Kostelić, Katarina

Article

Dynamic awareness and strategic adaptation in cybersecurity: A game-theory approach

Games

Provided in Cooperation with:
MDPI – Multidisciplinary Digital Publishing Institute, Basel

Suggested Citation: Kostelić, Katarina (2024) : Dynamic awareness and strategic adaptation in cybersecurity: A game-theory approach, Games, ISSN 2073-4336, MDPI, Basel, Vol. 15, Iss. 2, pp. 1-28,
https://doi.org/10.3390/g15020013

This Version is available at:
https://hdl.handle.net/10419/330082

games

MDPI

Article

Dynamic Awareness and Strategic Adaptation in Cybersecurity: A Game-Theory Approach

Katarina Kostelić

Faculty of Economics and Tourism "Dr. Mijo Mirković", Department of Mathematics, Statistics and Informatics, Juraj Dobrila University of Pula, Preradovićeva 1/1, 52100 Pula, Croatia; katarina.kostelic@unipu.hr

Abstract: Awareness and human factors are becoming ever more important in cybersecurity, particularly in the context of small companies that may need more resources to deal with cybersecurity effectively. This paper introduces a theoretical framework for game analysis of the role of awareness in strategic interactions between the manager and a hacker. A computable approach is proposed based on Bayesian updating to model awareness in a cybersecurity context. The process of gaining awareness considers the manager's perception of the properties of the hacker's actions, game history, and common knowledge. The role of awareness in strategy choices and outcomes is analyzed and simulated, providing insights into decision-making processes for managers and highlighting the need to consider probabilistic assessments of threats and the effectiveness of countermeasures. The accuracy of the initial frequencies plays a significant role in the manager's success, with aligned frequencies leading to optimal results. Inaccurate information on prior frequencies still outperforms complete uncertainty, emphasizing the value of any available intelligence. However, the results suggest that other awareness modeling approaches are necessary to enhance the manager's agility and adaptiveness when the prior frequencies do not reflect the immediate attacker's type, indicating the need for improved intelligence about cyber-attacks and examinations of different awareness modeling approaches.

Keywords: awareness; game theory; cybersecurity; attacks; strategies

Citation: Kostelić, K. Dynamic Awareness and Strategic Adaptation in Cybersecurity: A Game-Theory Approach. *Games* **2024**, *15*, 13. https://doi.org/10.3390/g15020013

Academic Editors: Ulrich Berger and Jun Zhuang

Received: 19 February 2024
Revised: 29 March 2024
Accepted: 6 April 2024
Published: 8 April 2024

1. Introduction

The transition to the digital era has brought unprecedented opportunities for small- and medium-sized enterprises (SMEs) and significantly increased their exposure to cyber threats. As digitalization becomes increasingly integral to business operations, SMEs, which often lack the robust cybersecurity infrastructure of larger corporations, find themselves particularly vulnerable. This paper proposes a game-theory framework to enhance managerial awareness of cybersecurity threats, offering insights into strategic decision-making in the face of evolving cyber risks. In an age where cybercrime's economic impact is measured in trillions of dollars [1] and the COVID-19 pandemic has further accelerated digital dependency [2], SMEs' need to strengthen their cyber defenses has never been more critical.

The array of cybersecurity threats that SMEs face is vast and varied, encompassing everything from the psychological manipulations of social engineering to the technical exploits of software vulnerabilities and the overwhelming assaults of distributed denial of service (DDoS) attacks [3–5]. Each type of threat demands a tailored strategic response, highlighting the paramount importance of human factors—particularly managerial awareness—in successfully identifying, preventing, and mitigating cyber threats.

As cybersecurity threats evolve and increase in complexity, small- and medium-sized enterprises (SMEs) find themselves particularly vulnerable due to resource constraints and often limited cybersecurity expertise. While modern organizations' cybersecurity challenges are vast and varied, this paper specifically addresses the problem of dynamic

awareness and strategic adaptation to cybersecurity threats within SMEs. The importance of this problem lies in the critical role that awareness and strategic decision-making play in preempting and mitigating cyber-attacks. With SMEs contributing significantly to economic growth and innovation, ensuring their resilience against cyber threats is not only vital for the survival of these enterprises but also for broader economic security. Therefore, this paper introduces a game-theory framework to enhance the managerial awareness of cybersecurity threats, offering insights into strategic decision-making that can fortify SMEs against evolving cyber risks. This targeted focus addresses a gap in the literature and provides a novel approach to understanding and improving cybersecurity management in a context where it is most needed.

This emphasis on human factors is crucial; cybersecurity is not solely a technical challenge but also a human one. Managers and decision-makers play an important role in shaping an organization's cybersecurity posture, from setting policies and allocating resources to fostering a culture of awareness and resilience among all staff members. Despite the complexity of the cyber threat landscape, the human element remains both a potential vulnerability and a powerful asset in cybersecurity defense.

