially valuable insights. Furthermore, an exploration into the role of incentives and disincentives in fostering sound cybersecurity practices within smart homes has the potential to offer significant contributions to the field.

Another intriguing area for future exploration is the evaluation of different cybersecurity education programs tailored for smart-home users across various age groups. In addition, further research could study the repercussions of cybersecurity incidents on the behavior of smart-home users, along with potential strategies for mitigating these effects. It would also be prudent for researchers to embark on a thorough analysis aimed at validating the assumptions that underlie our game-theoretical model.

For a more accurate grasp of the ever-evolving landscape of cybersecurity education for smart-home users, researchers may consider the application of evolutionary game theory to model the intricate interactions between users and potential attackers. By adopting this approach, researchers can effectively scrutinize how the strategies employed by cohorts of participants evolve over time in response to the altering environment. This mirrors the dynamic nature of the real world, where individuals adapt their approaches in light of the ever-changing threat landscape.

3.6 Summary

In Chapter 3, we used a classical game-theoretic approach to evaluate the costs and benefits of cybersecurity education for smart-home users. The chapter presented a normal-form game that involved four players: an attacker and three smart-home users of different age groups. We analyzed the game and identified the conditions for achieving pure and mixed Nash equilibria. The results demonstrated that investing in cybersecurity education would be favorable for users under the assumptions of all players adopting pure strategies, the smart home furnishing users with valuable assets, and users receiving substantial rewards for upholding good cybersecurity practices. Finally, the chapter suggested using evolutionary game theory to model interactions between populations of users and attackers for a more realistic analysis of players' strategic behavior over time.

4. An Evolutionary Game-Theoretic Analysis of Cybersecurity Investment Strategies for Smart-Home Users Against Cyberattacks

In this chapter, we use an evolutionary game-theoretic approach to analyze the costs and benefits of cybersecurity investment of smart-home users against cyberattacks. The chapter begins with a description of evolutionary game theory in Section 4.1. Section 4.2 introduces the proposed game model. Section 4.3 derives the replicator dynamic and analyzes the stability of equilibrium solutions. Section 4.4 presents the numerical results. Section 4.5 discusses the findings. Finally, Section 4.6 provides a summary of the chapter.

4.1 Introduction

Evolutionary game theory (EGT) was developed following the work of John Maynard Smith [55, 56] aiming to adapt the traditional game-theoretic approaches [57, 58], in which players are assumed to be rational, to study natural biological selection. This investigation led to the development of the concept of "evolutionarily stable strategy" also known as "evolutionary stable strategy" (ESS), which explains the existence of ritual conflicts between animals. In a game model that involves populations of individuals competing with different strategies, an ESS is a strategy that cannot be bettered (or invaded) by any other existing strategy that everyone else in the population chooses. The ESS describes the stability of the game dynamics over time, and this dynamic is often modeled using the replicator dynamics [59]. In this work, we adopt the replicator dynamics to identify the ESS of our game model.

The objective of this chapter is to analyze the cybersecurity investment strategies of smart-home users against cyberattacks in complex and dynamic smart-home environments using EGT. The smart-home environment involves many IoT devices, smart-home users, and multiple stakeholders (e.g., manufacturers). In [60], it was observed that attackers have a wide range of potential targets and attack scenarios include both direct attacks and supply chain attacks. The latter is an indirect attack in which an attacker compromises one or more parts of a

supply chain to reach and compromise its primary target. We utilize EGT to model a game consisting of three populations: smart-home users, stakeholders, and attackers. We analyze the costs and benefits of the decision-making of each of these populations in the context of smart-home security.

Much research has used formal methods to address cybersecurity issues in IoT-based smart environments. For example, Krichen and Alroobaea [61] used attack trees to represent attack scenarios on IoT systems and transformed a given attack tree into a network of priced timed automata to test the security of IoT systems. Tabrizi and Pattabiraman used model checking to automatically analyze and identify possible attacks on smart-home devices known as smart meters [62]. Similarly, Kumar et al. [63] used model checking to address authentication, anonymity, and integrity in a smart-home environment. In addition to these formal methods, we can use EGT to analyze decision-making in smart environments.

The choice of EGT in the present study is motivated by its effectiveness in studying the decision-making of large populations of agents who repeatedly engage in strategic interactions [64]. Similar formal methods, such as classical game theory and agent-based modeling, have limitations when it comes to modeling the evolution of populations over time. Classical game theory assumes that all players are rational and make decisions based on their payoffs only, which is often unrealistic in real-world scenarios. Agent-based modeling can be used to simulate the behavior of individual agents and their interactions with each other and the environment, but it may not capture the strategic interactions between agents as effectively as EGT. In contrast, EGT focuses specifically on strategic interactions among agents and describes the outcomes of these interactions as payoff distributions.

By using EGT, we can examine how different costs and benefits of cybersecurity investment influence the behavior of smart-home users and stakeholders, and how attackers might adapt to these changes. EGT allows us to study the evolution of different strategies and their effects on the population over time, which is important for understanding how to design effective cybersecurity measures. Several previous studies have used EGT to study cybersecurity issues, demonstrating its effectiveness and relevance in this field. For example, Tosh et al. [65] used EGT to examine a Cybersecurity Information Exchange (CYBEX) framework,

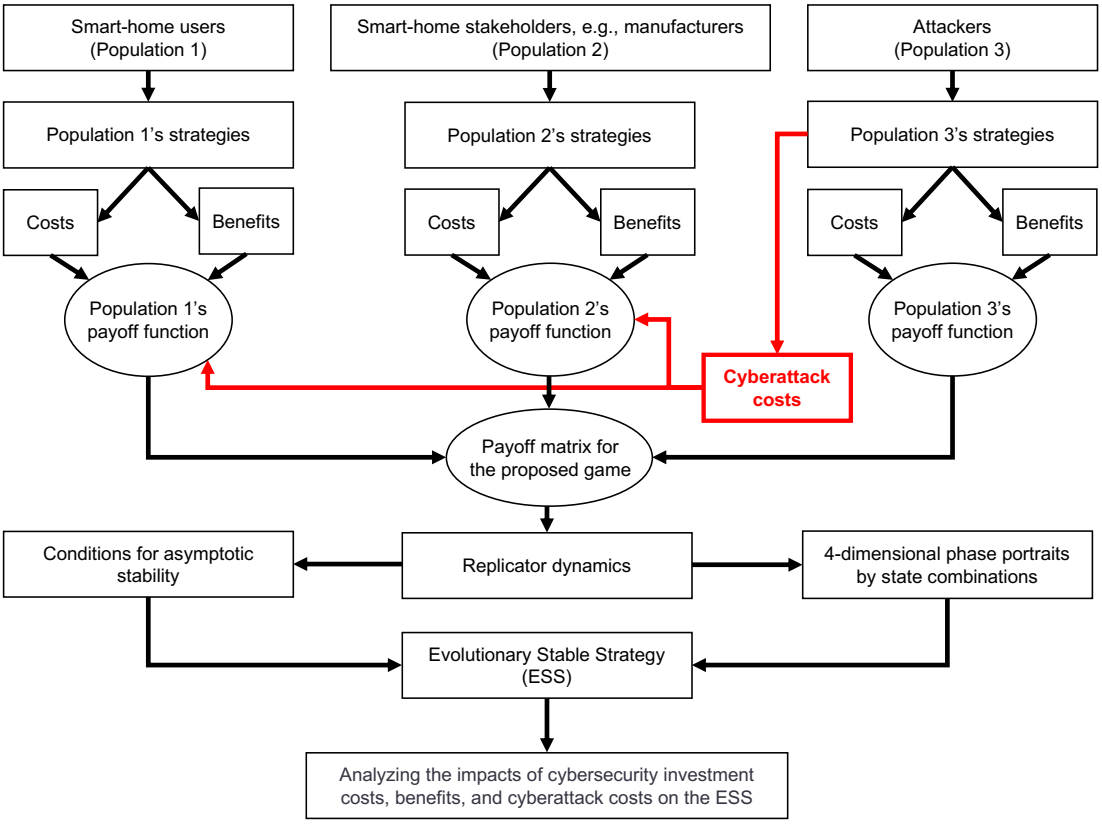


Figure 6: Flowchart of our approach using evolutionary game theory.

while Abass et al. [66] used EGT to analyze advanced persistent threats. These studies highlight the value of EGT in addressing cybersecurity challenges and advancing our understanding of how strategic interactions shape the evolution of populations over time. Figure 6 illustrates our proposed approach, which outlines how we investigate the ESS and the properties of the evolutionary dynamics to analyze the impacts of cybersecurity investment costs, benefits, and cyberattack costs on the ESS.

4.2 Proposed Game Model

This section begins by introducing our proposed system. Next, we define the parameters of the game, followed by the presentation of the payoff matrix.

4.2.1 System

Our system comprises three populations: smart-home users ($population_1$), manufacturers ($population_2$), and attackers ($population_3$). Figure 7 illustrates our system. $Population_1$ uses the IoT devices (e.g., IP cameras, smart speakers, and smartwatches) manufactured by $population_2$ for conveniences, such as house physical security, entertainment, and healthcare. The rise of cyberattacks on IoT devices may lead $population_1$ to invest in cybersecurity awareness training to learn how to protect IoT devices from cyberattacks and adopt good cybersecurity hygiene at home.

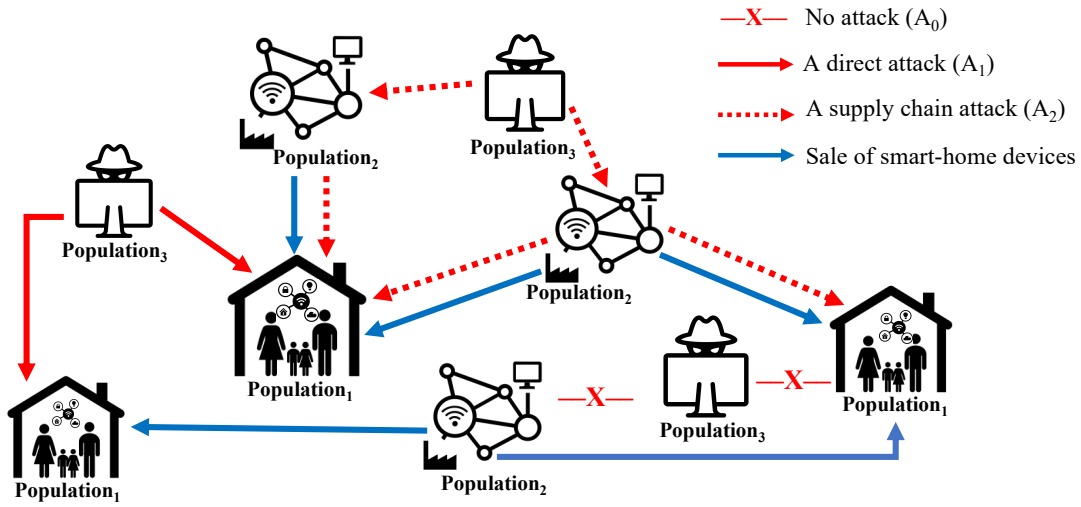


Figure 7: Illustration of the proposed evolutionary game system.

Recent cyberattacks showed that manufacturing is among the most targeted industries. The IBM Security X-Force Threat Intelligence Index 2022 reported that manufacturing was the top attacked industry in 2021 [67]. It is worth noting that manufacturers do not always implement cybersecurity best practices due to the effects of supply chain pressures and delays and the high costs of security. Thus, we consider that $population_2$ may comply with cybersecurity best practices and implement them for smart-home devices.

Regarding attackers, they may gain interest in compromising smart homes for various motives, such as accessing private information, using IoT-based home devices to execute Distributed Denial-of-Service (DDoS) attacks, and the absence of

resistance such as a dedicated cybersecurity team. We consider that $population_3$'s attacks may target supply chains that include manufacturers (i.e., $population_2$). As a result, $population_3$ may deceive $population_1$ indirectly, through the exploitation of IoT device vulnerabilities. Furthermore, $population_3$ may discern that $population_1$ is not aware of cybersecurity best practices, such as changing default passwords, employing multi-factor authentication, installing and utilizing endpoint security solutions, maintaining up-to-date software and firmware, and identifying and avoiding phishing links. This lack of awareness could potentially lead to various vulnerabilities. Consequently, individuals in $population_3$ may be able to directly deceive those in population 1, through social engineering tactics, for example.

The proposed system model is designed to mitigate security challenges related to smart homes. These homes frequently contain numerous IoT devices that are susceptible to diverse attacks, partly due to manufacturers prioritizing cost reduction over robust security measures. Furthermore, users' limited knowledge of cybersecurity best practices makes smart homes even more vulnerable to cyber threats. In light of these factors, the proposed system aims to bolster the security of smart homes by advocating for increased investments in cybersecurity. This approach seeks to mitigate the risks associated with insecure IoT devices, human factors, and other vulnerabilities, thus safeguarding smart homes from potential cyber threats.

4.2.2 Game Modeling

This subsection presents the parameters used to describe the proposed game, as shown in Table 5.

Let T and $\bar{T}$, respectively, be the strategies that $population_1$ invests in cybersecurity awareness training and $population_1$ does not invest in cybersecurity awareness training. Let S and $\bar{S}$, respectively, be the strategies that $population_2$ implements and does not implement cybersecurity best practices for IoT technology when manufacturing smart-home devices. Let A_1 be the strategy that $population_3$ attacks $population_1$ directly. A_2 is the strategy that $population_3$ attacks $population_1$ after compromising $population_2$. Since we will show that the attacker incurs some costs for the direct/indirect attack, we also consider the

Table 5: List of parameters used in the proposed evolutionary game model.

Parameters	Descriptions
T	$population_1$ invests in cybersecurity awareness training.
$\bar{T}$	$population_1$ does not invest in cybersecurity awareness training.
S	$population_2$ implements cybersecurity best practices.
$\bar{S}$	$population_2$ does not implement cybersecurity best practices.
A_0	$population_3$ adopts the strategy of no attack.
A_1	$population_3$ deceives $population_1$ directly.
A_2	$population_3$ deceives $population_1$ after compromising $population_2$.
$P(A_1/T)$	Probability of $population_3$ compromising $population_1$ given the strategy T.
$P(A_1/\bar{T})$	Probability of $population_3$ compromising $population_1$ given the strategy $\bar{T}$.
$P(A_2/S)$	Probability of $population_3$ to compromise $population_2$ given the strategy S.
$P(A_2/\bar{S})$	Probability of $population_3$ compromising $population_2$ given the strategy $\bar{S}$.
C_{10}	Cost of smart-home adoption.
C_{11}	Households' expenditure.
C_{12}	Cost related to the strategy T.
C_{13}	Cost of a security breach given the strategy $\bar{S}$.
C_{14}	Cost of cyberattacks on $population_1$ involving interruption costs of smart-home services and affecting $population_1$'s comfort and safety.
C_{20}	Cost of security implementation related to the strategy S.
C_{21}	Cost of cyberattacks on $population_2$ involving loss of intellectual property and customer confidential information, and lost revenue.
C_{30}	Cost of conducting a cyberattack targeting $population_1$, given that $population_1$ takes the strategy T.
C_{31}	Cost of conducting a cyberattack targeting $population_1$, given that $population_1$ takes the strategy $\bar{T}$.
C_{32}	Cost of conducting a cyberattack targeting $population_2$, given that $population_2$ takes the strategy S.
C_{33}	Cost of conducting a cyberattack targeting $population_2$, given that $population_2$ takes the strategy $\bar{S}$.
I_{10}	Households' income.
P_{20}	Amount of profit obtained by $population_2$ from selling smart-home devices given the strategy S.
P_{21}	Amount of profit obtained by $population_2$ from selling smart-home devices given the strategy $\bar{S}$.
R_{10}	Measure of the improved lifestyle that $population_1$ may enjoy by living in smart homes.
R_{11}	Reward of $population_1$ for noticing security countermeasures based on the strategy T.
R_{20}	Measure of $population_1$'s trust obtained by $population_2$ when considering the strategy S.

strategy of no attack, i.e., A_0.

Probabilities: We consider $P(A_1/T)$ and $P(A_1/\bar{T})$, respectively, to be the probabilities of $population_3$ to compromise $population_1$ given the strategies T and $\bar{T}$. Moreover, we consider $P(A_2/S)$ and $P(A_2/\bar{S})$, respectively, to be the probabilities of $population_3$ to compromise $population_2$ given the strategies S and $\bar{S}$. We assume that

$$P(A_1/\bar{T}) > P(A_1/T) \tag{23}$$

$$P(A_2/\bar{S}) > P(A_2/S) \tag{24}$$

$$P(A_2/\bar{S}) > P(A_1/T) \tag{25}$$

$$P(A_1/\bar{T}) > P(A_2/S) \tag{26}$$

$$P(A_2/\bar{S}) > P(A_1/\bar{T}) \tag{27}$$

$$P(A_1/T) > P(A_2/S) \tag{28}$$

We have (23) and (24) because we consider that $population_1$ and $population_2$ are more secure (i.e., less at risk of cyberattacks) when choosing the strategies T and S, respectively. We have (25) and (26) because we consider that an attacker is more likely to compromise a target that does not invest in cybersecurity. Moreover, we have (27) because $population_2$ has more assets (e.g., people, hardware, software, networks, cloud servers, and websites) resulting in more possible entry points for a cyberattack than $population_1$ in the case of strategies S and T, respectively. Finally, we have (28) because companies have more financial means than smart-home users to invest in cybersecurity and acquire adequate tangible, intangible, and human resources to ensure the implementation of security policies. Therefore, we assume that $population_1$ choosing the strategy T is less protected from cyberattacks than $population_2$ choosing the strategy S.

Costs: Let C_{10}, C_{11}, C_{12}, C_{13}, and C_{14} be the costs related to $population_1$. C_{10} measures the cost of buying a smart home and IoT devices. C_{11} measures smart-home users' expenditures on goods and services such as education, food, furniture, transportation, communication, and medical care. C_{12} measures the costs related to the strategy T. C_{13} measures the costs of a security breach given the strategy $\bar{S}$, i.e., an unnoticed breach of $population_2$'s insecure computer systems that allows $population_3$ to create backdoors to $population_1$'s IoT devices. C_{14} measures the costs incurred by cyberattacks on $population_1$, which could involve interruption costs of smart-home services (e.g., home automation, electric power, healthcare, entertainment, the Internet) and affect $population_1$'s comfort, convenience, and safety. Moreover, let C_{20} and C_{21} be the costs related to $population_2$. C_{20} measures the security implementation costs related to the strategy S. C_{21} measures the costs incurred by cyberattacks on $population_2$, which could involve loss of intellectual property and confidential customer information, reputational damage, business operation disruption, and lost revenue. Finally, let C_{30}, C_{31}, C_{32}, and C_{33} be the costs related to $population_3$. C_{30} and C_{31} respectively measure the costs of conducting cyberattacks targeting $population_1$ when this population takes the strategies T and $\bar{T}$. C_{32} and C_{33} respectively measure

the costs of conducting cyberattacks targeting $population_2$ when this population takes the strategies S and $\bar{S}$.

In what follows, we give rational assumptions about the relationships between system parameters. We first assume that all the cost parameters are non-negative:

$$C_{ij} \geq 0 \tag{29}$$

where $(i, j) = (1, 0), (1, 1), (1, 2), (1, 3), (1, 4), (2, 0), (2, 1), (3, 0), (3, 1), (3, 2), (3, 3)$

$$C_{21} > C_{14} \tag{30}$$

We also assume (30) because company assets are likely to be more valuable than smart-home assets. Thus the costs of cyberattacks on $population_2$ should be higher than those on $population_1$.

As for the relationship between cost parameters of $population_3$, we have the following assumptions.

$$C_{30} > C_{31} \tag{31}$$

$$C_{32} > C_{33} \tag{32}$$

We assume (31) and (32) because $population_3$ would require more resources to implement cyberattacks when $population_1$ (or $population_2$) takes the strategy T (or S) instead of the strategy $\bar{T}$ (or $\bar{S}$). We also assume that:

$$(C_{13} + C_{14})P(A_1/\bar{T}) > C_{14}P(A_1/\bar{T}) > C_{31} \tag{33}$$

$$(C_{13} + C_{21})P(A_2/\bar{S}) > C_{33} \tag{34}$$

$$C_{30} > (C_{13} + C_{14})P(A_1/T) > C_{14}P(A_1/T) \tag{35}$$

$$C_{32} > (C_{13} + C_{21})P(A_2/S) \tag{36}$$

(33) and (34) indicate that the attacker, i.e., $population_3$, commits fewer resources for a large gain by compromising a target that does not invest in cybersecurity, e.g. when $population_1$ takes the strategy $\bar{T}$ and $population_2$ takes the strategy $\bar{S}$. In the case of (35) and (36), targets, i.e., $population_1$ and $population_2$ invest in cybersecurity. They are more aware of cyber threats and cybersecurity best

practices. In such a scenario, we presume that $population_3$ will incur higher costs than the gain from a successful attack on $population_2$ and $population_3$.

Income and profits: I_{10} measures smart-home users' income. P_{20} and P_{21}, respectively, measures the amount of profit obtained by $population_2$ from selling smart-home devices given the strategies S and $\bar{S}$.

Rewards: Let R_{10} and R_{11} be the rewards of $population_1$. R_{10} quantifies the improved lifestyle that $population_1$ may enjoy by living in smart homes. R_{11} is the reward of $population_1$ for adopting good cybersecurity practices based on the strategy T. This reward measures the increased sense of feeling safe and secure when using IoT devices at home. Moreover, let R_{20} be the reward of $population_2$. R_{20} quantifies $population_1$'s trust obtained by $population_2$ when considering the strategy S.

$$R_{11} > C_{12} \tag{37}$$

We have (37) because $population_1$ would be willing to take the strategy T only if the merit of investing in cybersecurity awareness training, i.e., R_{11}, is larger than its cost, i.e., C_{12}.