By intertwining the domains of game theory, behavioral science, and cybersecurity, this paper aims to address these multifaceted challenges. It proposes a model designed to deepen the understanding of managerial cybersecurity awareness within SMEs, thereby enhancing their capability to navigate the myriad of cyber threats. This approach seeks to bolster SMEs' cybersecurity infrastructure and empower their human resources—managers and employees alike—with the awareness and strategic insight necessary to anticipate, recognize, and effectively respond to cyber threats.

In doing so, we acknowledge the dual nature of cybersecurity as a field that requires both advanced technological tools and sophisticated human insight. The integration of game theory and behavioral science into cybersecurity strategies offers a pathway to the future development of more holistic and effective defenses, underpinning the critical role of human factors in securing the digital age. Through this exploration, we aim to contribute to the broader discourse on cybersecurity, emphasizing the indispensable role of human awareness and decision-making in safeguarding digital enterprises against the ever-evolving threats they face.

The goal is to introduce a game-theory framework to analyze dynamic awareness in cybersecurity by using a computable approach with Bayesian updating to model strategic choices in interactions between managers and hackers. Its usefulness is demonstrated through simulated scenarios, highlighting its practical implications for SMEs.

2. Theoretical Background

A recent review [6] on situation awareness in the Security Operations Center, focusing on cybersecurity, showed that human factors emphasizing situation awareness are important in understanding and improving human performance in complex systems. Another study [7] identified organizational awareness in security management as the most important factor, along with security controls and supportive top management. Due to the ongoing digitalization trend, many companies engage in digital businesses without a complete digital transformation of the company or the formation of a Security Operations Center. These enterprises often operate with limited resources, making it challenging to implement comprehensive cybersecurity strategies. In a small company, a person may take many roles at once—the role of the owner, investor, and manager—but he/she is also likely to deal with cyber security. Moreover, many small companies lack the resources to handle cybersecurity appropriately. While they will likely have the basic tools, they might lack the policies, procedures, and training [1]. In small companies, managers may deal with cybersecurity by themselves, outsource the issue to external experts if their budget allows it, or occasionally delegate to expert employees if such employees exist in the company [2,8].

Cybersecurity threats take many forms [2,3], from accidental data leaking to different forms of social engineering, ransomware, exploiting software vulnerabilities, and dis-

tributed denial of service attacks (Figure 1). The best company's strategy against attacks is a multi-layered approach that includes several activities and practices that encompass the entire organization and can help reduce the risk of successful attacks and minimize the impact of any attacks that do occur [4]. While some of these activities can be easily done by laypeople and multi-tasking managers of small companies (patching and updating software and setting authentication with strong passwords), others require knowledge and experience (for example, vulnerability testing or network segmentation). In addition, at least some of these practices must be taught to employees, even temporarily [5].

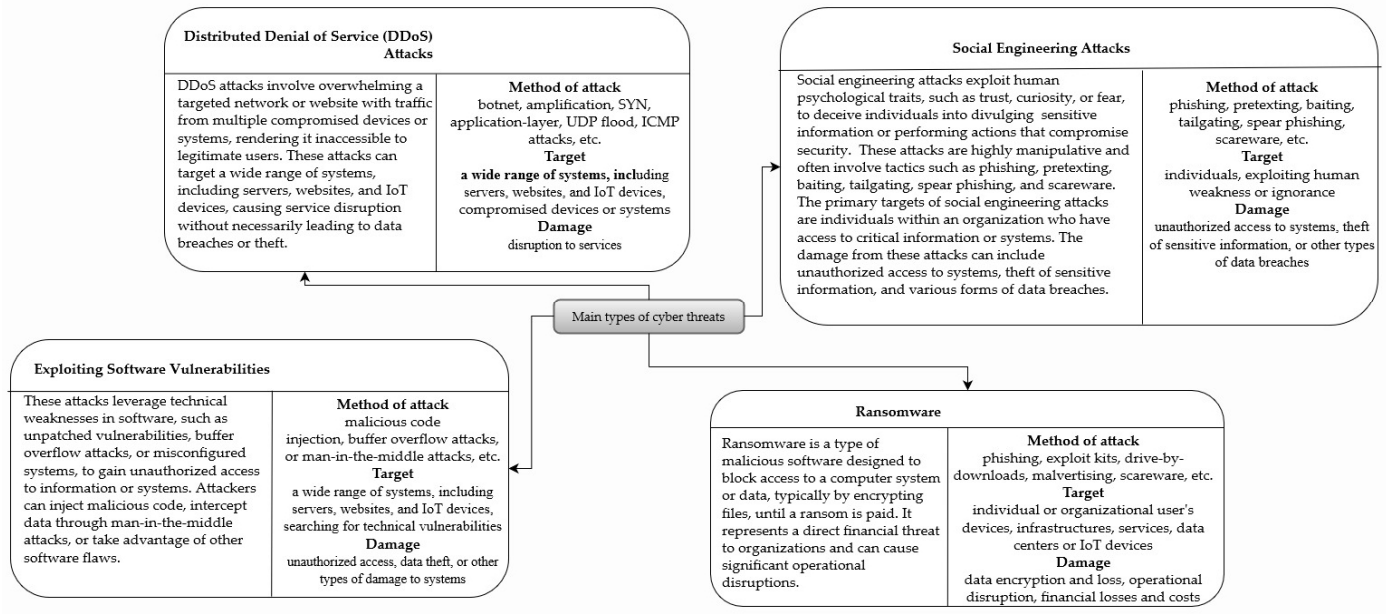

Figure 1. Most common types of cyber-attacks. Source: systematization based on [9–11].

However, companies' best strategies will depend on the type of attack (Figure 1). For example, the manager should implement a specific defense strategy to protect the company from social engineering. Nevertheless, they should first recognize that it is a social-engineering attack or any other type. They may do that by observing the detectable attack properties, such as the method of the attack, target, or damage (Figure 1). In the case of a social-engineering attack, the strategy should include raising awareness and education, security policies and procedures, technical controls, incident response, and continuous monitoring and improvement. On the other hand, if a manager wants to defend the company against a DDoS attack, he/she should change the strategy and implement one that involves DDoS mitigation solutions, network segmentation, scalable infrastructure, an incident-response plan, testing and simulation, collaboration, and information sharing (as in cybersecurity alliances [12]). The best company's strategy against software vulnerability exploits may include patching and updating software, vulnerability scanning and testing, access control and authentication, network segmentation, incident response plan, and employee training and raising awareness. Different companies' strategies are required to counteract each type of attack because the attacks differ in the method of attack, target, and resulting damage. However, managers must be aware of the attacks and their properties to do so.

Understanding human factors, particularly the impact of errors and biases, is crucial in cybersecurity. Leng et al. [13] provide a game-theory model that analytically describes the strategic interactions between software manufacturers and hackers (ethical and malicious). They explore the relationship between the credibility of white hats and software information disclosure and the dynamics of information theft by black hats. The study [14] bridges the gap between theoretical cybersecurity measures and practical, data-driven defense strategies by modeling cyber threats within a game-theory framework. This model

considers both attackers' and defenders' strategies, offering insights into optimal defense mechanisms based on real-world data. Moreover, Aggarwal et al. [15] introduce the concept of using deception as a strategic countermeasure against cyber-attacks. This is the game's theoretical discourse on innovative defense mechanisms beyond conventional security solutions, emphasizing cybersecurity's psychological and strategic dimensions.

A novel simulation tool, HackIt, was designed to enhance the understanding of human factors in cybersecurity [16]. It enables the creation of dynamic and realistic cyber-attack scenarios, offering a platform for studying the behavior of attackers and defenders in a controlled environment. The HackIt tool's development and application in studying deception strategies open avenues for future research on human factors in cybersecurity game dynamics, suggesting the creation of various cyber scenarios and investigating different aspects of cybersecurity. Further study regarding HackIt outlines how deception can mislead attackers, potentially delaying or thwarting cyber-attacks, thus providing a practical application of theoretical deception strategies within cybersecurity [17]. The integration between game theory, behavioral science, and cybersecurity practices enables us to analyze attackers' probing and attack behaviors, learning patterns, and responses to deception. It provides a comprehensive framework for understanding adversarial cognition in cybersecurity contexts, emphasizing the cognitive and behavioral aspects of cybersecurity.

As a specific human factor possibly expanded by technology, Aggarwal et al. [18] emphasize the critical role of cyber situational awareness in defending against cyber-attacks. Cyber situational awareness refers to the ability to identify, process, and comprehend information about cyber threats. It involves understanding the current cybersecurity state, potential impacts of threats, and necessary actions to mitigate risks. They discuss how Intrusion Detection Systems (IDSs) contribute to situational awareness by alerting defenders about possible threats. IDSs are security technologies that monitor network or system activities. By analyzing how the presence and accuracy of IDS influence the decision-making processes of both defenders and adversaries, the paper shows that IDS alerts significantly affect the sequential defenders' and adversaries' decisions across multiple trials presented in the paper, offering a deeper understanding of how individuals adapt their strategies over time in response to IDS recommendations. They rely on Instance-Based Learning Theory (IBLT), a theory of decision-making that explains how individuals make choices based on their past experiences. In essence, IBLT suggests that when individuals are faced with a decision, they recall instances from their memory similar to the current situation and use them to guide their decision. IBLT can be a robust framework for understanding decision-making in dynamic environments, which is particularly relevant for computational cognitive modeling and can simulate complex human behaviors in cybersecurity contexts [19].