We also assume that

$$P_{20} + R_{20} > C_{20} + P_{21} \tag{38}$$

We have (38) because companies, including $population_2$ (i.e., manufacturing companies), would be willing to invest in cybersecurity and take the strategy S only if the profit P_{20} obtained from sales using the strategy S and the good reputation R_{20} obtained based on the same strategy are larger than the cost of the strategy S plus the profit P_{21} obtained from sales using the strategy $\bar{S}$.

With the parameters of the game defined, we describe the strategy sets of each population in a matrix called the normal form.

4.2.3 Normal-Form Game

This subsection presents the strategies and payoffs resulting from our proposed game. Table 6 describes the strategic form of the game, also known as the normal-form game. Each cell $(row, column)$ from (5, 3) to (7, 6) represents the payoffs

Table 6: Normal-form game representation for the proposed evolutionary game.

		$Population_2$	
		S	
		$Population_1$	
		T	$\bar{T}$
$Population_3$	A_0	$I_{10}+R_{10}-C_{10}-C_{11}-C_{12}+R_{11}$ $P_{20}-C_{20}+R_{20}$ 0	$I_{10}+R_{10}-C_{10}-C_{11}$ $P_{20}-C_{20}+R_{20}$ 0
	A_1	$I_{10}+R_{10}-C_{10}-C_{11}-C_{12}+R_{11}-C_{14}P(A_1/T)$ $P_{20}-C_{20}+R_{20}$ $C_{14}P(A_1/T)-C_{30}$	$I_{10}+R_{10}-C_{10}-C_{11}-C_{14}P(A_1/\bar{T})$ $P_{20}-C_{20}+R_{20}$ $C_{14}P(A_1/\bar{T})-C_{31}$
	A_2	$I_{10}+R_{10}-C_{10}-C_{11}-C_{12}+R_{11}-C_{13}P(A_2/S)$ $P_{20}-C_{20}+R_{20}-C_{21}P(A_2/S)$ $(C_{13}+C_{21})P(A_2/S)-C_{32}$	$I_{10}+R_{10}-C_{10}-C_{11}-C_{13}P(A_2/S)$ $P_{20}-C_{20}+R_{20}-C_{21}P(A_2/S)$ $(C_{13}+C_{21})P(A_2/S)-C_{32}$
		$Population_2$	
		$\bar{S}$	
		$Population_1$	
		T	$\bar{T}$
	A_0	$I_{10}+R_{10}-C_{10}-C_{11}-C_{12}+R_{11}$ P_{21} 0	$I_{10}+R_{10}-C_{10}-C_{11}$ P_{21} 0
	A_1	$I_{10}+R_{10}-C_{10}-C_{11}-C_{12}+R_{11}-(C_{13}+C_{14})P(A_1/T)$ P_{21} $(C_{13}+C_{14})P(A_1/T)-C_{30}$	$I_{10}+R_{10}-C_{10}-C_{11}-(C_{13}+C_{14})P(A_1/\bar{T})$ P_{21} $(C_{13}+C_{14})P(A_1/\bar{T})-C_{31}$
	A_2	$I_{10}+R_{10}-C_{10}-C_{11}-C_{12}+R_{11}-C_{13}P(A_2/\bar{S})$ $P_{21}-C_{21}P(A_2/\bar{S})$ $(C_{13}+C_{21})P(A_2/\bar{S})-C_{33}$	$I_{10}+R_{10}-C_{10}-C_{11}-C_{13}P(A_2/\bar{S})$ $P_{21}-C_{21}P(A_2/\bar{S})$ $(C_{13}+C_{21})P(A_2/\bar{S})-C_{33}$

of each population. The first line of these cells shows *population*$_1$'s payoffs, the second line shows *population*$_2$'s payoffs, and the third line shows *population*$_3$'s payoffs. As an illustration, we explain the payoffs described in the cell Row 6 - Column 3. The strategies of *population*$_1$, *population*$_2$, and *population*$_3$, respectively, consist of playing the strategies T, S, and A_1. When each population engages in this contest, the payoffs of *population*$_1$, *population*$_2$, and *population*$_3$ are $I_{10}+R_{10}-C_{10}-C_{11}-C_{12}+R_{11}-C_{14}P(A_1/T)$, $P_{20}-C_{20}+R_{20}$, and $C_{14}P(A_1/T)-C_{30}$, respectively.

4.3 Game Analysis

This section aims to analyze the evolutionary stability of the proposed game, which relates to three populations: *population*$_1$, *population*$_2$, and *population*$_3$. We first derive the replicator equation related to each population. Then, we analyze the conditions that satisfy the evolutionary stability of the game.

4.3.1 Replicator Dynamics

The replicator dynamic is a fundamental concept in evolutionary game dynamic [64]. It is a deterministic model that describes selection dynamics (frequency dependent selection) through the use of equations.

Let $x(t)$, $y(t)$, $z_1(t)$, and $z_2(t)$, respectively, be the frequencies of the strategies T, S, A_1, and A_2 at time t ($t \geq 0$), where $0 \leq x(t), y(t), z_1(t), z_2(t) \leq 1$. Whenever possible, we will omit the time t for brevity. Note that the frequencies of the strategies $\bar{T}, \bar{S}$, and A_0 are given by $1-x, 1-y$, and $1-z_1-z_2$, respectively.

Replicator equation of *population*$_1$

Let F_T and $F_{\bar{T}}$, respectively, be the fitness of T and $\bar{T}$. $\overline{F_1}$ is the average expected fitness for *population*$_1$. The replicator equation of *population*$_1$ is:

$$\frac{dx}{dt} = x(F_T - \overline{F_1}) \tag{39}$$

We obtain

$$\begin{aligned}\frac{dx}{dt} =& x(x-1)[C_{12} - R_{11} + z_1 C_{13} P(A_1/T) + z_1 C_{14} P(A_1/T) - z_1 C_{13} P(A_1/\bar{T}) \\ & - z_1 C_{14} P(A_1/\bar{T}) - y z_1 C_{13} P(A_1/T) + y z_1 C_{13} P(A_1/\bar{T})]\end{aligned} \tag{40}$$

Replicator equation of *population*$_2$

Let F_S and $F_{\bar{S}}$, respectively, be the fitness of S and $\bar{S}$. $\overline{F_2}$ is the average expected fitness for *population*$_2$. The replicator equation of *population*$_2$ is:

$$\frac{dy}{dt} = y(F_S - \overline{F_2}) \tag{41}$$

We obtain

$$\frac{dy}{dt} = y(y-1)[C_{20} - P_{20} + P_{21} - R_{20} + z_2 C_{21} P(A_2/S) - z_2 C_{21} P(A_2/\bar{S})] \tag{42}$$

Replicator equations of *population*$_3$

Let F_{A_0}, F_{A_1}, and F_{A_2}, respectively, be the fitness of A_0, A_1 and A_2. $\overline{F_3}$ is the average expected fitness for *population*$_3$. The replicator equation of *population*$_3$ regarding the strategy A_1 is:

$$\frac{dz_1}{dt} = z_1(F_{A_1} - \overline{F_3}) \tag{43}$$

We obtain

$$\begin{aligned}\frac{dz_1}{dt} =& - z_1[z_1[(x(C_{30} - P(A_1/T)(C_{13} + C_{14})) - (C_{31} - P(A_1/\bar{T})(C_{13} + C_{14}))(x- \\ & 1))(y-1) - y(x(C_{30} - C_{14}P(A_1/T)) - (C_{31} - C_{14}P(A_1/\bar{T}))(x-1))] - [x \\ & (C_{30} - P(A_1/T)(C_{13} + C_{14})) - (C_{31} - P(A_1/\bar{T})(C_{13} + C_{14}))(x-1)](y- \\ & 1) + z_2[(x(C_{33} - P(A_2/\bar{S})(C_{13} + C_{21})) - (C_{33} - P(A_2/\bar{S})(C_{13} + C_{21}))(x- \\ & 1))(y-1) - y(x(C_{32} - P(A_2/S)(C_{13} + C_{21})) - (C_{32} - P(A_2/S)(C_{13}+ \\ & C_{21}))(x-1))] + y[x(C_{30} - C_{14}P(A_1/T)) - (C_{31} - C_{14}P(A_1/\bar{T}))(x-1)]]\end{aligned} \tag{44}$$

The replicator equation of *population*$_3$ regarding the strategy A_2 is:

$$\frac{dz_2}{dt} = z_2(F_{A_2} - \overline{F_3}) \tag{45}$$

We obtain

$$\begin{aligned}\frac{dz_2}{dt} =& - z_2[z_1[(x(C_{30} - P(A_1/T)(C_{13} + C_{14})) - (C_{31} - P(A_1/\bar{T})(C_{13} + C_{14})) \\ & (x-1))(y-1) - y(x(C_{30} - C_{14}P(A_1/T)) - (C_{31} - C_{14}P(A_1/\bar{T}))(x-1))] \\ & - [x(C_{33} - P(A_2/\bar{S})(C_{13} + C_{21})) - (C_{33} - P(A_2/\bar{S})(C_{13} + C_{21}))(x-1)] \\ & (y-1) + z_2[(x(C_{33} - P(A_2/\bar{S})(C_{13} + C_{21})) - (C_{33} - P(A_2/\bar{S})(C_{13} + C_{21})) \\ & (x-1))(y-1) - y(x(C_{32} - P(A_2/S)(C_{13} + C_{21})) - (C_{32} - P(A_2/S) \\ & (C_{13} + C_{21}))(x-1))] + y[x(C_{32} - P(A_2/S)(C_{13} + C_{21})) - (C_{32}- \\ & P(A_2/S)(C_{13} + C_{21}))(x-1)]]\end{aligned} \tag{46}$$

Let f be a multivariate function. We can observe from (40), (42), (44), and (46) that the following system of equations defines the game.

$$\begin{cases} f(x) & = \frac{dx}{dt} \\ f(y) & = \frac{dy}{dt} \\ f(z_1) & = \frac{dz_1}{dt} \\ f(z_2) & = \frac{dz_2}{dt} \end{cases} \tag{47}$$

4.3.2 Conditions for ESS

Any solution of the system defined in (47) is a Nash equilibrium of the proposed evolutionary game model. Moreover, any stable equilibrium of the replicator equations is an ESS. A Jacobian matrix could be used to analyze the stability of equilibrium solutions [68].

Nash equilibrium

In each Nash equilibrium, any agent (player) cannot improve its own payoff if other players do not change their strategies. This situation can be interpreted as a steady state of the system as a result of individuals' rational decision making for their payoff maximization. A pure strategy Nash equilibrium refers to a game in which every player's mixed strategy in a mixed strategy Nash equilibrium assigns probability 1 to a single action [54]. A mixed strategy Nash equilibrium 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. In an attack-defense game, we use the Nash equilibrium to identify the best set of actions that will maximize the defenders' payoff against cyberattacks.

We solve (47) to identify the Nash equilibrium solutions of the proposed game. $f(x) = f(y) = f(z_1) = f(z_2) = 0$, we obtain 22 solutions. Thus, the proposed evolutionary game model admits 22 Nash equilibrium solutions: 12 pure and 10 mixed solutions. According to Abass et al. [66], when the game is asymmetric, only the pure solutions are necessary to build the Jacobian matrix. The pure Nash equilibrium solutions of the proposed game are $E_1 = (0,0,0,0); E_2 = (1,0,0,0); E_3 = (0,1,0,0); E_4 = (0,0,1,0); E_5 = (0,0,0,1); E_6 = (1,1,0,0); E_7 = (1,0,1,0); E_8 = (0,1,1,0); E_9 = (1,0,0,1); E_{10} = (0,1,0,1); E_{11} = (1,1,1,0);$

$E_{12} = (1, 1, 0, 1)$.

Jacobian matrix

We use the Jacobian matrix to analyze the sign of eigenvalues and evaluate the stability of the Nash equilibrium solutions that we found. Let J be the Jacobian matrix of the multivariate function f. By analyzing the eigenvalues of J, we can gain valuable insights into the stability properties of the Nash equilibrium solutions.

$$\mathbf{J} = \begin{bmatrix} \frac{\partial f(x)}{\partial x} & \frac{\partial f(x)}{\partial y} & \frac{\partial f(x)}{\partial z_1} & \frac{\partial f(x)}{\partial z_2} \\ \frac{\partial f(y)}{\partial x} & \frac{\partial f(y)}{\partial y} & \frac{\partial f(y)}{\partial z_1} & \frac{\partial f(y)}{\partial z_2} \\ \frac{\partial f(z_1)}{\partial x} & \frac{\partial f(z_1)}{\partial y} & \frac{\partial f(z_1)}{\partial z_1} & \frac{\partial f(z_1)}{\partial z_2} \\ \frac{\partial f(z_2)}{\partial x} & \frac{\partial f(z_2)}{\partial y} & \frac{\partial f(z_2)}{\partial z_1} & \frac{\partial f(z_2)}{\partial z_2} \end{bmatrix} \tag{48}$$

For a comprehensive understanding of the calculations involved in equilibrium stability analysis using J, we provide a detailed description of f in Appendix A.

Equilibrium stability analysis

This section studies the stablity of equilibrium solutions. Among the existing Nash equilibrium solutions, $E_1 = (0, 0, 0, 0)$, $E_2 = (1, 0, 0, 0)$, $E_3 = (0, 1, 0, 0)$, and $E_6 = (1, 1, 0, 0)$ are desirable solutions. As a matter of fact, the proposed game is based on attack-defense strategies in which the defenders' strategies consist of investing in cybersecurity, i.e., playing 1 (S or T), to protect themselves effectively against cyberattacks. It is obvious that the ultimate and invariable condition that guarantees that the defenders will always be safe regardless of their choice of strategy is the absence of attacks, i.e., when the attacker plays $(0, 0)$.

We analyze the sign of eigenvalues of the Jacobian matrices, i.e., $J(E_1), \ldots, J(E_{12})$, obtained using the corresponding solutions, i.e., $E_1, \ldots, E_{12}$, respectively. An equilibrium solution E_p (with $p = 1, \ldots, 12$) is asymptotically stable if the eigenvalues obtained from $J(E_p)$ have all negative real parts. Table 7 presents the results of equilibrium stability analysis. The eigenvalues associated with each

Table 7: Summary of equilibrium stability analysis.

Pure Nash equilibrium solutions	Eigenvalues				Sign of eigenvalues	Conditions for stability	ESS
	λ_1	λ_2	λ_3	λ_4			
$E_1 = (0,0,0,0)$	$R_{11} - C_{12}$	$P_{20} - C_{20} - P_{21} + R_{20}$	$(C_{13} + C_{14})P(A_1/\bar{T}) - C_{31}$	$(C_{13} + C_{21})P(A_2/\bar{S}) - C_{33}$	$\lambda_1 > 0$ $\lambda_2 > 0$ $\lambda_3 > 0$ $\lambda_4 > 0$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_2 = (1,0,0,0)$	$C_{12} - R_{11}$	$P_{20} - C_{20} - P_{21} + R_{20}$	$(C_{13} + C_{14})P(A_1/T) - C_{30}$	$(C_{13} + C_{21})P(A_2/\bar{S}) - C_{33}$	$\lambda_1 < 0$ $\lambda_2 > 0$ $\lambda_3 < 0$ $\lambda_4 > 0$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_3 = (0,1,0,0)$	$R_{11} - C_{12}$	$C_{20} - P_{20} + P_{21} - R_{20}$	$C_{14}P(A_1/\bar{T}) - C_{31}$	$(C_{13} + C_{21})P(A_2/S) - C_{32}$	$\lambda_1 > 0$ $\lambda_2 < 0$ $\lambda_3 > 0$ $\lambda_4 < 0$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_4 = (0,0,1,0)$	$(C_{13} + C_{14})[P(A_1/\bar{T}) - P(A_1/T)] + R_{11} - C_{12}$	$P_{20} - C_{20} - P_{21} + R_{20}$	$(-C_{13} - C_{14})P(A_1/\bar{T}) + C_{31}$	$(-C_{13} - C_{14})P(A_1/\bar{T}) + (C_{13} + C_{21})P(A_2/\bar{S}) + C_{31} - C_{33}$	$\lambda_1 > 0$ $\lambda_2 > 0$ $\lambda_3 < 0$ Uncertain	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_5 = (0,0,0,1)$	$R_{11} - C_{12}$	$C_{21}[P(A_2/\bar{S}) - P(A_2/S)] + P_{20} - C_{20} - P_{21} + R_{20}$	$(C_{13} + C_{14})P(A_1/\bar{T}) + (-C_{13} - C_{21})P(A_2/\bar{S}) + C_{33} - C_{31}$	$(-C_{13} - C_{21})P(A_2/\bar{S}) + C_{33}$	$\lambda_1 > 0$ $\lambda_2 > 0$ Uncertain $\lambda_4 < 0$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_6 = (1,1,0,0)$	$C_{12} - R_{11}$	$C_{20} - P_{20} + P_{21} - R_{20}$	$C_{14}P(A_1/T) - C_{30}$	$(C_{13} + C_{21})P(A_2/S) - C_{32}$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✓
$E_7 = (1,0,1,0)$	$(C_{13} + C_{14})[P(A_1/T) - P(A_1/\bar{T})] + C_{12} - R_{11}$	$P_{20} - C_{20} - P_{21} + R_{20}$	$(-C_{13} - C_{14})P(A_1/T) + C_{30}$	$(-C_{13} - C_{14})P(A_1/T) + (C_{13} + C_{21})P(A_2/\bar{S}) + C_{30} - C_{33}$	$\lambda_1 < 0$ $\lambda_2 > 0$ $\lambda_3 > 0$ Uncertain	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_8 = (0,1,1,0)$	$C_{14}[P(A_1/\bar{T}) - P(A_1/T)] + R_{11} - C_{12}$	$C_{20} - P_{20} + P_{21} - R_{20}$	$-C_{14}P(A_1/\bar{T}) + C_{31}$	$-C_{14}P(A_1/\bar{T}) + (C_{13} + C_{21})P(A_2/S) + C_{31} - C_{32}$	$\lambda_1 > 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ Uncertain	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_9 = (1,0,0,1)$	$C_{12} - R_{11}$	$C_{21}[P(A_2/\bar{S}) - P(A_2/S)] + P_{20} - C_{20} - P_{21} + R_{20}$	$(C_{13} + C_{14})P(A_1/T) + (-C_{13} - C_{21})P(A_2/\bar{S}) + C_{33} - C_{30}$	$(-C_{13} - C_{21})P(A_2/\bar{S}) + C_{33}$	$\lambda_1 < 0$ $\lambda_2 > 0$ Uncertain $\lambda_4 < 0$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_{10} = (0,1,0,1)$	$R_{11} - C_{12}$	$C_{21}[P(A_2/S) - P(A_2/\bar{S})] + C_{20} - P_{20} + P_{21} - R_{20}$	$C_{14}P(A_1/\bar{T}) + (-C_{13} - C_{21})P(A_2/S) + C_{32} - C_{31}$	$(-C_{13} - C_{21})P(A_2/S) + C_{32}$	$\lambda_1 > 0$ $\lambda_2 < 0$ Uncertain $\lambda_4 > 0$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_{11} = (1,1,1,0)$	$C_{14}[P(A_1/T) - P(A_1/\bar{T})] + C_{12} - R_{11}$	$C_{20} - P_{20} + P_{21} - R_{20}$	$-C_{14}P(A_1/T) + C_{30}$	$-C_{14}P(A_1/T) + (C_{13} + C_{21})P(A_2/S) + C_{30} - C_{32}$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 > 0$ Uncertain	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_{12} = (1,1,0,1)$	$C_{12} - R_{11}$	$C_{21}[P(A_2/S) - P(A_2/\bar{S})] + C_{20} - P_{20} + P_{21} - R_{20}$	$C_{14}P(A_1/T) + (-C_{13} - C_{21})P(A_2/S) + C_{32} - C_{30}$	$(-C_{13} - C_{21})P(A_2/S) + C_{32}$	$\lambda_1 < 0$ $\lambda_2 < 0$ Uncertain $\lambda_4 > 0$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗

equilibrium solution, i.e., $J(E_p)$, are real. On the other hand, the sign of each eigenvalue depends on the Nash equilibrium.

We have the following theorem.

Theorem 3. *The proposed evolutionary game model admits a unique ESS. Only* $E_6 = (1, 1, 0, 0)$ *satisfies the conditions for asymptotic stability (*$\lambda_q < 0$*, where* $q = 1, \ldots, 4$*).*

Proof. We show that the eigenvalues of E_6 are all negative. Then we demonstrate that the other Nash equilibrium solutions have at least one positive eigenvalue.

E_6 is asymptotically stable.

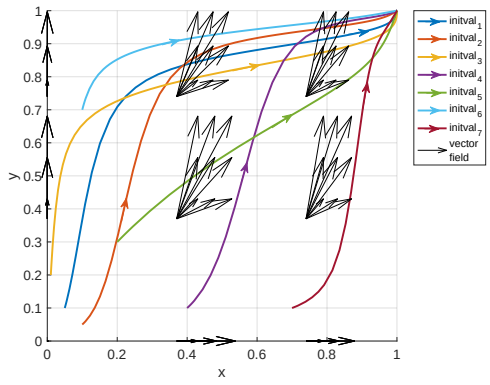
The eigenvalues of E_6 are $\lambda_1 = C_{12} - R_{11}$, $\lambda_2 = C_{20} - P_{20} + P_{21} - R_{20}$, $\lambda_3 = C_{14}P(A_1/T) - C_{30}$, and $\lambda_4 = (C_{13} + C_{21})P(A_2/S) - C_{32}$. First, we have $\lambda_1 < 0$ because $R_{11} > C_{12}$ (37). Then, we have $\lambda_2 < 0$ because $P_{20} + R_{20} > C_{20} + P_{21}$ (38). Next, we have $\lambda_3 < 0$ because $C_{30} > C_{14}P(A_1/T)$ (35). Finally, we have $\lambda_4 < 0$ because $C_{32} > (C_{13} + C_{21})P(A_2/S)$ (36). The eigenvalues λ_1, λ_2, λ_3, and λ_4 are negative. Therefore, E_6 is asymptotically stable.