The exploration of awareness in strategic interactions, particularly through the lens of the Prisoner's Dilemma, reveals profound implications for game theory modeling and decision-making processes [20]. This inquiry not only enriches our understanding of how players' perceptions and levels of awareness influence their strategic choices but also highlights the necessity for game-theory models to incorporate cognitive and informational nuances to reflect real-world dynamics accurately. By offering insights into the deviations caused by (un)awareness and extending these findings to practical domains such as management and security operations, this research underscores the critical role of awareness in shaping strategic outcomes. It bridges a gap in the literature and sets a foundation for future investigations, thereby providing a link between theoretical insights on awareness in game theory and their practical applications in strategic decision-making. This is a pivotal transition to a deeper dive into the role of awareness in game theory within the theoretical framework, emphasizing its importance in developing more sophisticated and realistic models of strategic interaction.

Game theory provides a framework to analyze strategic interactions and understand how players with different awareness and information levels can reach equilibrium out-

comes. The concept of awareness is central to modeling and analyzing these interactions, as it allows players to anticipate and respond to each other's actions strategically. In game theory, awareness is a key concept in understanding and analyzing strategic interactions between players. It refers to each player's knowledge or belief about the game structure, the possible actions of other players, and the payoffs associated with different outcomes. Awareness allows players to make decisions based on their understanding of the game and their expectations of how other players will behave.

Defining and modeling awareness in game theory is still a developing area of research, but the interest in (un)awareness has been ongoing in various disciplines involving human actors. For example, given the different areas of research, awareness receives distinctive adjectives, such as context awareness, situational awareness, space situational awareness, cyber awareness, temporal awareness, dynamic unawareness, partial awareness, individual awareness, knowledge awareness, public awareness, environmental awareness, brand awareness, etc. ([6,21–30]). Given the application, the research spans cyber security, surveillance, autonomous vehicles, wireless technologies, the Internet of things, intelligence and software methods, operations research, management, and marketing.

However, the core research on defining and modeling (un)awareness in game theory is limited. Game (un)awareness is frequently examined from an epistemic game theory standpoint ([25,31–34]), along with the attempts from the computable and behavioral standpoint (for example, Refs. [35–39]). While existing research offers different approaches to modeling (un)awareness, there are still discrepancies. For example, Halpern and Piermont [26] propose partial awareness, where the player values different objects (or different states of the objects) the same if their properties are the same and can value objects differently if they can be distinguished in some way that the individual is aware of; and the player can base his/her preferences only on the properties that he/she are aware of. Such an approach implies that an individual must be able to differentiate the properties and evaluate them to become at least partially aware of them. Similarly, Sadzik [40] assumes propositionally determined semantic awareness, while unawareness denotes the inability to differentiate between situations based on certain propositions. These approaches diminish the vagueness of the (un)awareness concept, as the (un)awareness is often described as a function denoting a general level of existing (un)awareness in computable versions. The computable approach to building (un)awareness based on the object or action's properties in this way has not been previously attempted. Therefore, this paper examines such an approach, aiming to contribute to solving the problem of modeling human (un)awareness in a computable game setting.

These approaches allow for an applicative approach to building awareness. The information to develop initial awareness of possible attacks may be available to managers through publicly available reports (for example, Ref. [41]). However, some of the properties of the attack may be perceivable to the manager only after the attack begins. These properties, as imperfectly perceived by the manager, and the probabilities assigned to them may serve as building blocks of awareness.

While a consensus exists that (un)awareness affects players' behavior, strategies, and outcomes, the results will heavily depend on how the (un)awareness is modeled and its place in the model. Different proposals exist regarding how (un)awareness affects strategies and payoff. For example, (un)awareness can be directly implemented in a payoff function as a coefficient or a function (for example, as performed by [42,43]), thus moderating the perceived payoff and, with backward induction, the strategies. Nevertheless, such an approach does not reflect the intrinsic and probabilistic aspects of (un)awareness and provides much less opportunity for properties examination. Another possible method is to build (un)awareness as a function that influences the probabilities of strategy choices based on the grasped properties of the opponent's actions. However, that function should be updated after each stage in a dynamic game. The notion of humans as intuitive Bayesian statisticians ([44]) can be helpful. Given that the (un)awareness updating in dynamic games occurs in the same setting, applying Bayes' rule in the game (un)awareness updating is

reasonable. However, such an approach calls for examining the role of previous or common knowledge and game histories. In general, prior knowledge is desirable, especially for the experts. While the previous knowledge of inexperienced managers will be limited, they might rely on publicly available reports, which can be referred to as common knowledge and should serve as a guideline.

This exploration sets the stage for a deeper analysis of game-theory models in enhancing cybersecurity awareness among managers, particularly in SMEs. This paper aims to address the issue of a computable approach to modeling a person's awareness involving awareness about the opponent strategy's properties in a cybersecurity framework. The next section defines a game framework that allows for the further examination of the manager's (un)awareness. The role of a manager's (un)awareness in strategy choices and equilibrium is further analyzed in the following section.

3. Game Setting

This study employs a dynamic game model to analyze the strategic interactions between a manager and a hacker, focusing on the iterative Bayesian updating of beliefs and optimization of current payoffs [44]. This dynamic approach allows us to capture the evolving nature of cybersecurity threats and the corresponding defensive strategies employed by managers in SMEs. A dynamic game model is a mathematical representation of a situation where players (in this context, a manager in the role of defender and a hacker in the role of the attacker) make a sequence of decisions over time. This approach considers the evolving nature of interactions and the impact of previous choices on future decisions.

In this paper, we primarily focus on the actions of black-hat hackers who seek to exploit cybersecurity vulnerabilities for malicious purposes. This approach will allow for the examination of the most pressing cybersecurity challenges faced by SMEs and the development of awareness of defensive strategies that are both effective and feasible for managers with varying levels of cybersecurity expertise [3,4]. However, it is also assumed that the hacker has a type, which, in this case, presumes a form of specialization. As for the manager, the term refers to an employee or an owner in a small- or medium-sized enterprise (SME) who is responsible for making cybersecurity decisions. This role may encompass a range of responsibilities, from a generalist overseeing multiple aspects of business operations and security, including cybersecurity, to a more specialized individual with specific training in IT or cybersecurity management. The framework developed herein does not presuppose advanced cybersecurity expertise, making it applicable to a broad spectrum of managerial roles within SMEs [6]. Managerial awareness refers to the knowledge and understanding that managers have about cybersecurity threats and how these threats can affect their organization. Enhancing managerial awareness involves educating managers about potential cyber risks, attack vectors, and effective countermeasures.

In the game setting, the Instance-Based Learning Theory (IBLT) plays a role in modeling the decision-making processes of players acting as defenders and attackers within a cybersecurity context [19]. This theoretical framework posits that individuals make decisions based on recollections of similar past instances, including the context, actions taken, and outcomes. Starting with prior beliefs, players engage with the game over multiple rounds; they accumulate experiences that enhance common knowledge (for example, from reports on cybersecurity), forming a database of instances in their memory. These data are then retrieved and blended to inform decisions in new yet similar situations.

However, they need at least some elements present to compare the situation to their past experiences. Thus, a rudimentary Intrusion Detection System is presumed to exist, albeit nascent, which serves as a critical tool for the manager [18]. This system continuously monitors network traffic and activities, analyzing them for patterns or anomalies that could indicate malicious intent. By evaluating the data collected by this IDS, the manager can discern insights into the nature and potential strategies of the hacker, which we refer to here as the properties of the hacker's strategy. This information, in turn, shapes the manager's beliefs regarding the hacker's type, specifically the distribution of probabilities over the

hacker's strategies. This integration adds a layer of realism but also underscores the pivotal role of cyber situational awareness in forming strategic defenses against cyber threats.

The game setting is designed to elicit adaptive decision-making behaviors, where the frequency of specific cyber-attack or defense outcomes significantly influences future actions [14,20]. IBLT elucidates how participants adapt their strategies based on the outcomes of their interactions with the game environment and the IDS alerts within the constraints of their cognitive capacities. Integrating IBLT into this game setting aims to capture the dynamic and adaptive nature of human decision-making in the complex and evolving landscape of cybersecurity threats and defenses, providing insights into how cyber situational awareness develops and influences behavior over time.

To address the gap between the theoretical payoff structures and their real-world implications in cybersecurity challenges, it is necessary to contextualize the strategic decisions within the dynamic landscape of cyber threats SMEs face. The model's payoff matrices represent abstract gains and losses and mirror the tangible outcomes of cybersecurity breaches—ranging from financial losses and reputational damage to regulatory penalties [1,6]. In the real world, a defender's choice of strategy, such as investing in advanced security infrastructure (represented by strategy M2) or focusing on employee training to mitigate social engineering attacks (strategy M1), directly impacts the organization's vulnerability and resilience to attacks [3,4]. The payoff for a successful defense (negative payoff for the hacker) encapsulates avoided costs and preserved trust. In contrast, the price of a breach (positive payoff for the hacker) reflects direct and indirect losses. By illustrating how each strategic interaction within the model corresponds to these real-world outcomes, we can better appreciate the practical significance of these theoretical insights.

However, the model of awareness and Bayesian updating stands as a distinctive approach within the landscape of decision-making models, especially when juxtaposed with the frameworks presented in papers by [15,18,19]. Unlike Aggarwal et al. [15], who propose using deception as a strategic countermeasure in cybersecurity, this model emphasizes the dynamic and iterative process of awareness building through Bayesian updating. This process allows managers to refine their strategies based on observed actions and adjust their defense mechanisms in real time, offering a more adaptive response to cybersecurity threats. In contrast to the model in [18], which underscores the importance of cyber situational awareness facilitated by Intrusion Detection Systems (IDSs), this framework delves deeper into the cognitive aspects of decision-making. It captures how managers update their beliefs and strategies based on historical data and the immediate context of cyber threats, aligning closely with the Instance-Based Learning Theory (IBLT) described in [19]. This approach, therefore, complements these existing models by exploring how awareness evolves through Bayesian inference, contributing to the strategic decision-making process in cybersecurity management. This comparison not only situates this work within the existing body of knowledge but also highlights its potential to bridge theoretical insights with practical applications in enhancing cybersecurity defenses.