The other Nash equilibrium solutions are not asymptotically stable.

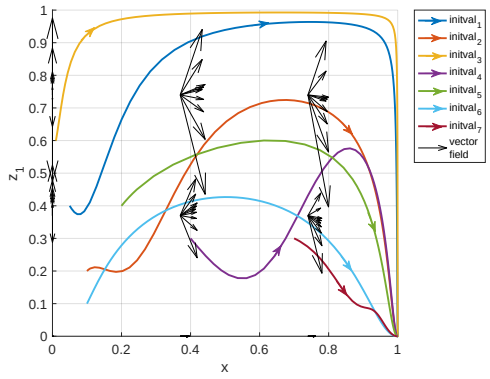
The eigenvalue λ_1 of Nash equilibrium solutions E_1, E_3, E_4, E_5, E_8, and E_{10} is positive because of (37). The eigenvalue λ_2 of E_2 and E_7 is positive because of (38). Similarly, the eigenvalue λ_2 of E_9 is positive because of (24), (29), and (38). From (35), we can notice that the eigenvalue λ_3 of E_{11} is positive. Moreover, the eigenvalues λ_4 of E_{12} is positive because of (36). As a result, the Nash equilibrium solutions E_p (with $p = 1, \ldots, 12, p \neq 6$) have at least one positive eigenvalue. For this reason, they are not asymptotically stable. □

4.4 Numerical Results

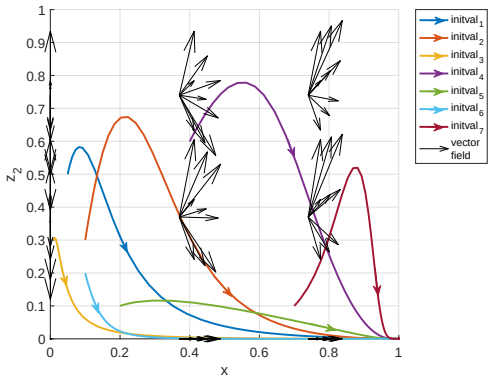
This section presents the numerical results of the proposed game using the analyses conducted in Section 4.3. First, we show graphically that E_6 is an ESS. Next, we investigate the impacts of cybersecurity investment costs and benefits on E_6. We choose the parameter settings described in Table 8 to illustrate the numerical results.



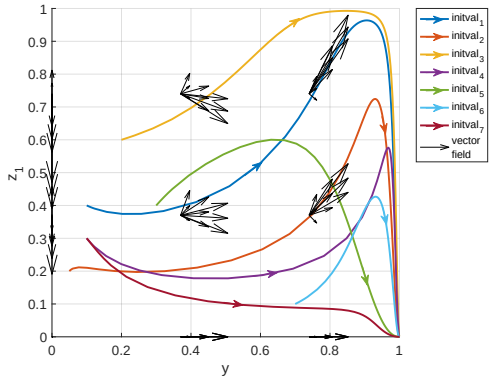
(a) Phase portrait view (x y).



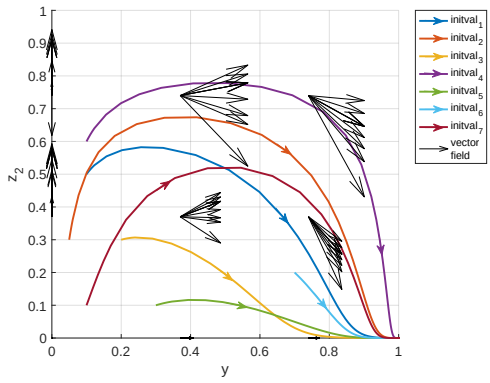
(b) Phase portrait view (x z_1).



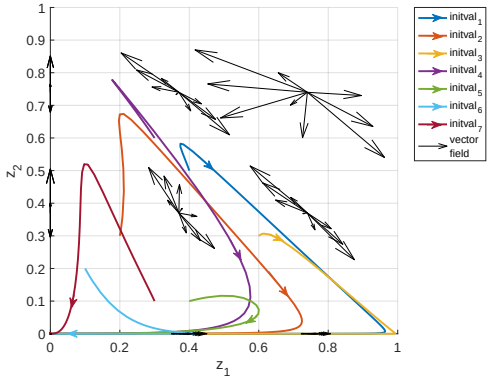
(c) Phase portrait view (x z_2).



(d) Phase portrait view (y z_1).



(e) Phase portrait view (y z_2).



(f) Phase portrait view (z_1 z_2).

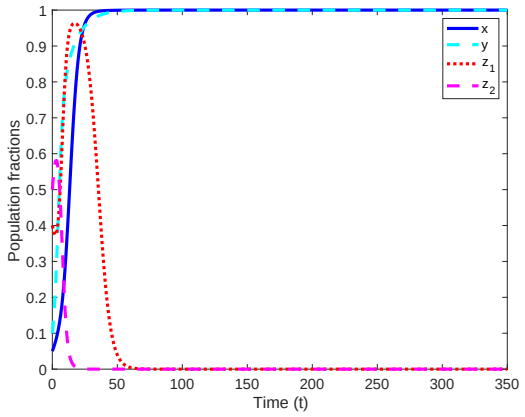
Figure 8: 4-dimensional phase portraits by state combinations.

Table 8: List of parameter values used in the numerical results.

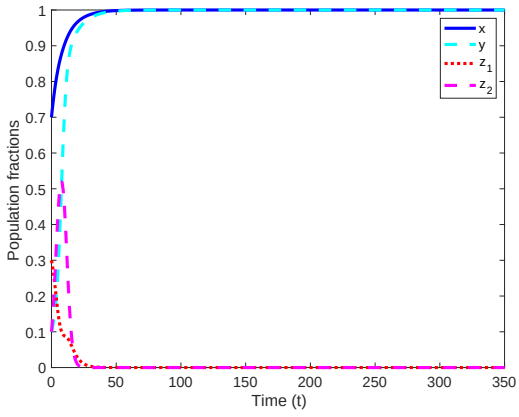
Parameters	Values
$P(A_1/T)$	0.3
$P(A_1/\bar{T})$	0.6
$P(A_2/S)$	0.1
$P(A_2/\bar{S})$	0.8
C_{12}	0.1
C_{13}	0.2
C_{14}	0.6
C_{20}	0.2
C_{21}	0.8
C_{30}	0.4
C_{31}	0.15
C_{32}	0.7
C_{33}	0.25
P_{20}	0.25
P_{21}	0.1
R_{11}	0.2
R_{20}	0.15
Seven kinds of initial values	(0.05, 0.1, 0.4, 0.5); (0.1, 0.05, 0.2, 0.3);
$(x(0), y(0), z_1(0), z_2(0))$:	(0.01, 0.2, 0.6, 0.3); (0.4, 0.1, 0.3, 0.6);
$initval_1, \ldots, initval_7$	(0.2, 0.3, 0.4, 0.1); (0.1, 0.7, 0.1, 0.2); (0.7, 0.1, 0.3, 0.1).

4.4.1 Numerical Validation of the Stability of E_6

We start by demonstrating that the proposed system is asymptotically stable by using the n-dimensional phase portraits by state combinations [69]. According to this method, Figure 8 illustrates the phase portrait views for the $m = 6$ combinations of states where $m = \frac{n!}{2(n-2)!}$ with $n = 4$. In addition to the vector fields, we plot the system trajectories using different colored lines (blue, brown, orange, purple, green, cyan, and maroon) based on the seven initial values described in Table 8. Figures 8(a), (b), (c), (d), (e), and (f), respectively, show that the vector fields converge to $(x, y) = (1, 1)$, $(x, z_1) = (1, 0)$, $(x, z_2) = (1, 0)$, $(y, z_1) = (1, 0)$, $(y, z_2) = (1, 0)$, and $(z_1, z_2) = (0, 0)$. The analysis of the view of each state combination reveals that the vector fields converge to the Nash equilibrium $E_6 = (1, 1, 0, 0)$. Figures 9(a) and (b) show the evolution of population fractions x, y, z_1, and z_2 over time under the initial values $initval_1$ and $initval_7$,



(a) Evolution of population fractions over time with initial values $x(0)$=0.05, $y(0)$=0.1, $z_1(0)$=0.4, and $z_2(0)$=0.5.



(b) Evolution of population fractions over time with initial values $x(0)$=0.7, $y(0)$=0.1, $z_1(0)$=0.3, and $z_2(0)$=0.1.

Figure 9: Population evolution of x, y, z_1, and z_2 over time.

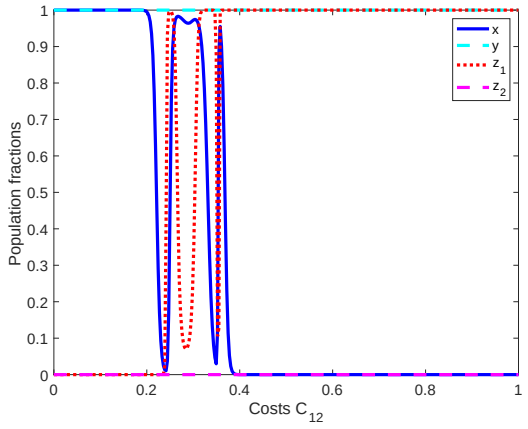
respectively. We can confirm from both Figures 9(a) and (b) that the system converges to the Nash equilibrium E_6. The convergence of directional fields and the asymptotical stability of the evolution of x, y, z_1, and z_2 over time validate the correctness of our theoretical analysis regarding the stability of E_6.

In the following, we examine the effects of various parameters on the ESS, i.e., E_6.

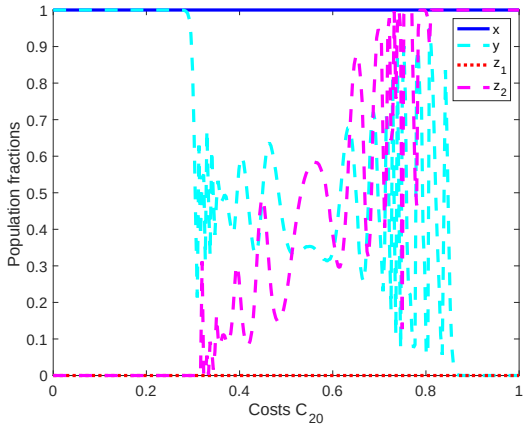
4.4.2 Analyzing the Effects of Cybersecurity and Cyberattack Costs on E_6

The impact of cybersecurity costs

We first focus on the cybersecurity costs (C_{12} and C_{20}) and numerically evaluate their impacts by changing one of them. Recall that $C_{12} < 0.2$ is required by (37) for making E_6 ESS. Similarly, $C_{20} < 0.3$ is required by (38). Figure 10(a) presents the evolution of population fractions over C_{12}. We can see that the system converges to $E_6 = (1, 1, 0, 0)$ and $E_8 = (0, 1, 1, 0)$ when $C_{12} < 0.2$ and $C_{12} > 0.38$, respectively. On the other hand, the population fractions x and z_1 fluctuate when $0.2 < C_{12} < 0.38$. Figure 10(b) presents the evolution of



(a) Evolution of population fractions x, y, z_1, and z_2 over C_{12}.



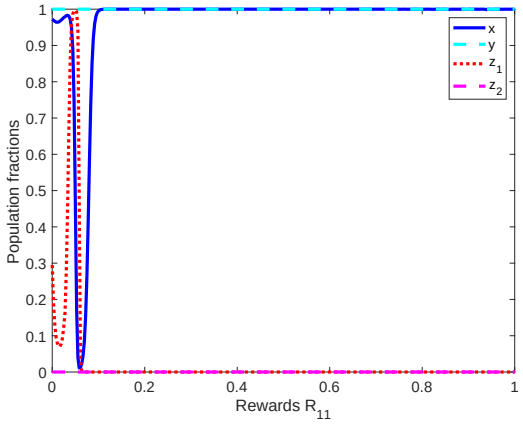
(b) Evolution of population fractions x, y, z_1, and z_2 over C_{20}.

Figure 10: The impact of cybersecurity costs on the ESS E_6.

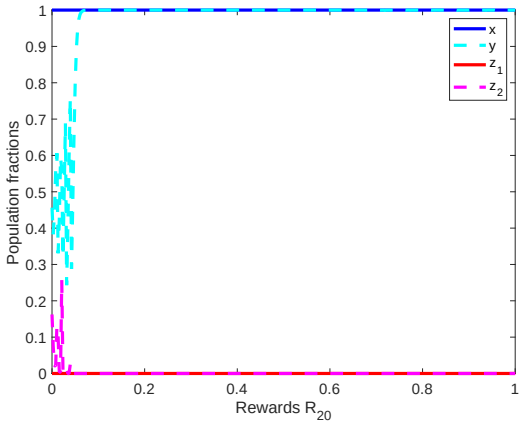
population fractions over C_{20}. The system converges to $E_6 = (1, 1, 0, 0)$ and $E_9 = (1, 0, 0, 1)$ when $C_{20} < 0.3$ and $C_{20} > 0.86$, respectively. On the other hand, the population fractions y and z_2 fluctuate when $0.3 < C_{20} < 0.86$. The evaluation of cybersecurity cost parameters shows that $C_{12} < 0.2$ and $C_{20} < 0.3$ satisfy the ESS conditions for E_6.

The impact of rewards for commitment to cybersecurity

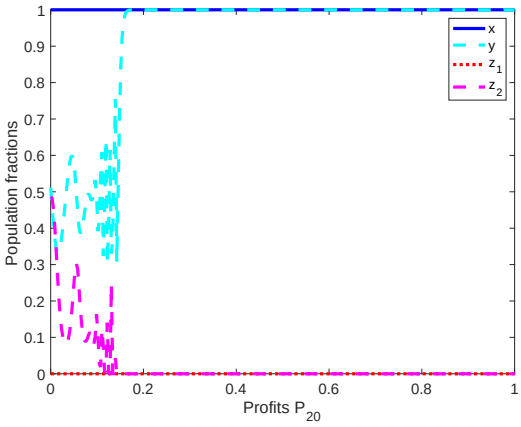
We now numerically evaluate the impacts of rewards (R_{11} and R_{20}) and profits (P_{20}) for commitment to cybersecurity. Recall that $R_{11} > 0.1$ is required by (37) for making E_6 ESS. Similarly, $R_{20} > 0.05$ and $P_{20} > 0.15$ are required by (38). Figure 11(a) presents the evolution of population fractions over R_{11}. We can see that the system converges to $E_6 = (1, 1, 0, 0)$ when $R_{11} > 0.1$. On the other hand, the population fractions x and z_1 fluctuate when $R_{11} < 0.1$. Figures 11(b) and (c) show that the population fractions x, y, z_1, and z_2 over R_{20} and P_{20} remain constant and equivalent to E_6 when $R_{20} > 0.05$ and $P_{20} > 0.15$, respectively. When $R_{20} < 0.05$ and $P_{20} < 0.15$, y and z_2 fluctuate. The evaluation of profit and reward parameters shows that $R_{11} > 0.1$, $R_{20} > 0.05$, and $P_{20} > 0.15$ satisfy the ESS conditions for E_6.



(a) Evolution of population fractions x, y, z_1, and z_2 over R_{11}.



(b) Evolution of population fractions x, y, z_1, and z_2 over R_{20}.

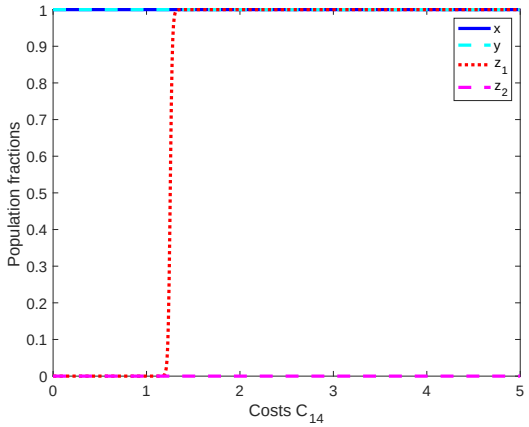


(c) Evolution of population fractions x, y, z_1, and z_2 over P_{20}.

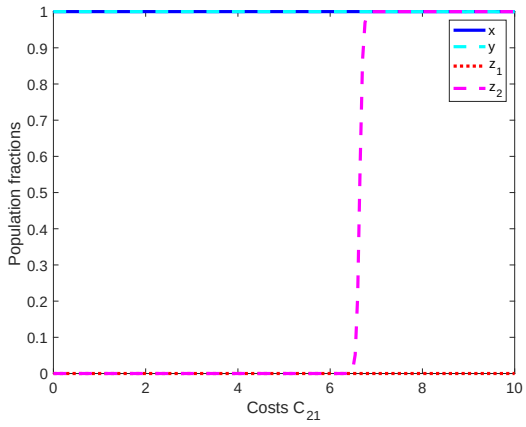
Figure 11: The impact of rewards for cybersecurity commitment on the ESS E_6.

The impact of cyberattack costs

We also investigate the cyberattack costs and numerically evaluate their impacts by changing one of them. Recall that $C_{14} < 0.8$ and $C_{21} > 0.6$ are required by (30) for making E_6 ESS. Figure 12(a) presents the evolution of population fractions over C_{14}. We can see that the system converges to $E_6 = (1, 1, 0, 0)$ when $C_{14} \leq 1.333$. Otherwise, it converges to $E_{11} = (1, 1, 1, 0)$. Figure 12(b) presents the evolution of population fractions over C_{21}. The system converges to



(a) Evolution of population fractions x, y, z_1, and z_2 over C_{14}.



(b) Evolution of population fractions x, y, z_1, and z_2 over C_{21}.

Figure 12: The impact of cyberattack costs on the ESS E_6.

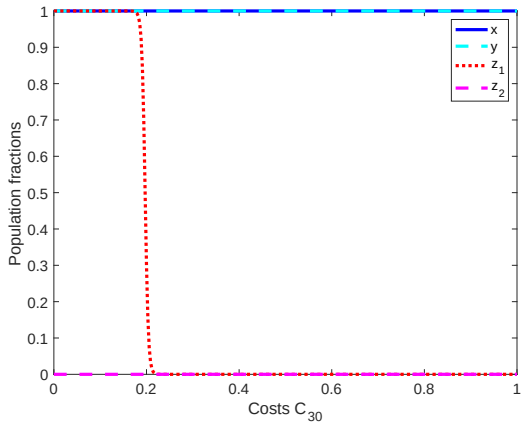
E_6 when $C_{21} < 6.8$. Otherwise, it converges to $E_{12} = (1, 1, 0, 1)$. The evaluation of cyberattack costs show that $C_{14} \leq 1.333$ and $C_{21} < 6.8$ satisfy the ESS conditions for E_6.

Costs of setting up cyberattack operations

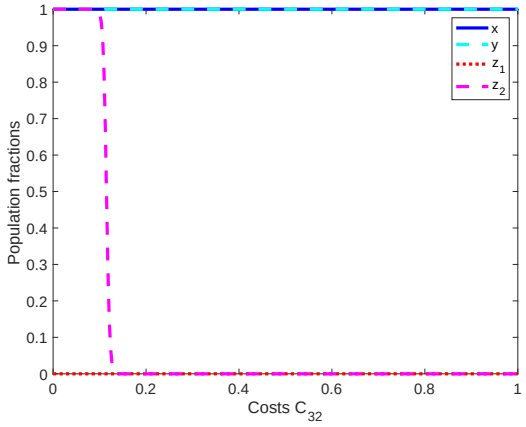
We finally investigate the operation costs of cyberattacks and numerically evaluate their impacts by changing one of them. Recall that $C_{30} > 0.15$ is required by (31) for making E_6 ESS. Similarly, $C_{32} > 0.25$ is required by (32). Figure 13(a) shows that the system converges to $E_6 = (1, 1, 0, 0)$ and $E_{11} = (1, 1, 1, 0)$ when $C_{30} > 0.18$ and $C_{30} < 0.18$, respectively. Figure 13(b) shows that the system converges to E_6 and $E_{12} = (1, 1, 0, 1)$ when $C_{32} > 0.1$ and $C_{32} < 0.1$, respectively. The evaluation of cost parameters of implementing cyberattacks show that $C_{30} > 0.18$ and $C_{32} > 0.1$ satisfy the ESS conditions for E_6.

4.5 Discussion

This section discusses the findings, highlights the limitations, and presents future work.



(a) Evolution of population fractions x, y, z_1, and z_2 over C_{30}.



(b) Evolution of population fractions x, y, z_1, and z_2 over C_{32}.

Figure 13: The impact of operation costs of cyberattacks on the ESS E_6.

4.5.1 Interpretation of the Results

With the purpose of verifying whether it is worthwhile for smart-home users to invest in cybersecurity over time, we defined and analyzed a smart-home ecosystem-based game model using an evolutionary game theory. The numerical results showed that the best strategy set for smart-home users is $E_6 = (1, 1, 0, 0) = (T, S, A_0)$. This implies that smart-home users and smart-home stakeholders must invest in cybersecurity and follow cybersecurity best practices. If they commit to cybersecurity as recommended, we found that adversaries would abstain from attacking because the costs of setting up cyberattack operations would be higher than the expected gain. Thus, it is beneficial for smart-home users to incur some costs for engaging in cybersecurity awareness training.