The insights gained from these studies inform this investigation, underscoring the need for a nuanced understanding of the dynamic interplay between cybersecurity threats and managerial strategies. In a dynamic game between the manager and a hacker,

Let $S_h = \{s_{h1}, \ldots, s_{hn}\}$ denote the strategy set for the hacker,

Let each strategy, s_{h1}, have a set of properties, $\{a_1, b_1, c_1\}$.

Let the manager perceive the hacker's set of strategies according to its general meaning derived through the combination of its properties as subsets:

Let $T \subset S_h$ such that $T = \{s_1, \ldots, s_k\}$.

Let $V \subset S_h$ such that $V = \{s_{k+1}, \ldots, s_l\}$.

Let $Z \subset S_h$ such that $Z = \{s_{l+1}, \ldots, s_n\}$.

And, for simplicity, observe each subset as a single strategy.

The manager is not aware of how the opponent perceives his/her payoff or all available strategies in his/her set, S_h, but guesses that the hacker may choose a strategy, s_{hT} from the subset T, s_{hV} from the subset V, or s_{hZ} from the subset Z.

To offer a relationship to a realistic situation, let us describe the following hacker's strategy subsets and their properties, where, for example, we have the following (simplified):

T refers to social engineering—(*a*) method of attack, exploiting human weaknesses; (*b*) target, individuals; and (*c*) result, data breaches.

V denotes software vulnerabilities exploit—(*a*) method of attack, exploiting technical weaknesses; (*b*) target, a wide range of systems; and (*c*) result, data breach or system damage.

Z denotes DDoS attack—(*a*) method of attack, exploiting compromised devices or systems by flooding with traffic; (*b*) target, a wide range of systems; and (*c*) result, disruption to services.

Strategies in subsets T and V partially share property c, and strategies in subsets V and Z partially share property b. Thus, a strategy subset refers to a group of strategies with common characteristics or objectives. In cybersecurity, subsets might include various types of attacks (e.g., social engineering and software vulnerabilities) or defense mechanisms.

Based on the external security reports, the manager starts with the knowledge of the frequencies of a certain type of attack: F. The manager chooses his/her strategies from a set of strategies: $M = \{M1,\ M2,\ M3\}$.

The game is mainly observed from the manager's perspective. Based on the awareness of the properties of opponent strategies, the manager weighs them and assigns a probability to each strategy. The manager chooses his/her strategy based on the assigned probability of the opponent's strategy and expected payoffs (Table 1). However, the manager also knows that his/her best response to the hacker's choice of strategy T is $M1$, the best response to strategy V is $M2$ and the best response to the hacker's choice of Z is $M3$. Strategies $M1$ and $M2$ share some of the actions, so $M2$ can somewhat counteract attack T, and $M1$ can partially counteract attack V. Similarly, strategies $M2$ and $M3$ overlap in regard to other actions, so strategy $M2$ can somewhat thwart attack Z, and strategy $M3$ can somewhat resist attack Z. The manager chooses strategy $M1$ with probability p'_{M1}, strategy $M2$ with probability p'_{M2}, and strategy $M3$ with probability p'_{M3}.

Table 1. Payoff matrix.

	M1	**M2**	**M3**
T	−c, c	a, b	c, −c
V	a, b	−c, c	a, b
Z	c, −c	a, b	−c, c

Note: $|c| > |b| > |a|$. While properties are denoted in italics, the payoffs are regular font.

The game unfolds as follows. At the beginning of the game, the manager knows publicly available data on cyber-attacks, F. In the first stage, the manager chooses the strategy to counter the most common attack. The hacker chooses one of the available strategies from a strategy set, S_h. Then, the manager observes the properties of the hacker's strategy and assigns a probability of occurrence to each property based on his/her understanding of the detected properties. Then, based on the probabilities assigned to the properties, the manager updates his/her awareness about a taken strategy. Based on the updated awareness, the manager updates the probabilities of choosing his/her strategies in the next stage, aiming for a higher expected payoff. By establishing a comprehensive game-theory framework, we pave the way for a detailed examination of the strategic interactions between managers and hackers.

Small- and medium-sized enterprises (SMEs) exhibit unique characteristics that shape their vulnerability to cyber-attacks and influence the types of attacks they are more likely to encounter than larger corporations. Among these characteristics are limited financial resources, less cybersecurity awareness, and often a lack of dedicated IT and cybersecurity personnel. These constraints mean that SMEs may not have the comprehensive cybersecurity measures typically found in larger organizations, such as advanced Intrusion Detection Systems, regular cybersecurity audits, and employee training programs. Consequently,

SMEs may be more susceptible to various cyber threats, from social engineering and phishing attacks aimed at exploiting human errors to direct attacks on unpatched systems or those without sophisticated defense mechanisms.