On the basis of the findings, we discuss the essential parameters used in this study.

Cybersecurity Costs

The results indicate that low cybersecurity costs ($C_{12} < 0.2$ and $C_{20} < 0.3$) maintain the desired equilibrium solution E_6 while the increasing costs of cybersecurity awareness training and implementing cybersecurity best practices for IoT technol-

ogy lead smart-home users and manufacturers to stop investing in cybersecurity strategies, respectively. This outcome is consistent with the finding that reducing investment costs promote information security investments [42]. Moreover, smart-home users are willing to commit to cybersecurity awareness training if the training costs are zero [70]. Indeed, not all smart-home users have the means to pay for additional training outside of spending on everyday goods and services. Therefore, governments could promote cybersecurity awareness among smart-home users by elevating its significance within national cybersecurity strategies and providing subsidies for associated training expenses.

Rewards

The results indicate that offering rewards and benefits ($R_{11} > 0.1$, $R_{20} > 0.05$, and $P_{20} > 0.15$) based on commitment to cybersecurity helps maintain the desired equilibrium solution E_6 in which smart-home users are involved in cybersecurity. The findings align with previous research [70] showing through a static game model that providing smart-home users with tangible rewards could engage them in cybersecurity education programs. Indeed, rewards (both financial and non-financial) can have positive effects on user security behavior [71]. From this perspective, additional research on non-financial rewards that might motivate smart-home users to engage in cybersecurity would be appropriate.

Cyberattack Costs

The results indicate that if the costs incurred by cyberattacks on smart-home users and manufacturers, respectively, are low ($C_{14} \leq 1.333$ and $C_{21} < 6.8$), adversaries would be less interested in carrying out cyberattacks. Therefore, the desired equilibrium E_6 would remain intact. We obtain this outcome because the proposed model considers that attackers incur costs to carry out cyberattacks. Even though this is true in reality, it is clear that with the sources of information available in this digital era, attackers could carry out cyberattacks at almost no cost. Thus, even with low costs incurred by cyberattacks on smart-home users and manufacturers, attackers would not refrain from attacking. This pattern would break the desired equilibrium and expose smart-home users and manufacturers to potential cyberattacks. It is therefore essential to strengthen the cybersecu-

rity of smart homes by taking into consideration international standards such as ISO/IEC 27403 [72], which is currently under development. The objective is to not tolerate any costs due to cyberattacks so as to deter attackers.

Operation Costs of Cyberattacks

The results indicate that if the costs, i.e., $C_{30} > 0.18$ and $C_{32} > 0.1$, of setting up cyberattack operations become very expensive, adversaries will abandon attack strategies, which will help preserve the desired equilibrium solution E_6. On the other hand, the results show that smart-home users and manufacturers will continuously be exposed to cyberattacks if the costs of implementing cyberattacks are low or negligible. In this increasingly digitalized world, attackers can afford to develop targeted attack scenarios at little or no cost that could have a significant global impact. From this observation, it is apparent that if attackers can develop attacks at a lower cost, it is also necessary to allow smart-home users to get educated and trained in cybersecurity at a lower cost. We need to ensure cybersecurity for all, by all, and of all, in the near future to lessen the likelihood of successful cyberattacks.

4.5.2 Limitations and Recommendations

Although our evolutionary game model yields significant findings about the costs and benefits of cybersecurity investment strategies for smart-home users, the study has several limitations that future studies should address to improve the accuracy and applicability of the findings.

Firstly, our proposed model assumes that all independent stakeholders, such as IoT device manufacturers, network providers, and cloud service providers, can be grouped into a single entity (i.e., $population_2$) to provide a holistic analysis of the system. However, this approach may oversimplify the complexity of interactions among stakeholders. Therefore, future studies should design a more sophisticated game model that includes a greater depth and volume of agents, their strategy sets, and payoffs to improve the applicability of the findings. Monte Carlo simulation ca be a valuable approach to achieve it.

Secondly, our model assumes that attackers can either target smart-home users directly or indirectly via stakeholders, but not both at the same time. How-

ever, this assumption may not capture the reality of smart-home attacks, where attackers can use multiple techniques to target different entities simultaneously. Future research should address this scenario to improve the model's accuracy.

Additionally, while our study focuses only on monetary costs, other research could consider time-related costs in their models and simulations. It is worth noting that the time required to learn and implement cybersecurity best practices could deter smart-home users from engaging in cybersecurity awareness training. Furthermore, the time taken to identify vulnerabilities and develop cyberattacks may be a significant factor that influences attackers' decisions to refrain from attacking. Therefore, including time-related costs in the model can provide a more realistic representation of the system.

Finally, another limitation of our study is the challenge of verifying the accuracy of the parameter values used to obtain the numerical results. Future research should aim to collect empirical data and compare it with the theoretical results to validate the model. Empirical validation can enhance the reliability of our findings.

4.6 Summary

In Chapter 4, we studied the costs and benefits of cybersecurity investment strategies against cyberattacks for smart-home users using an evolutionary game-theoretic approach. We modeled the interactions between three populations, i.e., smart-home users, stakeholders, and attackers. We derived and analyzed the replicator dynamics of this game to identify the evolutionarily stable strategy (ESS). Furthermore, we investigated the impacts of the costs and benefits of cybersecurity investment and cyberattack costs on the ESS. The results showed that the optimal strategy for smart-home users involved both users and stakeholders investing in cybersecurity, reducing the likelihood of successful attacks and discouraging attackers from continuing their attack efforts unless they were willing to incur losses. However, the training costs must be low and affordable for smart-home users to ensure their participation and engagement. Additionally, providing rewards for their commitment to cybersecurity is crucial in sustaining their interest and investment in the long term. Finally, the chapter suggested that empirical investigations should support the theoretical results.

5. Examining Smart-Home Users' Interests in Cybersecurity Awareness Training and Behavioral Incentives

This chapter investigates the interests of smart-home users in adopting sound cybersecurity practices through cybersecurity awareness training and non-financial rewards. Section 5.1 outlines the rationale for selecting Japan and the United Kingdom (UK) as the contexts for our cross-cultural study. Section 5.2 describes the research methodology employed to collect and analyze data. Section 5.3 presents our key findings. In Section 5.4, we interpret and contextualize the results, highlighting the similarities and differences between the two countries. Finally, Section 5.5 summarizes the chapter.

5.1 Introduction

Smart homes have gained immense popularity worldwide, with a projected global smart home market worth of $444.98 billion by 2030 [73]. The increasing adoption of smart-home devices has revolutionized people's lives, providing enhanced comfort, convenience, and energy efficiency. However, this growth has also created new security challenges, especially in regards to the cybersecurity of smart-home devices and networks. Therefore, smart-home users must be aware of the potential cyber risks associated with their devices and take appropriate measures to mitigate those risks.

This chapter explores the potential interests of adult smart-home users in cybersecurity awareness training and the non-financial incentives that may encourage them to adopt good cybersecurity practices. The study focuses on two leading nations for smart-home technologies, Japan and the UK. In Japan, the household penetration of smart homes is projected to reach 70.2% by 2027, with 40.17 million active smart-home users, while in the UK, the penetration is expected to reach 98.8% by 2027, with 29.70 million active smart-home users [74, 75].

Japan and the UK have significant differences in their socio-economic status (SES), including income inequality, education, and job security. Japan has lower income inequality, better health, and social well-being than the UK [76, 77]. In

addition, Japan emphasizes job security and lifetime employment, with a more homogeneous education system. In contrast, the UK has a diverse education system and a more flexible labor market. Furthermore, the two countries have distinct cultural disparities, as illustrated by Hofstede's six dimensions of national cultures [34]. Figure 14 shows that Japan tends to adhere to hierarchical positions in society more than the UK, with collectivism, conformity, and harmony being their primary focus. In contrast, the British prioritize individualism, and competitiveness between groups is more apparent in Japan.

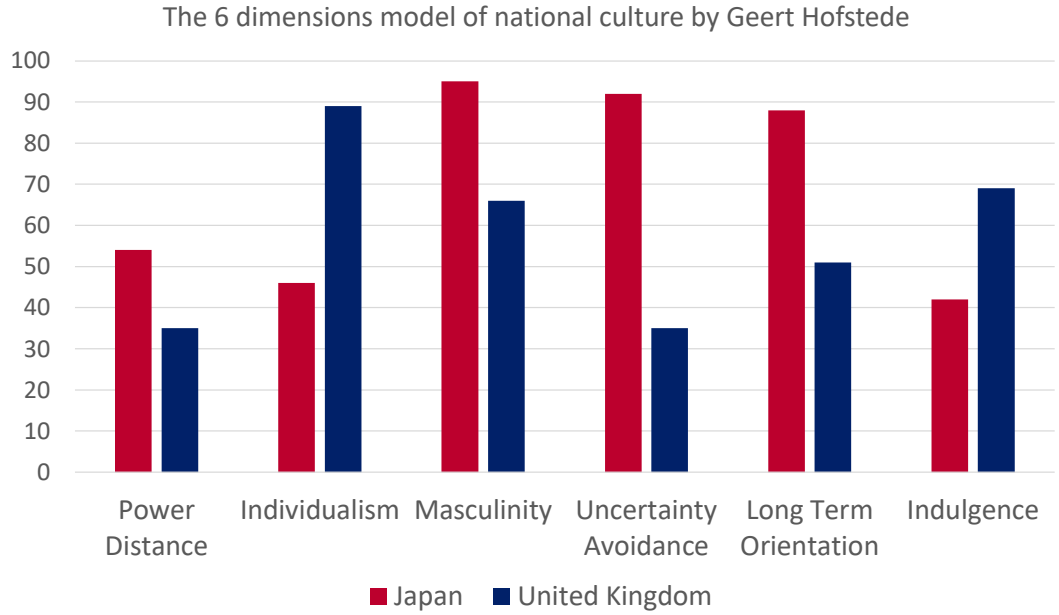


Figure 14: Cultural differences between Japan and the UK based on Hofstede's cultural dimensions.

Moreover, both Japan and the UK have recently introduced new national cybersecurity strategies that aim to raise public awareness of cyber risks and promote a free, open, peaceful, and secure cyberspace. For instance, Japan's new cybersecurity strategy aims to enhance socio-economic vitality, realize a digital society where people can live with a sense of safety and security, and contribute to the peace and stability of the international community and Japan's national security [78]. The UK's cybersecurity strategy, on the other hand, aims to strengthen the UK cyber ecosystem, build a resilient and prosperous digital UK, take the

lead in the technologies vital to cyber power, advance UK global leadership and influence for a more secure, prosperous and open international order, and deter adversaries to enhance UK security in and through cyberspace [79].

In recent years, both Japan and the UK have developed strategies for enhancing IoT security. Japan has published two sets of guidelines, the "IoT Security Guidelines" [80] and the "IoT Safety/Security Development Guidelines" [81], which recommend security-by-design principles to ensure the security of IoT devices and services. These guidelines are designed to raise awareness among IoT stakeholders, such as manufacturers and service providers, about the importance of security. However, they do not provide clear legal guidance on the responsibilities of stakeholders in the event of a cybersecurity incident. In the UK, the government has taken a different approach. At the end of 2021, the Product Security and Telecommunications Infrastructure (PSTI) Bill was introduced to Parliament, which aims to promote security by design for consumer IoT products and services [82]. The PSTI Bill requires manufacturers, importers, and distributors to comply with new security requirements for IoT devices and creates an enforcement regime with civil and criminal sanctions to prevent insecure products from entering the UK market.

By examining the potential interests of smart-home users in cybersecurity awareness training and behavioral incentives, this study aims to contribute to the development of effective cybersecurity policies and strategies for smart homes. We denote the research questions to be addressed in this chapter as follows:

- Research Question 1: Is there a relationship between adult smart-home users' citizenship and their interest in cybersecurity awareness training?
- Research Question 2: Is there a relationship between adult smart-home users' citizenship and their interest in non-financial rewards?
- Research Question 3: Do Japanese and British adult smart-home users agree that it is imperative to educate children on cybersecurity to ensure that they do not inadvertently endanger the security of smart homes?
- Research Question 4: Do Japanese and British adult smart-home users agree that it is imperative to educate senior citizens on cybersecurity to ensure that they do not inadvertently endanger the security of smart homes?

5.2 Methodology

This section outlines the methodology used in the study. We first describe the survey design, including the sampling strategy and data collection procedure. Then, we present the participant preselection criteria to ensure the validity and reliability of the data. Finally, we explain a detailed description of the statistical analysis techniques used to analyze the collected data.

5.2.1 Survey Design

Our research collected quantitative data using online survey platforms. The survey took approximately 10 minutes to complete. We used a Japanese crowdsourcing platform called CrowdWorks [83] to recruit online participants from Japan. Moreover, we used Prolific [84], a UK-based online crowdsourcing platform, to recruit UK respondents. We paid 1,000 Japanese Yen (about 7 Pounds Sterling) per hour for each participant. This is a standard rate that our institution pays to research participants.

We designed two survey questionnaires to align the survey results when considering the national language of Japan and the UK. We validated the translation correctness in three steps. Firstly, native Japanese speakers translated the questionnaire from English to Japanese. Then, another Japanese speaker who did not have knowledge of the original English questionnaire translated the previously translated questionnaire from Japanese back to English. Lastly, we compared the original English questionnaire with the translated one and found that the questionnaires were identical with the same semantics. Previous research articles [85, 86] used the same approach to verify translation correctness.

We piloted the survey questionnaires with 14 volunteers, six from Japan (50% female, 50% male) and eight from overseas (12.5% female and 87.5% male). We tested and revised the questionnaires accordingly. Our survey collected data using several constructs across the following five categories (see Appendix B):

(1) Demographics were measured using seven constructs (Dem_i, where $i = 1, \ldots, 7$)

(2) Knowledge of smart homes was measured using two constructs (KSH_1 and KSH_2)

(3) Smart-home security was measured using three constructs (SHS_1, SHS_2, and SHS_3)

(4) Cybersecurity awareness training was measured using five constructs (CAT_j, where $j = 1, \ldots, 5$)

(5) Non-financial rewards for good cybersecurity behavior were measured using four constructs (NFR_k, where $k = 1, \ldots, 4$)

On the other hand, we looked at the compliance of the questionnaires with ethical standards and procedures for research with human participants before distributing the survey to the target audience. It is noteworthy that we received our institution's Institutional Review Board (IRB) approval, which demonstrated that our research aligned with regulations and ethics in research studies involving human subjects.

Participants took the survey on a completely voluntary basis. We clarified the purpose of the study and the usage of the participants' responses before they took the survey. Eligibility criteria included being between the ages of 25 and 64 and either Japanese residents of Japan or British residents of the UK. Moreover, we provided informed consent to the participants. The participants who agreed to take the survey were requested to answer questions related to demographic information, knowledge about smart homes and their security, and interests in cybersecurity awareness training and non-financial rewards for good cybersecurity behavior at home.

5.2.2 Preselection Criteria of Participants

We collected 434 responses between June 08 to June 22, 2022, from individuals living in smart homes. To ensure that participants were familiar with IoT devices while accounting for the heterogeneity of smart homes, we only considered those who owned and used at least five IoT devices from at least two device types at home. To ascertain this information, we asked two questions (see Appendix B.2):

Q1. (KSH_1) How many IoT devices do you own?

Q2. (KSH_2) Please select all the types of IoT devices used in your house.

After screening for eligibility, we excluded seven respondents who did not meet the ownership criteria and four who did not disclose essential information, such as their citizenship or education levels. Our final sample size was 423 participants. For the purpose of this study, we use the term "citizenship" to refer to both citizenship and nationality.

5.2.3 Statistical Analysis

We first conducted a descriptive statistical analysis of the collected data to examine the demographics and background of the sample population. We presented the data using tables, summarizing categorical variables with frequencies (%) and numerical variables with measures of central tendency (mean: μ) and dispersion (standard deviation: σ). Afterward, we made predictions about the larger population of smart-home users through the application of inferential statistical methods on the collected data, thus providing a comprehensive understanding of the sample population and its relationship to the population of smart-home users. We performed data analysis using R.

To enhance data analysis, we combined or classified some categories due to limited data. Specifically, we grouped age categories 45-54 and 55-64 into a single category 45-64, and education was categorized into two levels: secondary education (junior and high school) and higher education (bachelor's, master's, and doctorate degrees). We also combined "very insecure" and "insecure" into "insecure". and "very secure" and "secure" into "secure" for the perception of security levels. In terms of employment status, we categorized individuals as "unemployed" if they were not "employed full-time", "self-employed", or "employed part-time". Additionally, the number of IoT devices owned was classified as 5-10 or more than 10, and known cyberattacks were classified into three groups: 0-2, 3-4, and 5-6. These modifications allowed for a more comprehensive and in-depth analysis of our data.

The subsequent section presents the statistics of the variables of interest.

5.3 Results

This section presents the findings of the data analysis. Firstly, we provide a summary of the descriptive statistics, which describe the characteristics of the sample. Secondly, we present the inferential statistics, which allow us to draw conclusions based on the sample data.

5.3.1 Descriptive Statistics

We surveyed 423 participants (52.96% from Japan and 47.04% from the UK), including 224 participants from Japan (46% female, 54% male) and 199 participants from the UK (45.2% female, 54.8% male). The ages of participants ranged from 25 to 64 years old. In the UK, the majority of participants were in the 25-34 age range (35.7%), followed by 33.2% in the 35-44 age range, and 31.2% in the 45-64 age range. In Japan, the majority of participants were in the 35-44 age range (45.1%), followed by 31.7% in the 25-34 age range, and 23.2% in the 45-64 age range.

Table 9 provides more information about our sample. The majority of participants from Japan (70.1%) and the UK (63.3%) had a higher education, while the remaining participants had completed their secondary education. Regarding employment status, the majority of participants from Japan (54%) and the UK (75.9%) were full-time employees, with the remainder being part-time employed, self-employed, or unemployed.

On average, Japanese households had one person under the age of 18 ($\sigma = 1.1$), while British households had an average of 0.9 persons ($\sigma = 1.0$) in this age group. Regarding persons aged 65 and older, Japanese households had an average of 0.4 persons ($\sigma = 0.8$), whereas British households had an average of 0.1 persons ($\sigma = 0.4$).

Most participants from Japan (95.1%) and the UK (73.4%) owned between five to ten IoT devices. On average, Japanese participants owned 5.7 ($\sigma = 1.8$) distinct categories of IoT devices, while British participants owned an average of 5.6 ($\sigma = 1.9$) categories.

The participants in the study had limited experience with cybersecurity, with only a minority of British (29.1%) and Japanese (22.8%) respondents reporting having received formal training or having worked or studied in the field.

Table 9: Descriptive statistics

	Japan		UK	
	Obs	% μ (σ)	Obs	% μ (σ)
Citizenship	224	52.96%	199	47.04%
Age group				
25 - 34	71	31.7%	71	35.7%
35 - 44	101	45.1%	66	33.2%
45 - 64	52	23.2%	62	31.2%
Gender				
Female	103	46%	90	45.2%
Male	121	54%	109	54.8%
Level of education				
Secondary Education	67	29.9%	73	36.7%
Higher Education	157	70.1%	126	63.3%
Employment status				
Unemployed	38	17%	25	12.6%
Employed full-time	121	54%	151	75.9%
Employed part-time	35	15.6%	12	6%
Self-employed	30	13.4%	11	5.5%
Number of household members under 18 years old	224	1 (1.1)	199	0.9 (1.0)
Number of household members aged 65 and older	224	0.4 (0.8)	199	0.1 (0.4)
Number of IoT devices owned				
5-10	213	95.1%	146	73.4%
More than 10	11	4.9%	53	26.6%
Number of distinct categories of IoT devices owned	224	5.7 (1.8)	199	5.6 (1.9)
Cybersecurity experience				
No	173	77.2%	141	70.9%
Yes	51	22.8%	58	29.1%
Number of known cyberattacks				
0 - 2	102	45.5%	43	21.6%
3 - 4	100	44.6%	105	52.8%
5 - 6	22	9.8%	51	25.6%
Perception of the security level of your smart home				
I don't know / Unsure	129	57.6%	87	43.7%
Insecure	50	22.3%	23	11.6%
Secure	45	20.1%	89	44.7%

When asked about their knowledge of different types of cyberattacks, 78.4% of British participants were able to recognize at least three out of the six common attack types presented, while 54.4% of Japanese participants had a similar level of knowledge.

Furthermore, the results showed that only 20.1% of Japanese participants

perceived their smart home as secure, compared to 44.7% of British participants. These findings suggest that there may be cultural differences in smart-home users' attitudes toward cybersecurity.

5.3.2 Inferential Statistics

This section analyzes the regression results obtained from the dependent variables aligned with our research questions. To visually showcase the findings, we provide a graphical comparison of the responses from Japan and the UK. Afterward, we present the results of logit models, along with their respective regression coefficients. Finally, we analyze and interpret the marginal effects.

SHUs' Interest in Cybersecurity Awareness Training

We analyze SHUs' interest in cybersecurity awareness training (CAT) using three dependent variables: need of CAT (CAT_1), willingness to spend money on CAT (CAT_2), and willingness to spend time on CAT (CAT_3).

Figures 15, 16, and 17 show that a majority of British and Japanese respondents recognized the importance of cybersecurity awareness training to secure smart homes, with 75.17% expressing agreement or strong agreement. However, despite this recognition, 62.6% were not willing to invest money in such training. Conversely, 80.6% of respondents agreed that spending time on cybersecurity awareness training is a worthwhile endeavor.

Table 10 summarizes the results of the logit and ordered logit models on British and Japanese respondents. The analysis shows that the variable *citizenship* significantly impacted the perceived need for cybersecurity awareness training for smart-home security ($p < 0.01$, column 2), willingness to spend money on training ($p < 0.01$, column 3), and willingness to allocate time for training ($p < 0.05$, column 4).

Table 11 summarizes the marginal effects resulting from the ordered logit regression analysis, which were estimated for the independent variable *citizenship*. The comparison between British and Japanese respondents revealed differences in their perceptions regarding the importance of cybersecurity awareness training for securing smart homes. Japanese respondents demonstrated a 0.8% decrease

Table 10: Regression Results of the Logit and Ordered Logit Models

	Dependent variables							
	CAT_1	CAT_2	CAT_3	CAT_4	CAT_5	NFR_1	NFR_2	NFR_3
	Ordered Logit	Logit	Logit	Ordered Logit	Ordered Logit	Ordered Logit	Ordered Logit	Ordered Logit
Citizenship (Japanese)	0.953***	1.287***	−0.717**	−0.899***	−1.219***	−0.955***	0.588***	1.050***
	(0.243)	(0.268)	(0.325)	(0.228)	(0.229)	(0.221)	(0.204)	(0.205)
Age (25 - 34)	0.141	0.516*	0.343	0.221	0.750***	0.190	0.127	−0.057
	(0.265)	(0.295)	(0.353)	(0.257)	(0.254)	(0.253)	(0.232)	(0.234)
Age (35 - 44)	0.133	0.250	0.349	0.418*	0.610**	−0.221	−0.030	−0.043
	(0.255)	(0.281)	(0.331)	(0.250)	(0.243)	(0.245)	(0.223)	(0.221)
Gender (Male)	−0.310	−0.005	−0.086	−0.390*	−0.309	0.174	0.053	0.288
	(0.220)	(0.234)	(0.289)	(0.210)	(0.207)	(0.206)	(0.190)	(0.190)
Level of education (Higher Education)	−0.082	−0.045	0.152	−0.231	−0.230	−0.047	−0.209	−0.101
	(0.220)	(0.240)	(0.285)	(0.214)	(0.211)	(0.212)	(0.196)	(0.197)
Employment status (Employed full-time)	0.426	1.162***	0.335	0.281	0.170	0.061	0.369	0.238
	(0.292)	(0.367)	(0.379)	(0.285)	(0.286)	(0.288)	(0.256)	(0.262)
Employment status (Employed part-time)	−0.138	0.743	−0.260	0.330	−0.554	−0.040	−0.094	0.409
	(0.389)	(0.457)	(0.470)	(0.385)	(0.387)	(0.385)	(0.346)	(0.350)
Employment status (Self-employed)	−0.114	0.945*	−0.414	0.018	0.146	−0.454	−0.267	−0.398
	(0.404)	(0.483)	(0.480)	(0.392)	(0.394)	(0.398)	(0.366)	(0.351)
Number of household members under the age of 18	−0.087	0.041	0.090	0.081	0.070			
	(0.097)	(0.103)	(0.130)	(0.095)	(0.092)			
Number of household members over the age of 65	−0.046	0.073	−0.255	0.093	0.280*			
	(0.169)	(0.177)	(0.200)	(0.166)	(0.163)			
Number of IoT devices owned (More than 10)	0.487	0.225	−0.389	0.386	0.424	0.248	0.942***	0.123
	(0.317)	(0.329)	(0.435)	(0.291)	(0.297)	(0.292)	(0.281)	(0.277)
Cybersecurity experience (Yes)	0.356	0.087	0.208	0.315	0.329	0.044	0.288	0.073
	(0.249)	(0.259)	(0.353)	(0.234)	(0.234)	(0.224)	(0.211)	(0.208)
Number of known cyberattacks (3 - 4)	0.587**	0.654**	0.845***					
	(0.233)	(0.254)	(0.291)					
Number of known cyberattacks (5 - 6)	0.166	0.436	0.881*					
	(0.337)	(0.366)	(0.473)					
Perception of the security level of your smart home (Insecure)	0.835***	0.465	0.735*	0.680**	0.230	0.040	0.191	0.375
	(0.291)	(0.297)	(0.390)	(0.277)	(0.268)	(0.267)	(0.247)	(0.248)
Perception of the security level of your smart home (Secure)	0.047	0.479*	0.490	0.081	0.282	0.642***	0.606***	0.595***
	(0.238)	(0.261)	(0.328)	(0.229)	(0.227)	(0.234)	(0.211)	(0.211)
Constant		−3.179***	0.701					
		(0.528)	(0.503)					
Observations	423	423	423	423	423	423	423	423

***p<0.01; **p<0.05; *p<0.1

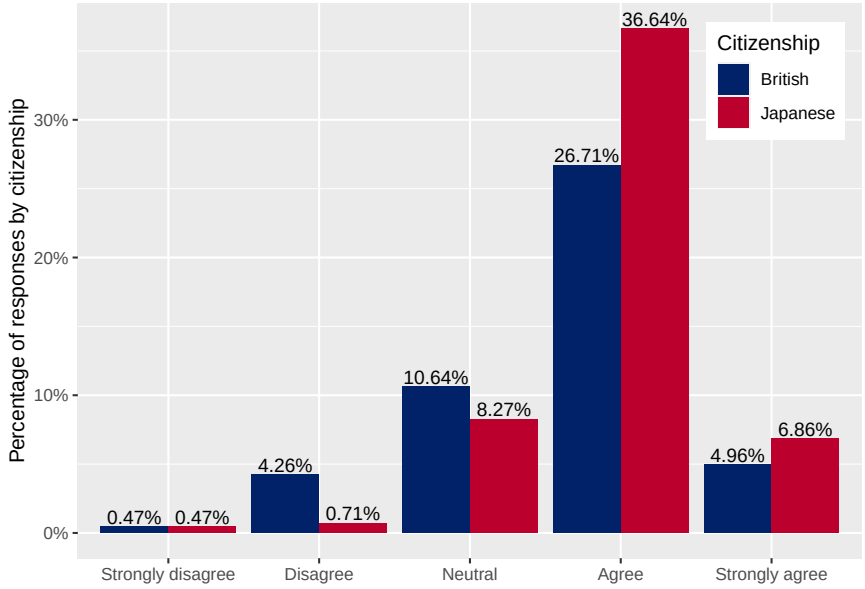


Figure 15: Agreement on the necessity of cybersecurity awareness training for securing smart homes effectively.

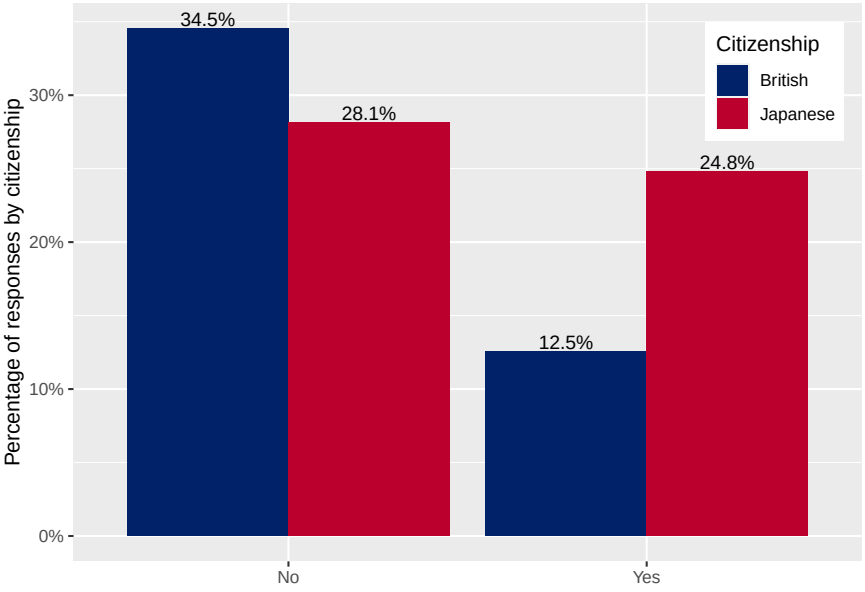


Figure 16: Willingness to spend money on cybersecurity awareness training.

in the likelihood of expressing a strong disagreement, a 4% decrease in the likelihood of expressing disagreement, a 12.3% decrease in the likelihood of holding a

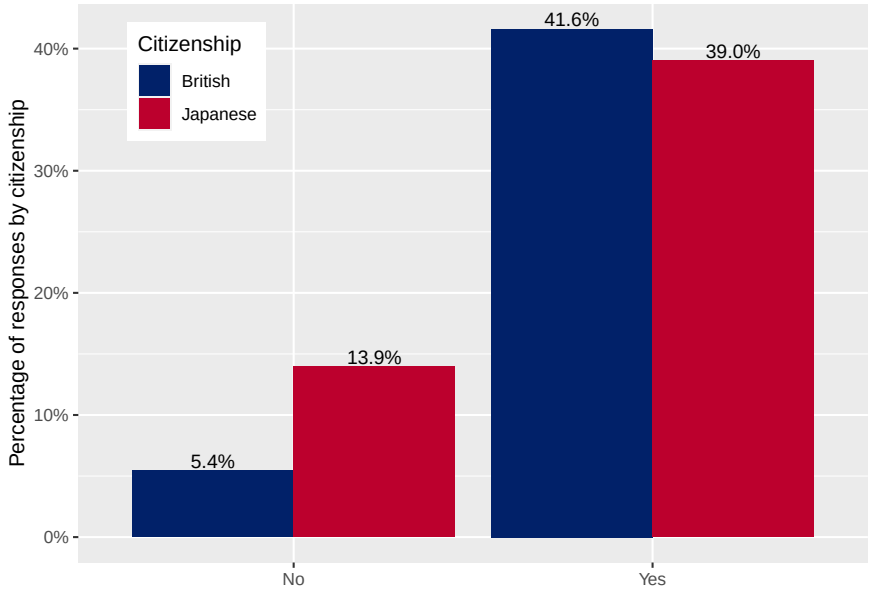


Figure 17: Willingness to spend time on cybersecurity awareness training.

Table 11: Marginal Effects of Citizenship for Ordered Logit Models CAT_1, CAT_4, CAT_5, NFR_1, NFR_2, and NFR_3

	Dependent variables	Strongly disagree (Very dissatisfied) (Not at all)	Disagree (Dissatisfied) (Slightly)	Neutral (I don't know/ Unsure) (Moderately)	Agree (Satisfied) (Very)	Strongly agree (Very satisfied) (Extremely)
Citizenship (Japanese)	CAT_1	-0.008*	-0.040***	-0.123***	0.083***	0.088***
	CAT_4	0.002	0.007*	0.077***	0.116***	-0.201***
	CAT_5	0.004	0.034***	0.109***	0.111***	-0.259***
	NFR_1		0.024***	0.192***	-0.141***	-0.075***
	NFR_2	-0.122***	-0.024**	0.070***	0.054***	0.022**
	NFR_3	-0.183***	-0.072***	0.059***	0.124***	0.072***

*** p <0.01; ** p <0.05; * p <0.1

neutral stance, an 8.3% increase in the likelihood of expressing agreement, and an 8.8% increase in the likelihood of expressing strong agreement when compared to British respondents. These findings suggest that Japanese respondents generally recognized the significance of cybersecurity awareness training more than British respondents.

Table 12 presents the marginal effects resulting from the logit regression analysis. The analysis compared the spending behavior of British and Japanese respondents regarding cybersecurity awareness training. The findings showed that, in

comparison to British respondents, Japanese respondents were 26.8% more likely to allocate financial resources toward cybersecurity awareness training. Conversely, Japanese respondents were 9.8% less likely to allocate time toward cybersecurity awareness training compared to British respondents. These results highlight the disparities in the resource allocation patterns between Japanese and British respondents in regard to cybersecurity awareness training.

Cybersecurity Awareness Training for Children

Our analysis of SHUs' opinions on the significance of cybersecurity awareness training for children, using the construct CAT_4, revealed noteworthy results.

As shown in Table 10, the independent variable *citizenship* has a statistically significant impact on SHUs' opinions regarding the importance of cybersecurity awareness training for children in maintaining the security of smart homes ($p < 0.01$).

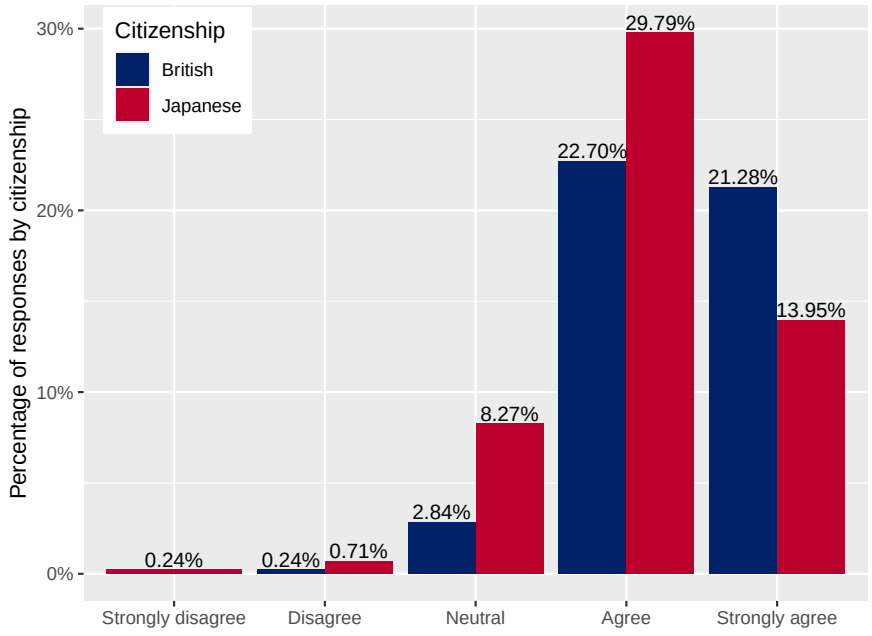


Figure 18: Cybersecurity awareness training for children.

The findings are further visualized in Figure 18, which highlights that a significant majority of British and Japanese respondents concurred that educating

children on cybersecurity is critical for ensuring the security of smart homes, with 87.72% indicating agreement or strong agreement.

On the other hand, Table 11 indicates that Japanese respondents had a slightly different attitude towards the issue compared to British respondents. They were 0.2% more likely to express strong disagreement, 0.7% more likely to express disagreement, 7.7% more likely to express a neutral stance, 11.6% more likely to express agreement, and 20.1% less likely to express strong agreement.

Cybersecurity Awareness Training for Senior Citizens

The analysis of SHUs' opinions regarding the importance of cybersecurity awareness training for senior citizens, using the construct CAT_5, revealed meaningful insights.

As presented in Table 10, our findings indicated that the independent variable *citizenship* has a statistically significant effect on SHUs' views about the significance of cybersecurity awareness training for senior citizens in securing smart homes ($p < 0.01$).

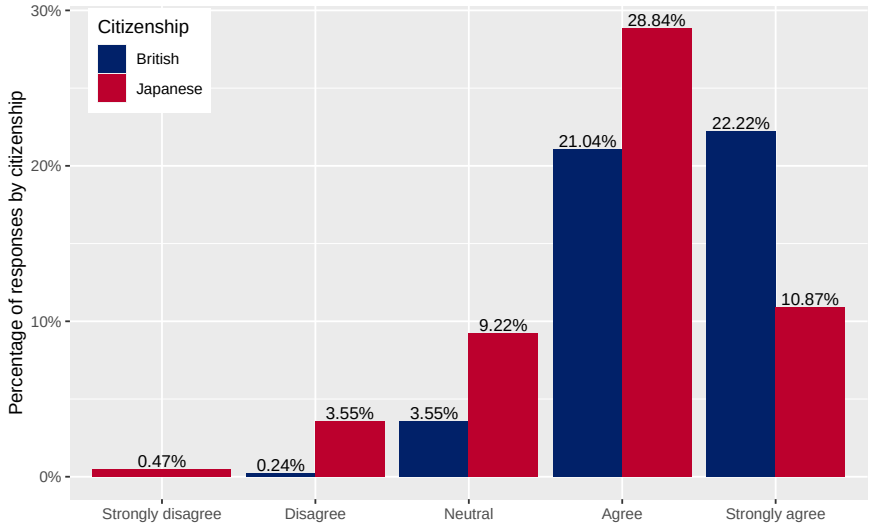


Figure 19: Cybersecurity awareness training for senior citizens.

In addition, Figure 19 shows that a substantial proportion of British and Japanese respondents considered that educating senior citizens on cybersecurity

is crucial for ensuring the security of smart homes, with 82.97% of respondents indicating agreement or strong agreement.

However, Table 11 reveals that compared to British respondents, Japanese respondents showed a slightly different attitude towards the issue. They were 0.4% more likely to express strong disagreement, 3.4% more likely to express disagreement, 10.9% more likely to hold a neutral stance, 11.1% more likely to express agreement, and 25.9% less likely to express strong agreement.

SHUs' Interest in Non-Financial Rewards for Promoting Cybersecurity Behavior

The analysis showed that the independent variable *citizenship* had a statistically significant impact on SHUs' satisfaction with non-financial rewards for good cybersecurity behavior in smart homes. Specifically, the significance level was $p < 0.01$ for the constructs NFR_1, NFR_2, and NFR_3, as shown in Table 10.

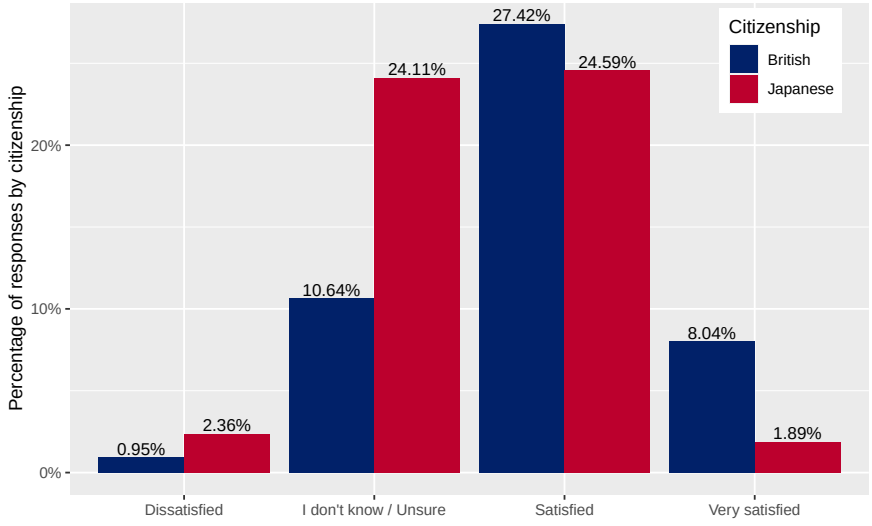


Figure 20: Level of satisfaction with non-financial rewards for promoting cybersecurity hygiene at home.

Figure 20 provides additional insights into participants' attitudes towards non-financial rewards. Most respondents, 61.94%, reported feeling satisfied or very satisfied with these types of rewards. Meanwhile, 34.75% of respondents were

Table 12: Marginal Effects of Logit Models CAT_2 and CAT_3

	Dependent variables	
	CAT_2	CAT_3
Citizenship (Japanese)	0.268 ***	-0.098 **
	(0.050)	(0.043)
Age (25 - 34)	0.107 *	0.050
	(0.060)	(0.051)
Age (35 - 44)	0.051	0.050
	(0.056)	(0.049)
Gender (Male)	-0.001	-0.012
	(0.049)	(0.040)
Level of education (Higher education)	-0.009	0.021
	(0.050)	(0.041)
Employment status (Employed full-time)	0.221 ***	0.046
	(0.059)	(0.055)
Employment status (Employed part-time)	0.132	-0.042
	(0.082)	(0.076)
Employment status (Self-employed)	0.174 *	-0.069
	(0.090)	(0.081)
Number of household members under the age of 18	0.008	0.013
	(0.022)	(0.018)
Number of household members over the age of 65	0.015	-0.036
	(0.037)	(0.028)
Number of IoT devices owned (More than 10)	0.047	-0.058
	(0.070)	(0.069)
Cybersecurity experience (Yes)	0.018	0.028
	(0.055)	(0.046)
Number of known cyberattacks (3 - 4)	0.134 ***	0.127 ***
	(0.050)	(0.045)
Number of known cyberattacks (5 - 6)	0.087	0.131 **
	(0.074)	(0.063)
Perception of the security level of your smart home (Insecure)	0.097	0.098 **
	(0.063)	(0.046)
Perception of the security level of your smart home (Secure)	0.100 *	0.069
	(0.054)	(0.044)
Observations	423	423

*** p <0.01; ** p <0.05; * p <0.1

unsure about their feelings towards non-financial rewards, and 3.31% reported feeling dissatisfied.

As presented in Table 11, Japanese respondents had a 2.4% higher probability of being dissatisfied, a 19.2% higher probability of holding a neutral stance, a 14.1% lower probability of being satisfied, and a 7.5% lower probability of being very satisfied with non-financial rewards for cybersecurity behavior in smart homes compared to British respondents.

The investigation of non-financial rewards, such as awards and virtual reality (VR) services, revealed notable findings. Japanese respondents demonstrated a higher level of interest in the "Certificate of Achievement for Good Cybersecurity Behavior at Home" than British respondents, with decreases of 12.2% and 2.4% in the "not at all interested" and "slightly interested" categories, respectively, and increases of 7%, 5.4%, and 2.2% in the "moderately interested", "very interested", and "extremely interested" categories, highlighting the cultural differences in the perceived value of this specific reward.

In addition, Japanese respondents showed a higher level of interest in having virtual reality services in smart homes as a non-financial reward, with a lower percentage of being categorized as "not at all interested" or "slightly interested", and a higher percentage of being categorized as "moderately interested", "very interested", or "extremely interested", as compared to British respondents. Specifically, Japanese respondents displayed a decrease of 18.3% for the "not at all interested" category, 7.2% for the "slightly interested" category, and an increase of 5.9% for the "moderately interested" category, 12.4% for the "very interested" category, and 7.2% for the "extremely interested" category, as compared to British respondents.