Reflecting these realities in our game-theory model required careful consideration of how SMEs' constraints influence their strategic choices and capabilities in responding to cyber threats. In the mathematical formulation of our model, these constraints are represented through the payoff structures and the strategy sets available to the 'manager' in our framework. The limited strategy sets capture the restricted cybersecurity measures available to SMEs. At the same time, the payoff structures are designed to reflect the potentially higher relative impact of successful attacks on SMEs, given their limited resources to absorb such shocks. Furthermore, the model accounts for the dynamic nature of SMEs' cybersecurity awareness and readiness. Through Bayesian updating, the manager's (SME's) awareness of cyber threats evolves based on observed actions and outcomes, modeling the learning process SMEs undergo in real time as they encounter and respond to cyber threats with limited prior cybersecurity knowledge. This modeling approach highlights the specific vulnerabilities of SMEs in the cyber domain and underscores the importance of adaptive strategies in managing cyber risks under resource constraints.

4. Building and Updating Awareness

The intricate relationship between awareness, strategy selection, and payoffs forms the cornerstone of our game-theory approach to cybersecurity management. While awareness may not directly alter the payoff matrix's intrinsic values, it critically shapes the decision-making process, leading to more informed strategy choices that, in turn, significantly influence expected payoffs.

Awareness, in this context, refers to the manager's understanding and recognition of potential cyber threats and the hacker's likely strategies. This comprehension is built upon both historical data and real-time observations, and it is continuously refined through Bayesian updating as the game progresses. Enhanced awareness allows the manager to assign higher probabilities to the strategies he/she believes the hacker is more likely to employ based on previous rounds' observed actions and outcomes.

This probabilistic assessment directly impacts the manager's strategic choices. For example, suppose the manager becomes aware, through Bayesian updating, that a hacker is increasingly employing a particular attack strategy (say, strategy T). In that case, the manager is more likely to choose a defensive strategy (e.g., M1) that is best suited to counteract that threat. This strategic alignment is not static but dynamically evolves with the manager's growing awareness and understanding of the threat landscape.

The selection of a well-aligned strategy, informed by updated awareness, indirectly affects the game's payoffs. A strategic choice that effectively counters the hacker's actions can mitigate potential losses, preserve the integrity of digital assets, and maintain organizational reputation. Thus, while awareness does not change the payoffs associated with each strategy combination directly, as there are always objective consequences and payoffs regardless of how a person is aware of them ([20,33]), it influences the likelihood of achieving more favorable outcomes by guiding the manager toward more effective defensive strategies. Moreover, this relationship highlights the game's adaptive nature, where the manager and the hacker are engaged in a continuous loop of action, observation, learning, and strategy adjustment. The manager's ability to update his/her awareness and strategically respond to the evolving cyber threat environment underscores the pivotal role of cognitive and informational elements in shaping strategic outcomes in cybersecurity management. Therefore, awareness is a critical intermediary that links information acquisition and processing to strategic decision-making, indirectly influencing the game's payoffs.

Initially, the manager first assigns probabilities about properties of the subset based on rudimentary Intrusion Detection Systems' data:

$$p_{Ta}(t),\ p_{Tb}(t),\ p_{Tc}(t),$$

$$p_{Va}(t),\ p_{Vb}(t),\ p_{Vc}(t),$$
$$p_{Za}(t),\ p_{Zb}(t),\ p_{Zc}(t).$$

At this point, it is important to recall that different attack strategies share some of the properties. If the hacker chooses strategy T, the manager observes properties $p_{Ta}(t),\ p_{Tb}(t),\ p_{Tc}(t)$ and assigns them a probability in the interval [0.5, 1] each, while the sum of assigned probabilities to the same property of other strategies is, for example, $p_{Va}(t) + p_{Za}(t) = 1 - p_{Ta}(t)$. The probabilities assigned to other properties' occurrence, $p_{Vb}(t),\ p_{Vc}(t),\ p_{Zb}(t),\ p_{Zc}(t)$, is assigned similarly. However, if the hacker chooses strategy V, then the manager assigns probabilities in the interval [0.5, 1] to $p_{Va}(t),\ p_{Vb}(t),\ p_{Vc}(t)$, and the rest of the beliefs of the properties' occurrence is calculated similarly to the first case. Since T and V may have similar properties of their attack method, the manager could, for example, imperfectly assign a probability of 0.51 to $p_{Ta}(t)$, and 0.49 to $p_{Va}(t)$, creating a high ambiguity. Therefore, this observation serves only as a first step and requires further assessment.

These probabilities denote the manager's awareness of the detected properties and are updated at each stage. Suppose the manager's awareness update functions describe the manager's reflection on the common knowledge, F, about the frequencies of a certain type of attack, the manager's awareness in time $(t-1)$, and the hacker's strategies in time $(t-1)$.