Figure 21 presents the results of our survey regarding the most desirable non-financial rewards. The two most popular rewards were "cyber insurance discounts" (31.44%) and "virtual point rewards" (26.24%). Interestingly, there were some differences in preferences between British and Japanese respondents. British respondents showed a greater interest in "cyber insurance discounts" as a reward (16.31%), while Japanese respondents were more interested in "virtual point rewards" (21.04%).

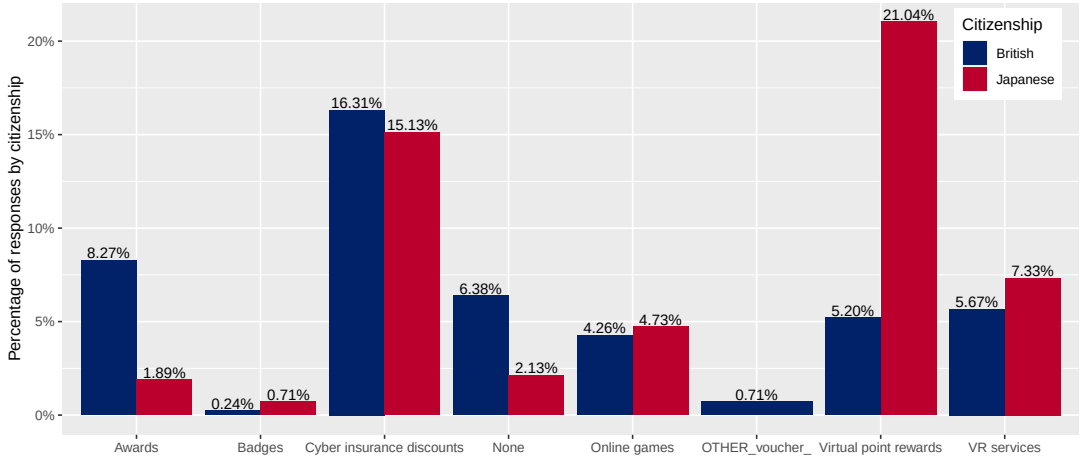


Figure 21: Non-financial rewards for secure behavior in smart homes.

5.4 Discussion

Our study investigated whether adult smart-home users had an interest in cybersecurity awareness training and non-financial rewards for good cybersecurity behaviors. To achieve our objective, we developed research questions centered around citizenship, interests in cybersecurity awareness training, interests in non-financial rewards, and opinions regarding educating children and senior citizens on cybersecurity. Our analysis indicates that national cultures play a significant role in shaping the interests of adult smart-home users in cybersecurity awareness training and their perceptions of its significance for children and senior citizens. Furthermore, our findings unveil that national cultural differences influence the interest of smart-home users in non-financial rewards.

The following sections provide a detailed analysis of the results obtained from the study. We begin by discussing the significant findings and their implications. In addition, we identify the limitations of our study and suggest avenues for future work.

5.4.1 Users' Cybersecurity Awareness for Smart-Home Security

This section discusses the results of the study related to cybersecurity awareness training for adults, including their interests and opinions regarding children and senior citizens.

Adult SHUs' Interest in Cybersecurity Awareness Training

Our results suggest that there is a significant correlation between citizenship and interest in cybersecurity awareness training. Specifically, Japanese respondents are more likely than British respondents to recognize the importance of cybersecurity education and allocate money toward it. However, they are less likely to allocate time for cybersecurity awareness training.

The data analysis indicates that while most Japanese and British respondents expressed interest in cybersecurity awareness training, there were differences in the level of interest between the two groups. These findings are consistent with previous studies that have emphasized the importance of cultural differences in shaping users' cybersecurity attitudes [43, 44]. The present study contributes to the growing body of evidence supporting the idea that cultural disparities exert a significant influence on adult smart-home users' engagement with cybersecurity awareness training. Hofstede's cultural dimensions suggest that Japanese prioritize collectivism, while British people focus on individualism. These cultural differences may have influenced the perceived importance of cybersecurity awareness training for each group of respondents. It is plausible that Japanese respondents were more likely to acknowledge the importance of cybersecurity awareness training due to their cultural attitudes towards safety and security, which emphasize collective responsibility. In contrast, British respondents may be less interested in cybersecurity awareness training due to their individualistic cultural attitudes. Furthermore, the higher level of perceived insecurity among Japanese respondents regarding the security of their smart homes compared to British respondents could also explain the difference in interest levels.

The findings indicate that there were significant differences in the willingness of Japanese and British respondents to allocate money toward cybersecurity awareness training, which could be influenced by socio-economic and cultural factors. While both groups demonstrated limited willingness to invest money in training, the extent of their allocation varied. Prior research has shown that Japan has lower income inequality and higher social well-being than the UK [77, 76]. These factors could impact the resources that individuals are willing or able to allocate toward cybersecurity awareness training. Furthermore, Japanese respondents may be more likely to prioritize spending on cybersecurity education

due to cultural values of collective responsibility and a stronger social safety net. Conversely, British respondents may have less disposable income and less motivation to spend money on cybersecurity education due to higher income inequality.

The data reveals that British respondents were more willing to allocate time to cybersecurity awareness training compared to their Japanese counterparts. Nonetheless, it is worth noting that both groups demonstrated a willingness to invest some time in training. The disparity could be attributed to Hofstede's cultural dimensions theory, which suggests that Japanese people tend to experience more stress and uncertainty about the future than the British due to their higher level of uncertainty avoidance. Consequently, Japanese people may exhibit a greater reluctance to invest time in training that is not directly related to their primary occupation. Our findings are consistent with previous research highlighting the importance of considering both time and monetary costs when designing effective education programs for household security [70].

Cybersecurity Awareness Training for Children

The findings indicate that the majority of adults surveyed believe that providing education on cybersecurity to children is crucial for smart-home security. This result aligns with the previous research of Ahmad et al. [28], who identified a lack of parental awareness regarding their children's online activities. Providing children with cybersecurity awareness training could address the issue of parental unawareness, as it would help children understand the risks posed by cyber threats and learn how to behave safely on the Internet.

In addition, our study shows a significant relationship between the citizenship of adult smart-home users and their attitudes towards the importance of cybersecurity awareness training for children in maintaining the security of smart homes. Specifically, the results indicate that cultural differences between Japan and the UK influence adults' appreciation of children's training toward safe online activities in smart homes. Our findings differ from those of Sun et al. [33], who investigated smart-home users from two countries with similar cultural backgrounds according to Hofstede's cultural dimensions.

Cybersecurity Awareness Training for Senior Citizens

The findings of our study indicate that both Japanese and British participants share a common belief in the importance of cybersecurity awareness training for senior citizens to protect themselves against cyber threats. These results are consistent with prior research conducted by Blackwood-Brown, Levy, and D'Arcy [31], who have also shown that cybersecurity awareness training can empower senior citizens to defend against cyberattacks proactively.

However, our analysis shows a significant correlation between the nationality of adult smart-home users and their perception of the importance of cybersecurity awareness training for senior citizens to secure smart homes. This result suggests that cultural differences between the two groups could influence their overall attitudes towards this issue, with Japanese participants less inclined than their British counterparts.

A potential reason for this gap in perception could be that British participants may possess a more comprehensive knowledge of the different types of cyber threats than their Japanese counterparts. The lack of awareness of cyber threats may make the Japanese less concerned about the dangers that older adults face from cyberattacks. This emphasizes the importance of increasing awareness about cyber threats in Japan, particularly among senior citizens, to ensure that they can effectively protect themselves and their smart homes from potential cyber threats.

5.4.2 Non-Financial Reward for Cybersecurity

The findings of our study contribute to understanding the impact of national cultures on smart-home users' interests in non-financial rewards. The results confirm that cultural disparities have a significant influence on the inclination of smart-home users towards non-financial rewards as a means of incentivizing secure behavior. This outcome is in line with the work of Ndibwile et al. [45], who found significant differences in security perception between smartphone users from Japan and Tanzania, two countries with different cultural backgrounds based on Hofstede's cultural dimensions.

The findings indicate that cyber insurance discounts and virtual point rewards are the most significant non-financial rewards for participants. Notably, there

were differences in preference between British and Japanese participants, with the former showing a greater interest in cyber insurance discounts and the latter in virtual point rewards.

It is important to highlight that insurance solutions for cyber risks have been prevalent in the UK, especially within the corporate sector. Therefore, the inclination of British SHUs towards cyber insurance discounts in our study could be related to the fact that most participants were employees. Extending cyber insurance initiatives to smart-home users is recommended to promote a safe and secure smart environment and cyberspace.

On the other hand, the preference of Japanese participants for virtual points is not arbitrary. Instead, it reflects the common practice in Japan of earning points for purchases, which can be redeemed for future transactions. Moreover, the Japanese government has promoted cashless payment services based on point reward systems, which further strengthens this trend. For instance, the government launched the ongoing "MyNa Points" initiative, also known as the Individual Number Card Points initiative, in 2020. The widespread adoption of these reward systems in Japan underscores the importance of cultural norms in implementing incentive programs.

The primary interests of participants revolve around cyber insurance discounts and virtual point rewards, as opposed to alternatives such as awards, badges, or VR services. These preferences align with the findings of Rehnen et al. [22], who found that monetary incentives tend to be more effective in promoting user engagement. They compared the effects of direct non-monetary rewards (e.g., product/free service) and indirect monetary rewards (e.g., loyalty points) on users' engagement behaviors. This study substantiates the heightened interest in indirect monetary incentives that participants demonstrated in our research.

Finally, our study results align with the work of Argyris et al. [46], who underscored the significance of tailoring picture passwords to accommodate cultural differences. Likewise, our results emphasize the importance of customizing non-financial rewards according to users' cultural backgrounds to increase their effectiveness in encouraging good cybersecurity practices in smart homes.

5.4.3 Implications

Our study highlights the importance of cultural factors in shaping adult smart-home users' attitudes toward cybersecurity awareness training. It is essential to design training programs that are tailored to the target audience's cultural and socio-economic backgrounds.

Moreover, cost and time constraints must be considered when designing effective cybersecurity awareness training programs. Our study also emphasizes the need for training programs that address the unique cybersecurity challenges faced by children and senior citizens in smart-home environments. By providing smart-home users with the appropriate knowledge and competencies, it is possible to prevent human errors and foster secure and safe smart homes.

In addition, governments should support training programs by offering non-financial incentives. This study emphasizes the importance of developing and providing cyber insurance solutions and virtual rewards tailored to the distinct needs of smart-home users in the UK and Japan, respectively.

Finally, our study highlights the necessity for further research to enhance our understanding of how cultural differences influence users' attitudes towards cybersecurity. Furthermore, future studies should concentrate on implementing and assessing the effectiveness of non-financial rewards in fostering good cybersecurity practices in smart homes.

5.4.4 Limitations and Recommendations

It is important to recognize the limitations of this study. Firstly, while our research findings provide insights into the relationship between adult smart-home users' citizenship and their perceptions of the importance of cybersecurity awareness training and non-financial rewards, the underlying reasons that explain our results were not investigated in detail. Although our study provides some possible motivations, future research should focus on building and evaluating constructs that could provide a more detailed explanation of our findings.

Secondly, our study has limitations related to the profile of participants. Specifically, we were unable to verify whether participants possessed and used IoT devices in their homes. Additionally, the criteria used to define "smart-home users" in our study may be questionable because the exact number and types of

IoT devices required to qualify a house as a "smart home" are currently unknown. Therefore, future studies may need to refine the definition of "smart-home users" to ensure the high quality of data collected.

Finally, our study is limited to participants from only two countries and cultures. Investigating a more diverse range of cultures could provide valuable insights into the relevance and applicability of our study findings.

5.5 Summary

In Chapter 5, we investigated the potential interests of adult smart-home users in cybersecurity awareness training and non-financial rewards that may encourage them to adopt sound cybersecurity practices. We surveyed 423 British and Japanese individuals between the ages of 25 and 64 living in smart homes. The results showed that while most participants recognized the importance of cybersecurity education and considered spending time on cybersecurity awareness training worthwhile, they were not willing to pay for such training. Additionally, participants agreed that educating children and senior citizens on cybersecurity was crucial for protecting smart homes. We also found that non-financial incentives for good cybersecurity practices in smart homes would satisfy most participants. British participants were particularly interested in cyber insurance discounts, while Japanese participants showed greater interest in virtual point rewards. The findings of this study indicated noteworthy cultural differences between British and Japanese attitudes toward cybersecurity awareness training and non-financial incentives for securing smart homes.

6. Discussion

In this section, we discuss essential aspects of the research, providing an additional layer of insight that complements the discussions in Sections 3.5, 4.5, and 5.4.

Addressing the challenge of instilling cybersecurity best practices among smart-home users requires an understanding of the interplay between the costs and benefits of cybersecurity awareness training, along with individual motivations. Our research, which does not presuppose the existence of free online cybersecurity training, underscores the significance of motivating smart-home users to willingly invest in cybersecurity awareness training to protect their homes and families from potential cyberattacks. Furthermore, our study sheds light on a distinct interest in non-financial rewards to cultivate a strong culture of cybersecurity practices within smart homes, especially among British and Japanese smart-home users.

In the context of existing global initiatives, commendable efforts have been made to provide free cybersecurity awareness training on a worldwide scale. The Cybersecurity Learning Hub [87], initiated by the World Economic Forum, and the Cyber Aces program [88] by the SANS Institute exemplify this progress. Additionally, various government agencies offer free online resources for cybersecurity training, enhancing online safety for individuals and organizations. However, the effectiveness of these initiatives hinges on the level of engagement they manage to achieve. It is necessary for public and private initiatives to focus not only on resource availability but also on customizing trainings for specific targets, effective promotion, and thorough evaluation of these trainings to maximize its impact.

Moreover, it is imperative to underscore the importance of risk communication strategies for different demographics in order to build a more resilient society. Factors like age groups, gender identities, employment statuses, location, and others can all shape perceptions of cybersecurity risks and willingness to engage in cybersecurity practices. Tailoring risk communication to each group's unique perspective can bridge awareness gaps and foster an inclusive and effective culture of cybersecurity within smart homes.

Furthermore, advocating for enhanced IoT cybersecurity regulations emerges as a critical step toward securing smart homes. For instance, the EU Cyber Resilience Act (CRA)[89] introduces a framework aimed at enforcing security-

by-design principles and cybersecurity requirements for products incorporating digital elements. These regulations have the potential to reduce the necessity for smart-home users to proactively contemplate the security aspects of IoT devices and applications. Moreover, they can alleviate the need for in-depth cybersecurity awareness training among smart-home users. Nevertheless, a significant challenge persists: the establishment of robust trust mechanisms to encourage users to fully embrace these regulations. For example, if regulatory authorities recommend purchasing only certified IoT devices, individuals should exclusively consider acquiring those IoT devices endorsed as secure by trusted parties. This approach would not only promote adherence to the regulations but also foster a heightened level of confidence in the reliability and security of the certified devices.

The culmination of our research underscores the paramount importance of fostering collaboration between public and private entities to improve the communication of cybersecurity risks and initiatives to the broader public. In an era where the concept of home has transcended its traditional boundaries due to the pervasive influence of the IoT, the vulnerability of home users to cyberattacks has risen exponentially. Our increasingly interconnected digital world necessitates a reevaluation of security paradigms. Specifically, as smart homes and their users become prime targets for malicious actors, we advocate for the compelling integration of cybersecurity awareness training and non-financial incentives within regulatory frameworks governing smart-home security. This proactive approach can cultivate a culture of cybersecurity hygiene in smart homes, thereby enhancing users' sense of safety and security and safeguarding their well-being.

7. Future Directions

This section outlines several future directions to investigate human-centered cybersecurity strategies and behavioral incentives for securing smart homes.

7.1 Simulation-Based Models

Developing more realistic models using agent-based simulations presents a promising direction for future research. By incorporating stochastic and conditional strategies into these models, we can capture the complexities of user decision-making and behavior in the context of cybersecurity. Simulation-based models will enable us to gain deeper insights into the effectiveness of various cybersecurity interventions and refine existing theoretical frameworks.

7.2 Exploring Punishments and Rewards

To promote good cybersecurity practices among smart-home users, it can beneficial to investigate the effects of both punishments and rewards on users' security behaviors. Future research should also delve into the influence of different incentives, including financial and non-financial rewards, on users' intentions to adopt cybersecurity best practices. Exploring the avenue of designing a practical framework that incentivizes smart-home users to enhance their cybersecurity attitude holds promise.

7.3 Cultural Factors and Personalized Solutions

Future studies should focus on human-centered cybersecurity initiatives. Understanding the cultural factors influencing smart-home users' inclination toward cybersecurity services is a crucial area to consider. Examining cultural norms, values, and beliefs can help develop personalized solutions and interventions that effectively encourage good cybersecurity practices in smart homes. These culturally tailored approaches will contribute to increased adoption of cybersecurity measures among diverse user groups.

7.4 Long-Term Sustainability of Cybersecurity Education

Future studies should focus on the sustainability of training programs for smart-home users to ensure the long-term effectiveness of cybersecurity education. Central to this endeavor is recognizing the dynamic nature of cyber threats, which necessitates continuous updates to training programs. A pivotal aspiration revolves around developing cost-effective and time-efficient cybersecurity training programs that not only bolster widespread adherence to cybersecurity best practices but also seamlessly integrate into users' routines. An intriguing avenue to explore involves the integration of VR services. This innovative proposition envisions users seeking cybersecurity advice and recommendations through immersive VR experiences, thereby fostering a more personalized and engaging learning journey.

7.5 Quantifying the Financial Impact of Cyberattacks

One important avenue for future research is to conduct a comprehensive analysis that quantifies the financial implications of cyberattacks on smart homes. This study should aim to develop a framework that assesses the costs of cyberattacks related to smart-home assets and compares them with the return on investment of cybersecurity measures. Such an analysis will assist smart-home users in making informed decisions regarding resource allocation, enabling them to prioritize investments and ensure the cost-effectiveness of their cybersecurity efforts.

7.6 AI-Assisted Network and Device Management

Leveraging recent advancements in artificial intelligence, such as Language Model-based Artificial Intelligence (AI) systems, provides an opportunity to facilitate network, device, and security management for smart-home users. Future research should explore the potential of AI-driven tools or virtual assistants that provide personalized recommendations, automate security configurations, and simplify security management processes. The integration of AI technology into smart homes presents a range of benefits, including enhanced user experiences, proactive monitoring of networks and devices, and user-friendly management of security and privacy.

7.7 Friendly Security Dashboard

Developing a user-friendly dashboard that provides an intuitive and comprehensive overview of IoT device and network security in a smart home is another important future direction. This dashboard should present information in a clear and accessible manner, allowing users to monitor the security status of their smart homes at a glance. Providing actionable insights through the dashboard would empower users to make informed decisions regarding their smart-home security.

7.8 Collaborative Framework for Security Implementation

Future research should give priority to the development of a collaborative framework that effectively engages smart-home users and stakeholders in the implementation of security measures within smart homes. This framework should encourage active participation, knowledge sharing, and coordination among smart-home users, IoT device manufacturers, security experts, policymakers, and service providers. Cultivating a shared ethos of mutual assistance and promoting this collaborative framework can enhance awareness, adoption, and implementation of cybersecurity measures. This will lead to heightened effectiveness and success of cybersecurity initiatives in smart homes.

8. Conclusions

In this thesis, we explored cybersecurity investment strategies and non-financial incentives for smart-home users to mitigate cyberattacks. Through a combination of theoretical analysis and empirical research, we obtained valuable insights into the costs, benefits, and implications of cybersecurity practices in the context of smart homes.

From our theoretical analysis, we found that investing in cybersecurity education is advantageous for smart-home users if they receive substantial rewards and the smart home provides them with original value and essential comfort. By using classical game theory, we identified conditions for achieving pure and mixed Nash equilibria in the interactions between attackers and smart-home users. Furthermore, our study using an evolutionary game-theoretic approach revealed that the optimal strategy for smart-home users involves both users and stakeholders investing in cybersecurity, discouraging attackers from continuing their attack efforts. However, it is crucial to ensure that the costs of cybersecurity training are low and affordable, accompanied by non-financial rewards to sustain users' interest and long-term investment.

Our empirical investigation focused on adult smart-home users and their attitudes towards cybersecurity awareness training. We found that participants recognized the importance of cybersecurity education and believed it was worthwhile, but they were not willing to pay for such training. We also identified that educating children and senior citizens on cybersecurity was considered essential for protecting smart homes. In addition, cultural differences between British and Japanese participants were observed, with British participants showing interest in cyber insurance discounts and Japanese participants preferring virtual point rewards as non-financial incentives.

The theoretical and practical implications of our research are significant. We found that investing in cybersecurity education and recognizing non-financial incentives are essential to promote responsible cybersecurity behaviors among smart-home users. The findings also emphasized the need to consider cultural factors when designing training programs and non-financial incentives. Governments should support training initiatives by offering tailored cyber insurance solutions and virtual rewards to enhance users' engagement.

However, our investigation has some limitations. In theoretical modeling, we focus solely on individual cybersecurity decisions, omitting smart-home features (e.g., IoT devices, network configurations, and mobile applications) as well as some smart-home stakeholders (e.g., cyber insurance companies and regulatory authorities). Empirically, the study's confined scope to UK and Japan participants restricts generalizability, while survey-based quantitative data may involve response bias.

To address these limitations, future research should explore more sophisticated game models encompassing various smart home aspects and involving diverse stakeholders. Validating the models with real-world observations would enhance the applicability of the findings. Cross-cultural studies should encompass more countries and investigate the minimum level of non-financial incentives required to motivate smart-home users. Employing mixed methods, such as combining quantitative surveys with interviews, would enhance the quality of participant responses and yield more significant findings.

In conclusion, our research sheds light on the importance of human-centric approaches through cybersecurity investment and non-financial incentives for smart-home users to address the cybersecurity challenges in smart homes. Using theoretical and empirical approaches, we have provided valuable insights into the costs and benefits of cybersecurity investment from the perspectives of smart-home users. The findings and recommendations presented in this thesis lay the foundation for further research, industry initiatives, and policy development to establish a safer and more resilient smart-home environment capable of withstanding ever-evolving cyber threats.

Acknowledgements

I would like to take this opportunity to express my sincere gratitude to all those who have supported and guided me throughout the research and writing of this thesis.

First and foremost, I would like to express my deepest appreciation to my eminent supervisor, Professor Youki Kadobayashi, and co-supervisor Associate Professor Yuzo Taenaka, for their invaluable guidance, expertise, and unwavering support. Their encouragement and insightful feedback have been instrumental in shaping the direction and quality of this research. I am truly grateful for their mentorship and the opportunities they have provided for my professional growth.

I would also like to extend my gratitude to the members of my thesis committee, Professor Shoji Kasahara, Professor Yuichi Hayashi, and Professor Masahiro Sasabe. Their valuable input, constructive criticism, and suggestions have greatly contributed to the refinement of this work.

Special thanks go to Professor Karen Renaud from the Department of Computer and Information Sciences at Strathclyde University and Professor Masahiro Sasabe from the Faculty of Informatics at Kansai University for their valuable collaboration.

I am deeply grateful to Professor Keiichi Yasumoto from the Ubiquitous Computing Systems Laboratory at Nara Institute of Science and Technology (NAIST), Associate Professor Doudou Fall from the Ecole Supérieure Polytechnique at University Cheikh Anta Diop, Associate Professor Shigeru Kashihara from the Department of Network Design at Osaka Institute of Technology, and Assistant Professor Monowar Bhuyan from the Department of Computing Science at Umeå University for their invaluable advice and support during my academic journey.

I am indebted to the former and present members of the Laboratory for Cyber Resilience who have provided unwavering support and encouragement throughout this journey. I am immensely grateful to Assistant Professor Muhammad Delwar Hossain and Research Professor Bernhards Blumbergs for their insightful discussions. I extend my gratitude to Dr. Enkhtur Tsogbaatar and Shun Yonamine for their moral support. I would also like to thank my fellow Ph.D. candidates: Mohd Ruzeiny Bin Kamaruzzaman, Abraham Olufemi Abiodun, Taisho Sasada, Mohammad Hafiz Hersyah, Kabid Hassan Shibly, and Nahid Ferdous Aurna, for

the valuable and enjoyable time we have spent together. I am also grateful to every Master's student I have encountered at the laboratory for their teamwork and the fun moments during my journey. Warm thanks to the secretaries who have made me feel comfortable and continuously supported my daily life in the laboratory. Special appreciation goes to Ayana Ryono, Haruna Okumura, and Yoko Inada for their contributions to the translation of the survey questionnaires. In addition, I would like to acknowledge the insightful discussions I had with Dr. Jema David Ndibwile and Dr. Nissy Sombatruang in designing the survey questionnaires.

I am grateful to the participants in the study who generously shared their time and opinions, making this research possible. Their willingness to contribute and engage in our survey has enriched the findings and conclusions of this thesis.

I would like to express my heartfelt gratitude to my friends and former classmates in Japan, the Republic of Côte d'Ivoire, and across the globe for their unwavering support. I am thankful for their continuous encouragement.

I would like to express my heartfelt appreciation to Dr. Julian Saolotoga Wong Soon and Ph.D. candidate Moris Deri, with whom I formed a close friendship during our six-month Japanese language studies at Osaka University. While I continued my education in Information Science and Engineering at NAIST, they pursued their respective studies in different departments within Osaka University. Despite our different paths, they have remained a constant source of support and encouragement throughout my research journey and my time in Japan.

I would like to express my heartfelt gratitude to the Ivorian community in Japan, whose support and camaraderie have been invaluable throughout my journey. In particular, I would like to extend my thanks to Moussa Zieh Ouattara, my fellow Ph.D. candidate at Kobe University, for our extensive and enriching discussions on academic research. I am also indebted to Dr. Elder Hippocrate A. Akpa, Dr. William-Fabrice Brou, and Cedric Konan, former NAIST students, for their unwavering support and guidance in navigating this journey. Their assistance has been instrumental in helping me settle into this new chapter of my academic pursuit. Furthermore, I would like to express my sincere appreciation to the Association of Ivorians in Japan (AIJ), led by its current president, François-Joseph Dacoury-Tabley, and its members. My special thanks go to Dr. Georges Kakou

and his family, Kouamé André Kouassi and his wife, Laurent Cheick Konan and his wife, Lancine Sako, Guy-Pérol Mandoumou, Damien Eklou, Eli Kouassi Koffi, and Florent Adiamonon for their support and insightful guidance about professional life in Japan. The AIJ has provided a warm and welcoming environment away from my home country. Its love, support, and vibrant community have made my stay in Japan truly enjoyable.

I would like to acknowledge the financial support provided by the Japanese Government (MEXT or Monbukagakusho) scholarship and the Industrial Cyber Security Center of Excellence (ICS-CoE) Core Human Resources Development Program. Their funding has been essential in facilitating the effective execution of this research.

Furthermore, I would like to extend my thanks to NAIST and its staff for their continuous support and dedication to nurturing students throughout their academic journey. Their commitment to providing a conducive learning environment has been invaluable.

A special acknowledgement goes to the dedicated teachers and lecturers who have enriched my educational journey, imparting new knowledge and skills from the very first day I stepped into school in 1998 until the present.

I would like to express my heartfelt appreciation to my extended family for their constant love, encouragement, and belief in my abilities. Their unwavering support and understanding have been my source of strength throughout this journey.

Finally, I would like to express my gratitude to all the individuals who, directly or indirectly, have influenced and inspired me in my academic and personal life. Your presence and impact have shaped my perspective, and I am truly grateful for the knowledge and experiences I have gained through our interactions.

This thesis would not have been possible without the support, guidance, and encouragement of all those mentioned above. Their contributions have been invaluable, and I am sincerely grateful for their assistance in this academic endeavor.

Dedication

In loving memory of my parents, Koffi Jacques Douha and Brou Elise N'zue, whom I never had the chance to know, but whose presence I feel deeply within me. Your spirits guide and inspire me as I strive to make you proud. This work is dedicated to you.

To my brothers, Christian Kouadio Arnaud Douha and Koffi John Francis Logba, who have been my constant pillars of support. Your encouragement and belief in me have been invaluable throughout this challenging endeavor. This work is dedicated to both of you, as a symbol of our unbreakable bond and the shared pursuit of excellence.

I wholeheartedly dedicate this work to my beloved extended family and cherished friends who have played an instrumental role in shaping my journey.

To the memory of my former classmates who shared the same aspirations and dreams of becoming doctors. Though you are no longer with us, your memory lives on, and your aspirations continue to drive my pursuit of knowledge. This thesis is dedicated to each of you, as a testament to our shared ambition and the indelible impact you have had on my journey.

To my dear offspring, whose existence is yet to unfold. You are the embodiment of my hopes, dreams, and aspirations. This work is dedicated to you, as a testament to my commitment to creating a better world for your generation. May this journey inspire you to pursue knowledge, embrace curiosity, and fearlessly pursue your own path.

To the future mother of my children, who will bring love, joy, and new beginnings into our lives. Though you may be unknown to me at this moment, I dedicate this thesis to you, as a symbol of the profound bond we will share. May our partnership be built on trust, support, and shared goals, as we navigate the joys and challenges of parenthood together.

Lastly, I dedicate this work to myself, for the resilience, determination, and personal growth I have experienced on this academic journey. It is a tribute to the person I have become and a reminder to always embrace my individuality and strive for continuous self-improvement.

May this dedication stand as an expression of gratitude and a celebration of the extraordinary individuals who have touched my life in meaningful ways.

References

[1] Statista. Smart Home – Market Data & Forecast 2022, 2022. [Online]. Available: https://www.statista.com/outlook/dmo/smart-home/worldwide. Accessed 2023-08-22.

[2] SAM Seamless Network. 2021 Landscape Security IoT, 2021. [Online]. Available: https://securingsam.com/2021-iot-security-landscape/. Accessed 2023-08-22.

[3] Jian Yang and Liu Sun. A Comprehensive Survey of Security Issues of Smart Home System: "Spear" and "Shields," Theory and Practice. *IEEE Access*, 10:124167–124192, 2022.

[4] Ali Dorri, Salil S. Kanhere, Raja Jurdak, and Praveen Gauravaram. Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 618–623, 2017.

[5] Sajad Shirali-Shahreza and Yashar Ganjali. Protecting Home User Devices with an SDN-Based Firewall. *IEEE Transactions on Consumer Electronics*, 64(1):92–100, 2018.

[6] Sowmya Ramapatruni, Sandeep Nair Narayanan, Sudip Mittal, Anupam Joshi, and Karuna Joshi. Anomaly Detection Models for Smart Home Security. In *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pages 19–24, 2019.

[7] Aibin Wang, Zifeng Yuan, and Bin He. Design and Realization of Smart Home Security System Based on AWS. In *2020 International Conference on Information Science, Parallel and Distributed Systems (ISPDS)*, pages 291–295, 2020.

[8] Rongjuan Zhu, Xinke Wu, Jun Sun, and Zhihua Li. Research on Smart Home Security Threat Modeling based on STRIDE-IAHP-BN. In *2021 20th Inter-*

national Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES), pages 207–213, 2021.

[9] Qin Lan, Hong Wang, Yinggang Hao, Tan Li, Bo Zhang, and Zaituo Yue. Data Encryption System for Smart Homes. In *2022 International Symposium on Control Engineering and Robotics (ISCER)*, pages 171–174, 2022.

[10] N'guessan Yves-Roland Douha, Monowar Bhuyan, Shigeru Kashihara, Doudou Fall, Yuzo Taenaka, and Youki Kadobayashi. A survey on blockchain, sdn and nfv for the smart-home security. *Internet of Things*, 20:100588, 2022.

[11] John D'Arcy, Anat Hovav, and Dennis Galletta. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, 20:79–98, 03 2009. https://doi.org/10.1287/isre.1070.0160.

[12] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), nov 2018. https://doi.org/10.1145/3274469.

[13] J. Li, K. Sun, B. Huff, A. Bierley, Y. Kim, F. Schaub, and K. Fawaz. "It's up to the Consumer to be Smart": Understanding the Security and Privacy Attitudes of Smart Home Users on Reddit. In *2023 2023 IEEE Symposium on Security and Privacy (SP) (SP)*, pages 380–396, Los Alamitos, CA, USA, may 2023. IEEE Computer Society. https://doi.org/10.1109/SP46215.2023.00022.

[14] Hussain Aldawood and Geoffrey Skinner. Challenges of Implementing Training and Awareness Programs Targeting Cyber Security Social Engineering. In *2019 Cybersecurity and Cyberforensics Conference (CCC)*, pages 111–117, 2019.

[15] Joseph Ricci, Frank Breitinger, and Ibrahim Baggili. Survey Results on Adults and Cybersecurity Education. *Education and Information Technologies*, 24:231–249, 2019.

[16] Devjani Roy and Richard Zeckhauser. Grappling with ignorance: Frameworks from decision theory, lessons from literature. *Journal of Benefit-Cost Analysis*, 6(1):33–65, 2015.

[17] Kazuhisa Takemura. Behavioral Decision Theory. Oxford Research Encyclopedia of Politics, 2020. [Online]. Available: https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-958. Accessed 2023-08-22.

[18] Benjamin Morrison, Lynne Coventry, and Pam Briggs. How do Older Adults feel about engaging with Cyber-Security? *Human Behavior and Emerging Technologies*, 3(5):1033–1049, December 2021.

[19] Yang Lu. Cybersecurity research: A review of current research topics. *Journal of Industrial Integration and Management*, 3(04):1850014, 2018. https://doi.org/10.1142/S2424862218500148.

[20] Lynne Coventry, Pamela Briggs, John Blythe, and Minh Tran. *Using behavioural insights to improve the public's use of cyber security best practices.* Government Office for Science, May 2014.

[21] Assar Lindbeck. Incentives and social norms in household behavior. *The American Economic Review*, 87(2):370–377, 1997.

[22] Lena-Marie Rehnen, Silke Bartsch, Marina Kull, and Anton Meyer. Exploring the impact of rewarded social media engagement in loyalty programs. *Journal of Service Management*, 28(2):305–328, 2017.

[23] S.M. Furnell, P. Bryant, and A.D. Phippen. Assessing the security perceptions of personal internet users. *Computers & Security*, 26(5):410–417, 2007.

[24] Steven Furnell, Valleria Tsaganidi, and Andy Phippen. Security beliefs and barriers for novice internet users. *Computers & Security*, 27(7):235–240, 2008.

[25] E. Kritzinger and S.H. von Solms. Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 29(8):840–847, 2010.

[26] Adele E. Howe, Indrajit Ray, Mark Roberts, Malgorzata Urbanska, and Zinta Byrne. The psychology of security for the home computer user. In *2012 IEEE Symposium on Security and Privacy*, pages 209–223, 2012.

[27] Fayez Alotaibi, Nathan Clarke, and Steven Furnell. An analysis of home user security awareness & education. In *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 116–122, 2017.

[28] Nazilah Ahmad, Umi Asma' Mokhtar, Wan Fariza Paizi Fauzi, Zulaiha Ali Othman, Yusri Hakim Yeop, and Siti Norul Huda Sheikh Abdullah. Cyber Security Situational Awareness among Parents. In *Cyber Resilience Conference (CRC)*, pages 1–3, 2018.

[29] Farzana Quayyum, Daniela S. Cruzes, and Letizia Jaccheri. Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30:100343, 2021. https://doi.org/10.1016/j.ijcci.2021.100343.

[30] Łukasz Tomczyk and Katarzyna Potyrała. Parents' knowledge and skills about the risks of the digital world. *South African Journal of Education*, 41:1–19, 03 2021.

[31] Carlene Blackwood-Brown, Yair Levy, and John D'Arcy. Cybersecurity Awareness and Skills of Senior Citizens: A Motivation Perspective. *Journal of Computer Information Systems*, 61(3):195–206, 2021. https://doi.org/10.1080/08874417.2019.1579076.

[32] Eric Zeng, Shrirang Mare, and Franziska Roesner. End User Security and Privacy Concerns with Smart Homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 65–80, Santa Clara, CA, July 2017. USENIX Association.

[33] Kaiwen Sun, Yixin Zou, Jenny Radesky, Christopher Brooks, and Florian Schaub. Child Safety in the Smart Home: Parents' Perceptions, Needs, and Mitigation Strategies. *Proc. ACM Hum.-Comput. Interact.*, 5(CSCW2), oct 2021. https://doi.org/10.1145/3479858.

[34] Hofstede Insights. Compare Countries, 2022. [Online]. Available: https://www.hofstede-insights.com/product/compare-countries/. Accessed 2023-08-22.

[35] Reddit. HomeAutomation, 2023. [Online]. Available: https://www.reddit.com/r/homeautomation/. Accessed 2023-08-22.

[36] Huseyin Cavusoglu, Srinivasan Raghunathan, and Wei T. Yue. Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems*, 25(2):281–304, 2008.

[37] Anna Nagurney and Ladimer S Nagurney. A game theory model of cybersecurity investments with information asymmetry. *NETNOMICS: Economic Research and Electronic Networking*, 16:127–148, 2015.

[38] Anna Nagurney, Ladimer S Nagurney, and Shivani Shukla. A supply chain game theory framework for cybersecurity investments under network vulnerability. *Computation, cryptography, and network security*, pages 381–398, 2015.

[39] Anna Nagurney, Patrizia Daniele, and Shivani Shukla. A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints. *Annals of operations research*, 248:405–427, 2017.

[40] Deepak K. Tosh, Iman Vakilinia, Sachin Shetty, Shamik Sengupta, Charles A. Kamhoua, Laurent Njilla, and Kevin Kwiat. Three layer game theoretic decision framework for cyber-investment and cyber-insurance. In Stefan Rass, Bo An, Christopher Kiekintveld, Fei Fang, and Stefan Schauer, editors, *Decision and Game Theory for Security*, pages 519–532, Cham, 2017. Springer International Publishing.

[41] Burhan Hyder and Manimaran Govindarasu. Optimization of Cybersecurity Investment Strategies in the Smart Grid Using Game-Theory. In *2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pages 1–5, 2020.

[42] Wei Sun, Xiangwei Kong, Dequan He, and Xingang You. Information Security Problem Research Based on Game Theory. In *2008 International Symposium on Electronic Commerce and Security*, pages 554–557, 2008.

[43] Marian Harbach, Alexander De Luca, Nathan Malkin, and Serge Egelman. Keep on Lockin' in the Free World: A Multi-National Comparison of Smartphone Locking. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, CHI '16, page 4823–4827, New York, NY, USA, 2016. Association for Computing Machinery. https://doi.org/10.1145/2858036.2858273.

[44] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, CHI '17, page 2202–2214, New York, NY, USA, 2017. Association for Computing Machinery. https://doi.org/10.1145/3025453.3025926.

[45] Jema David Ndibwile, Edith Talina Luhanga, Doudou Fall, Daisuke Miyamoto, and Youki Kadobayashi. A Comparative Study of Smartphone-User Security Perception and Preference towards Redesigned Security Notifications. In *Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities*, AfriCHI '18, New York, NY, USA, 2018. Association for Computing Machinery. https://doi.org/10.1145/3283458.3283486.

[46] Argyris Constantinides, Anna Maria Pietron, Marios Belk, Christos Fidas, Ting Han, and Andreas Pitsillides. *A Cross-Cultural Perspective for Personalizing Picture Passwords*, page 43–52. Association for Computing Machinery, New York, NY, USA, 2020. https://doi.org/10.1145/3340631.3394859.

[47] Serge Egelman and Eyal Peer. The Myth of the Average User: Improving Privacy and Security Systems through Individualization. In *Proceedings of the 2015 New Security Paradigms Workshop*, NSPW '15, page 16–28, New York, NY, USA, 2015. Association for Computing Machinery. https://doi.org/10.1145/2841113.2841115.

[48] Matthew Hull, Leah Zhang-Kennedy, Khadija Baig, and Sonia Chiasson. Understanding individual differences: factors affecting secure computer behaviour. *Behaviour & Information Technology*, 41(15):3237–3263, 2021. https://doi.org/10.1080/0144929X.2021.1977849.

[49] Michael Silverman. Non-financial recognition. *The Most Effective of Rewards. Brighton: Institute for Employment Studies*, 2004.

[50] Bobby J Calder and Barry M Staw. Interaction of intrinsic and extrinsic motivation: Some methodological notes. *Journal of Personality and Social Psychology*, 31(1):76–80, 1975. https://doi.org/10.1037/h0076167.

[51] Incentive Research Foundation. Using Behavioral Economics Insights in Incentives, Rewards, and Recognition: The Neuroscience, 2017. [Online]. Available: https://theirf.org/wp-content/uploads/2017/05/final-neuroscience-study.pdf. Accessed 2023-08-22.

[52] Uri Gneezy, Stephan Meier, and Pedro Rey-Biel. When and why incentives (don't) work to modify behavior. *Journal of Economic Perspectives*, 25(4):191–210, December 2011. https://doi.org/10.1257/jep.25.4.191.

[53] John Von Neumann and Oskar Morgenstern. *Theory of Games and Economic Behavior*. Princeton, NJ, USA: Princeton University Press, 1944.

[54] M.J. Osborne. *An Introduction to Game Theory*. Oxford University Press, 2009.

[55] J Maynard Smith. Game theory and the evolution of fighting. *On evolution*, pages 8–28, 1972.

[56] JMPGR Smith and George R Price. The logic of animal conflict. *Nature*, 246(5427):15–18, 1973.

[57] John Nash. Non-cooperative games. *Annals of mathematics*, pages 286–295, 1951.

[58] Oskar Morgenstern and John Von Neumann. *Theory of games and economic behavior*. Princeton university press, 1953.

[59] Ross Cressman and Yi Tao. The replicator equation and other game dynamics. *Proceedings of the National Academy of Sciences*, 111(supplement_3):10810–10817, 2014.

[60] N'guessan Yves-Roland Douha, Doudou Fall, Yuzo Taenaka, and Youki Kadobayashi. Threat Level Assessment of Smart-Home Stakeholders Using EBIOS Risk Manager. In *The Fifteenth International Conference on Emerging Security Information, Systems and Technologies (IARIA SECURWARE 2021)*, pages 31–40, November 2021.

[61] Moez Krichen and Roobaea Alroobaea. A new model-based framework for testing security of iot systems in smart cities using attack trees and price timed automata. In *Proceedings of the 14th International Conference on Evaluation of Novel Approaches to Software Engineering*, ENASE 2019, page 570–577, Setubal, PRT, 2019. SCITEPRESS - Science and Technology Publications, Lda.

[62] Farid Molazem Tabrizi and Karthik Pattabiraman. Formal security analysis of smart embedded systems. In *Proceedings of the 32nd Annual Conference on Computer Security Applications*, ACSAC '16, page 1–15, New York, NY, USA, 2016. Association for Computing Machinery.

[63] Pardeep Kumar, An Braeken, Andrei Gurtov, Jari Iinatti, and Phuong Hoai Ha. Anonymous secure framework in connected smart home environments. *IEEE Transactions on Information Forensics and Security*, 12(4):968–979, 2017.

[64] William H. Sandholm. *Evolutionary Game Theory*, pages 1–38. Springer Berlin Heidelberg, Berlin, Heidelberg, 2017.

[65] Deepak Tosh, Shamik Sengupta, Charles Kamhoua, Kevin Kwiat, and Andrew Martin. An evolutionary game-theoretic framework for cyber-threat information sharing. In *2015 IEEE International Conference on Communications (ICC)*, pages 7341–7346, 2015.

[66] Ahmed A. Alabdel Abass, Liang Xiao, Narayan B. Mandayam, and Zoran Gajic. Evolutionary Game Theoretic Analysis of Advanced Persistent Threats Against Cloud Storage. *IEEE Access*, 5:8482–8491, 2017.

[67] IBM. X-Force Threat Intelligence Index 2022, 2022. [Online]. Available: https://www.ibm.com/security/data-breach/threat-intelligence/. Accessed 2023-08-22.

[68] Daniel Friedman. Evolutionary Games in Economics. *Econometrica*, 59(3):637–666, 1991.

[69] Martín-Antonio Rodríguez-Licea, Francisco-J. Perez-Pinal, José-Cruz Nuñez-Pérez, and Yuma Sandoval-Ibarra. On the n-Dimensional Phase Portraits. *Applied Sciences*, 9(5), 2019.

[70] N'guessan Yves-Roland Douha, Bernard Ousmane Sane, Masahiro Sasabe, Doudou Fall, Yuzo Taenaka, and Youki Kadobayashi. Cost-benefit Analysis Toward Designing Efficient Education Programs for Household Security . In *The Fifteenth International Conference on Emerging Security Information, Systems and Technologies (IARIA SECURWARE 2021)*, pages 59–68, November 2021.

[71] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Comput. Surv.*, 50(3), aug 2017.

[72] ISO. ISO/IEC CD 27403.2: Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics. [Online]. Available: https://www.iso.org/standard/78702.html. Accessed 2023-08-22.

[73] Grand View Research. Smart home automation market worth $444.98 billion by 2030. Press Release, 2023. [Online]. Available: https://www.grandviewresearch.com/press-release/global-smart-home-automation-market. Accessed 2023-08-22.

[74] Statista. Smart Home: Japan, 2023. [Online]. Available: https://www.statista.com/outlook/dmo/smart-home/japan. Accessed 2023-08-22.

[75] Statista. Smart Home: United Kingdom, 2021. [Online]. Available: https://www.statista.com/outlook/dmo/smart-home/united-kingdom. Accessed 2023-08-22.

[76] Kate Pickett and Richard Wilkinson. *The spirit level: Why equality is better for everyone*. Penguin UK, 2010.

[77] Dimitris Ballas, Danny Dorling, Tomoki Nakaya, Helena Tunstall, and Kazumasa Hanaoka. Income inequalities in japan and the uk: A comparative study of two island economies. *Social Policy and Society*, 13(1):103–117, 2014.

[78] The Government of Japan. Cybersecurity Strategy, 2021. [Online]. Available: https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf. Accessed 2023-08-22.

[79] GOV.UK. National Cyber Strategy 2022, 2022. [Online]. Available: https://www.gov.uk/government/publications/national-cyber-strategy-2022. Accessed 2023-08-22.

[80] IoT Acceleration Consortium. IoT Security Guidelines Ver. 1.0, 2016. [Online]. Available: http://www.iotac.jp/wp-content/uploads/2016/01/IoT-Security-Guidelines_ver.1.0.pdf. Accessed 2023-08-22.

[81] IPA. IoT Safety/Security Development Guidelines (Second Edition), 2016. [Online]. Available: https://www.ipa.go.jp/publish/qv6pgp000000114a-att/000053920.pdf. Accessed 2023-08-22.

[82] UK Parliament. Product Security and Telecommunications Infrastructure Bill, 2021. [Online]. Available: https://bills.parliament.uk/bills/3069/publications. Accessed 2023-08-22.

[83] CrowdWorks. Easy online ordering for any job., 2023. [Online]. Available: https://crowdworks.jp. Accessed 2023-08-22.

[84] Prolific. Quickly find research participants you can trust, 2023. [Online]. Available: https://www.prolific.co. Accessed 2023-08-22.

[85] Marian Harbach, Alexander De Luca, Nathan Malkin, and Serge Egelman. Keep on lockin' in the free world: A multi-national comparison of smartphone locking. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, CHI '16, page 4823–4827, New York, NY, USA, 2016. Association for Computing Machinery.

[86] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, CHI '17, page 2202–2214, New York, NY, USA, 2017. Association for Computing Machinery. https://doi.org/10.1145/3025453.3025926.

[87] World Economic Forum. Delivering free and globally accessible cybersecurity training, 2023. [Online]. Available: https://www.weforum.org/impact/cybersecurity-training/. Accessed 2023-08-22.

[88] SANS Institute. Free Cyber Security Training, 2023. [Online]. Available: https://www.sans.org/cyberaces/. Accessed 2023-08-22.

[89] European Commission. EU Cyber Resilience Act, 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act. Accessed 2023-08-22.

Appendix

A. Jacobian Matrix

$$
\begin{aligned}
\frac{\partial f(x)}{\partial x} =& x[C_{12} - R_{11} + z_1 C_{13} P(A_1/T) + z_1 C_{14} P(A_1/T) - z_1 C_{13} P(A_1/\bar{T}) - z_1 \\
& C_{14} P(A_1/\bar{T}) - y z_1 C_{13} P(A_1/T) + y z_1 C_{13} P(A_1/\bar{T})] + (x-1)[C_{12} - R_{11} \\
& + z_1 C_{13} P(A_1/T) + z_1 C_{14} P(A_1/T) - z_1 C_{13} P(A_1/\bar{T}) - z_1 C_{14} P(A_1/\bar{T}) \\
& - y z_1 C_{13} P(A_1/T) + y z_1 C_{13} P(A_1/\bar{T})] \\
\frac{\partial f(x)}{\partial y} =& - x(x-1)[z_1 C_{13} P(A_1/T) - z_1 C_{13} P(A_1/\bar{T})] \\
\frac{\partial f(x)}{\partial z_1} =& x(x-1)[C_{13} P(A_1/T) + C_{14} P(A_1/T) - C_{13} P(A_1/\bar{T}) - C_{14} P(A_1/\bar{T}) \\
& - y C_{13} P(A_1/T) + y C_{13} P(A_1/\bar{T})] \\
\frac{\partial f(x)}{\partial z_2} =& 0 \\
\frac{\partial f(y)}{\partial x} =& 0 \\
\frac{\partial f(y)}{\partial y} =& y[C_{20} - P_{20} + P_{21} - R_{20} + z_2 C_{21} P(A_2/S) - z_2 C_{21} P(A_2/\bar{S})] + (y-1) \\
& [C_{20} - P_{20} + P_{21} - R_{20} + z_2 C_{21} P(A_2/S) - z_2 C_{21} P(A_2/\bar{S})] \\
\frac{\partial f(y)}{\partial z_1} =& 0 \\
\frac{\partial f(y)}{\partial z_2} =& y(y-1)[C_{21} P(A_2/S) - C_{21} P(A_2/\bar{S})] \\
\frac{\partial f(z_1)}{\partial x} =& z_1[z_1[y[C_{30} - C_{31} - C_{14} P(A_1/T) + C_{14} P(A_1/\bar{T})] - (y-1)[C_{30} - C_{31} \\
& - P(A_1/T)(C_{13} + C_{14}) + P(A_1/\bar{T})(C_{13} + C_{14})]] - y[C_{30} - C_{31} - C_{14} \\
& P(A_1/T) + C_{14} P(A_1/\bar{T})] + (y-1)[C_{30} - C_{31} - P(A_1/T)(C_{13} + C_{14}) \\
& + P(A_1/\bar{T})(C_{13} + C_{14})]]
\end{aligned}
$$

$$\frac{\partial f(z_1)}{\partial y} = z_1[x(C_{30} - P(A_1/T)(C_{13} + C_{14})) - z_1[x(C_{30} - P(A_1/T)(C_{13} + C_{14}))$$
$$- x(C_{30} - C_{14}P(A_1/T)) - (C_{31} - P(A_1/\bar{T})(C_{13} + C_{14}))(x-1)+$$
$$(C_{31} - C_{14}P(A_1/\bar{T}))(x-1)] - x(C_{30} - C_{14}P(A_1/T)) - (C_{31} -$$
$$P(A_1/\bar{T})(C_{13} + C_{14}))(x-1) + z_2[x(C_{32} - P(A_2/S)(C_{13} + C_{21})) - x$$
$$(C_{33} - P(A_2/\bar{S})(C_{13} + C_{21})) - (C_{32} - P(A_2/S)(C_{13} + C_{21}))(x-1)+$$
$$(C_{33} - P(A_2/\bar{S})(C_{13} + C_{21}))(x-1)] + (C_{31} - C_{14}P(A_1/\bar{T}))(x-1)]$$

$$\frac{\partial f(z_1)}{\partial z_1} = [x(C_{30} - P(A_1/T)(C_{13} + C_{14})) - (C_{31} - P(A_1/\bar{T})(C_{13} + C_{14}))(x-1)]$$
$$(y-1) - 2z_1[(x(C_{30} - P(A_1/T)(C_{13} + C_{14})) - (C_{31} - P(A_1/\bar{T})(C_{13} +$$
$$C_{14}))(x-1))(y-1) - y(x(C_{30} - C_{14}P(A_1/T)) - (C_{31} - C_{14}P(A_1/\bar{T}))$$
$$(x-1))] - z_2[(x(C_{33} - P(A_2/\bar{S})(C_{13} + C_{21})) - (C_{33} - P(A_2/\bar{S})(C_{13} +$$
$$C_{21}))(x-1))(y-1) - y(x(C_{32} - P(A_2/S)(C_{13} + C_{21})) - (C_{32} -$$
$$P(A_2/S)(C_{13} + C_{21}))(x-1))] - y[x(C_{30} - C_{14}P(A_1/T))$$
$$- (C_{31} - C_{14}P(A_1/\bar{T}))(x-1)]$$

$$\frac{\partial f(z_1)}{\partial z_2} = - z_1[[x(C_{33} - P(A_2/\bar{S})(C_{13} + C_{21})) - (x-1)(C_{33} - P(A_2/\bar{S})$$
$$(C_{13} + C_{21}))](y-1) - y[x(C_{32} - P(A_2/S)(C_{13} + C_{21})) - (x-1)$$
$$(C_{32} - P(A_2/S)(C_{13} + C_{21}))]]$$

$$\frac{\partial f(z_2)}{\partial x} = z_1 z_2[y[C_{30} - C_{31} - C_{14}P(A_1/T) + C_{14}P(A_1/\bar{T})] - (y-1)[C_{30} - C_{31}$$
$$- P(A_1/T)(C_{13} + C_{14}) + P(A_1/\bar{T})(C_{13} + C_{14})]]$$

$$\frac{\partial f(z_2)}{\partial y} = - z_2[x(C_{32} - P(A_2/S)(C_{13} + C_{21})) - x(C_{33} - P(A_2/\bar{S})(C_{13} + C_{21}))+$$
$$z_1[x(C_{30} - P(A_1/T)(C_{13} + C_{14})) - x(C_{30} - C_{14}P(A_1/T)) - (C_{31} -$$
$$P(A_1/\bar{T})(C_{13} + C_{14}))(x-1) + (C_{31} - C_{14}P(A_1/\bar{T}))(x-1)] - (C_{32} -$$
$$P(A_2/S)(C_{13} + C_{21}))(x-1) + (C_{33} - P(A_2/\bar{S})(C_{13} + C_{21}))(x-1) - z_2$$
$$[x(C_{32} - P(A_2/S)(C_{13} + C_{21})) - x(C_{33} - P(A_2/\bar{S})(C_{13} + C_{21})) - (C_{32}$$
$$- P(A_2/S)(C_{13} + C_{21}))(x-1) + (C_{33} - P(A_2/\bar{S})(C_{13} + C_{21}))(x-1)]]$$

$$\frac{\partial f(z_2)}{\partial z_1} = - z_2[(y-1)[x(C_{30} - P(A_1/T)(C_{13} + C_{14})) - (C_{31} - P(A_1/\bar{T})(C_{13}+ C_{14}))(x-1)] - y[x(C_{30} - C_{14}P(A_1/T)) - (x-1)(C_{31} - C_{14}P(A_1/\bar{T}))]]$$

$$\frac{\partial f(z_2)}{\partial z_2} =[x(C_{33} - P(A_2/\bar{S})(C_{13} + C_{21})) - (C_{33} - P(A_2/\bar{S})(C_{13} + C_{21}))(x-1)] (y-1) - z_1[(x(C_{30} - P(A_1/T)(C_{13} + C_{14})) - (C_{31} - P(A_1/\bar{T})(C_{13}+ C_{14}))(x-1))(y-1) - y(x(C_{30} - C_{14}P(A_1/T)) - (C_{31} - C_{14}P(A_1/\bar{T})) (x-1))] - 2z_2[(x(C_{33} - P(A_2/\bar{S})(C_{13} + C_{21})) - (C_{33} - P(A_2/\bar{S})(C_{13} + C_{21}))(x-1))(y-1) - y(x(C_{32} - P(A_2/S)(C_{13} + C_{21})) - (C_{32}- P(A_2/S)(C_{13} + C_{21}))(x-1))] - y[x(C_{32} - P(A_2/S)(C_{13} + C_{21})) - (C_{32} - P(A_2/S)(C_{13} + C_{21}))(x-1)]$$

B. Survey Questionnaire

B.1 Demographics

1. (Dem_1) What is your citizenship?
    - Japanese
    - British
    - Other:_____
2. (Dem_2) What is your age?
    - 25 - 34
    - 35 - 44
    - 45 - 54
    - 55 - 64
3. (Dem_3) What is your gender?
    - Female
    - Male
    - Non-binary or non-conforming
4. (Dem_4) What is your level of education?
    - Japan
        - Junior high school
        - High school
        - Bachelor's Degree
        - Master's Degree
        - Doctorate Degree
        - Other:_____
    - UK
        - GCSE / National 5 (O-level)

- A-level / Higher / Advanced Higher
- Bachelor's Degree
- Master's Degree
- Doctorate Degree
- Other:_____

5. (Dem_5) What is your current employment status?

   - Employed full-time
   - Employed part-time
   - Home duties (Full-time stay-at-home)
   - Retired
   - Self-employed
   - Student
   - Unable to work
   - Unemployed looking for work
   - Unemployed not looking for work

6. (Dem_6) How many members of your household are under the age of 18?

7. (Dem_7) How many members of your household are of age 65 years and above?

B.2 Knowledge about Smart Homes

A smart home is a house equipped with many Internet-of-Things (IoT) devices (e.g., smart bulbs, smart TVs, smart speakers, smart kitchen appliances, smart locks, smart IP cameras, and smart cars) that automate tasks normally handled by humans and are typically remotely controlled.

8. (KSH_1) How many IoT devices do you own?

    - None
    - 1-4
    - 5-10
    - 11-15
    - 16-20
    - 21-25
    - 26-30
    - More than 30

9. (KSH_2) Please select all the types of IoT devices used in your house.

    - Smart bulbs
    - Smart cars
    - Smart displays (e.g., Google Nest Hub)
    - Smart fridges
    - Smart garage door openers
    - Smart hubs (smart-home hubs)
    - Smart IP cameras
    - Smart locks
    - Smart meters
    - Smart ovens
    - Smart plugs

- Smart speakers
- Smart thermostats
- Smart TVs
- Smart vacuum cleaners
- Other:_____

B.3 Smart-Home Security

A smart home is a convenient technology because it improves the quality of life at home. However, smart-home devices are not designed with security as a priority, and they collect and share private information targeted by cyber attackers. For instance, according to a recent experiment, smart homes could be exposed to more than 12,000 cyberattacks in a single week.

10. (SHS_1) Have you ever taken any formal cybersecurity awareness training, or have you worked or studied in the cybersecurity field? Please select "Yes" if any of these instances apply.

    - No
    - Yes

11. (SHS_2) Which of the following cyberattacks are you aware of?

    - Data and Identity theft
      Data generated by unprotected wearables and smart appliances provide cyberattackers with an ample amount of targeted personal information that can potentially be exploited for fraudulent transactions and identity theft.
    - Device hijacking
      The attacker hijacks and effectively assumes control of a device. It only takes one device to potentially gain access to an entire network and infect all IoT devices in the home.
    - Distributed Denial-of-Service (DDoS)
      A denial-of-service attack (DoS attack) attempts to render a machine

or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. In the case of a distributed DoS (DDoS), the incoming traffic flooding a target originates from multiple sources.

- Man-in-the-Middle (MITM)
  An attacker breaches, interrupts, or spoofs communications between two systems. For example, an attacker can disable vulnerable HVAC systems during a heat wave, creating a disastrous scenario for service providers with affected models.
- Permanent Denial of Service (PDoS)
  PDoS, also known as phlashing, is an attack that damages the device so badly that it requires replacement or reinstallation of hardware. For example, the attackers can feed fake data to thermostats in an attempt to cause irreparable damage via extreme overheating.
- Social engineering
  The attackers manipulate or trick people into divulging confidential information, transferring money, or downloading malware using social interactions (e.g., phone talking, email, social media).
- Other:_____
- None / Not applicable

12. (SHS_3) How secure or insecure do you think your smart home is?
    - Very insecure
    - Insecure
    - I don't know / Unsure
    - Secure
    - Very secure

B.4 Cybersecurity Awareness Training

Cybersecurity awareness training may help households to prevent and protect their smart homes from cyberattacks.

13. (CAT_1) Do you agree or disagree that you need cybersecurity awareness training to learn how to secure effectively your smart home?
    - Strongly disagree
    - Disagree
    - Neutral
    - Agree
    - Strongly agree
14. (CAT_2) Are you willing to spend **money** on cybersecurity awareness training every year in a personal capacity to protect your smart home?
    - No
    - Yes
15. (CAT_3) Are you willing to spend **time** on cybersecurity awareness training every year in a personal capacity to protect your smart home?
    - No
    - Yes
16. (CAT_4) Do you agree or disagree that children need cybersecurity awareness training?
    - Strongly disagree
    - Disagree
    - Neutral
    - Agree
    - Strongly agree

17. (CAT_5) Do you agree or disagree that senior citizens need cybersecurity awareness training?

    - Strongly disagree
    - Disagree
    - Neutral
    - Agree
    - Strongly agree

B.5 Non-Financial Rewards for Pro-Cybersecurity Behavior

We aim to provide non-financial rewards in smart homes to encourage users to adopt good cybersecurity behavior.

18. (NFR_1) How satisfied or dissatisfied would you be with receiving non-financial rewards to encourage you to practice good cybersecurity hygiene at home?

    - Very dissatisfied
    - Dissatisfied
    - I don't know / Unsure
    - Satisfied
    - Very satisfied

19. (NFR_2) Would you be interested in competing with other smart-home users to get the award of the "CERTIFICATE OF ACHIEVEMENT FOR GOOD CYBERSECURITY BEHAVIOR AT HOME"?

    - Not at all
    - Slightly
    - Moderately
    - Very
    - Extremely

20. (NFR_3) Would you be interested in having virtual reality (VR) services in your smart home as a reward? For instance, virtual aquarium tour, virtual beach tour, virtual city tour, virtual mountain climbing tour, virtual museum tour, virtual space station tour, virtual zoo tour

    - Not at all
    - Slightly
    - Moderately
    - Very
    - Extremely

21. (NFR_4) What non-financial reward would you like to get when behaving securely in your smart home?

    - Getting awards
    - Playing online games
    - Getting virtual point rewards
    - Getting access to virtual reality (VR) services
    - Getting cyber insurance discounts for households
    - Getting badges
    - Other:_____
    - None of the above

Publication List

Journals

1. **N'guessan Yves-Roland Douha**, Karen Renaud, Yuzo Taenaka, Youki Kadobayashi, "Smart Home Cybersecurity Awareness and Behavioral Incentives", *Information and Computer Security*, pp. 1-17, 2023, ISSN 2056-4961, DOI: 10.1108/ICS-03-2023-0032.

2. **N'guessan Yves-Roland Douha**, Masahiro Sasabe, Yuzo Taenaka, Youki Kadobayashi, "An Evolutionary Game Theoretic Analysis of Cybersecurity Investment Strategies for Smart-Home Users against Cyberattacks", *Applied Sciences*, Vol. 13, No. 7, 2023, 4645, ISSN 2076-3417, DOI: 10.3390/app13074645.

3. **N'guessan Yves-Roland Douha**, Monowar Bhuyan, Shigeru Kashihara, Doudou Fall, Yuzo Taenaka, Youki Kadobayashi, "A Survey on Blockchain, SDN and NFV for the Smart-Home Security", *Internet of Things*, Vol. 20, 2022, 100588, ISSN 2542-6605, DOI: 10.1016/j.iot.2022.100588.

International Conferences

4. **N'guessan Yves-Roland Douha**, Doudou Fall, Yuzo Taenaka, Youki Kadobayashi, "Threat Level Assessment of Smart-Home Stakeholders Using EBIOS Risk Manager", In *The Fifteenth International Conference on Emerging Security Information, Systems and Technologies (IARIA SECURWARE 2021)*, pp. 31-40, November 2021.

5. **N'guessan Yves-Roland Douha**, Bernard Ousmane Sane, Masahiro Sasabe, Doudou Fall, Yuzo Taenaka, Youki Kadobayashi, "Cost-benefit Analysis Toward Designing Efficient Education Programs for Household Security", In *The Fifteenth International Conference on Emerging Security Information, Systems and Technologies (IARIA SECURWARE 2021)*, pp. 59-68, November 2021.