To model awareness update functions, we use Bayesian updating, building on [44]. It is a statistical method that updates the probability as more evidence or information becomes available. Let $M_{(t-1)}$ denote the manager's awareness and $H_{(t-1)}$ denote the hacker's strategies at the time $(t-1)$. Let F denote the frequencies of a certain type of attack in the past that is common knowledge between the manager and the hacker. Let $p(T|H_{(t-1)})$ denote the probability that the hacker will choose a strategy from subset T given his/her strategies at the time $(t-1)$, and let $p(a|T, H_{(t-1)})$ denote the probability of property a being present in a strategy from subset T given the hacker's strategies at the time $(t-1)$. Similarly, we define $p(V|H_{(t-1)})$, $p(Z|H_{(t-1)})$, $p(b|T, H_{(t-1)})$, $p(c|T, H_{(t-1)})$, and so on for the other properties and subsets.

The manager's awareness update functions can then be defined as follows. To calculate $p(T_a|T, M_{(t-1)}, H_{(t-1)}, F)$, we use Bayes' rule:

$$p_{Ta}(t) = p(T_a|T, M_{(t-1)}, H_{(t-1)}, F) = \frac{p(a|T,H_{(t-1)})\cdot p(T|M_{(t-1)},H_{(t-1)},F)}{p(a|T,H_{(t-1)})\cdot p(T|M_{(t-1)},H_{(t-1)},F)+p(a|V,H_{(t-1)})\cdot p(V|M_{(t-1)},H_{(t-1)},F)+p(a|Z,H_{(t-1)})\cdot p(Z|M_{(t-1)},H_{(t-1)},F)} \quad (1)$$

where $p(a|T, H_{(t-1)})$ is the probability of the property a being observed given that the hacker chose subset T and the manager observed history, $H_{(t-1)}$, $p(T|M_{(t-1)}, H_{(t-1)}, F)$, is the probability of the hacker choosing subset T given that the manager chose action $M_{(t-1)}$ and has full awareness of prior attack frequencies, F; and $p(T_b|T, M_{(t-1)}, H_{(t-1)}, F)$ and $p(T_c|T, M_{(t-1)}, H_{(t-1)}, F)$ are defined similarly.

To calculate $p(V_a|V, M_{(t-1)}, H_{(t-1)}, F)$ and $p(Z_a|Z, M_{(t-1)}, H_{(t-1)}, F)$, we use the same approach:

$$p_{Va}(t) = p(V_a|V, M_{(t-1)}, H_{(t-1)}, F) = \frac{p(a|V,H_{(t-1)})\cdot p(V|M_{(t-1)},H_{(t-1)},F)}{p(a|T,H_{(t-1)})\cdot p(T|M_{(t-1)},H_{(t-1)},F)+p(a|V,H_{(t-1)})\cdot p(V|M_{(t-1)},H_{(t-1)},F)+p(a|Z,H_{(t-1)})\cdot p(Z|M_{(t-1)},H_{(t-1)},F)} \quad (2)$$

$$p_{Za}(t) = p(Z_a|Z, M_{(t-1)}, H_{(t-1)}, F) = \frac{p(a|Z,H_{(t-1)})\cdot p(Z|M_{(t-1)},H_{(t-1)},F)}{p(a|T,H_{(t-1)})\cdot p(T|M_{(t-1)},H_{(t-1)},F)+p(a|V,H_{(t-1)})\cdot p(V|M_{(t-1)},H_{(t-1)},F)+p(a|Z,H_{(t-1)})\cdot p(Z|M_{(t-1)},H_{(t-1)},F)} \quad (3)$$

And $p(V_b|T, M_{(t-1)}, H_{(t-1)}, F)$, $p(V_c|T, M_{(t-1)}, H_{(t-1)}, F)$, $p(Z_b|T, M_{(t-1)}, H_{(t-1)}, F)$, and $p(Z_c|T, M_{(t-1)}, H_{(t-1)}, F)$ are defined similarly.

While it is assumed that the manager is rational, the manager's perception of the properties does not have to be perfect. Moreover, this approach allows for partial awareness [26]. The manager assigns the probability that a certain property occurred and belongs to a specific strategy, allowing uncertainty about the property or a strategy and even a misjudgment in the early stages of a game. As the manager's knowledge of the game's history builds over the stages, a misjudgment is less likely to occur. This setting mimics life-like situations, allowing for learning and gaining awareness during the game.

It is worth noting that if one would like to add some noise in the update function to depict a human error, bias, or heuristic, small random numbers could be added to each probability derived as the output from the applied Bayes' rule. While such an approach may offer interesting insights, it might also make the game unsolvable and the behavior unpredictable.

By combining the updates based on the perceived properties described in (1)–(3), we obtain the following:

$$p(T|H_{(t-1)}) = \frac{p_{Ta}(t) + p_{Tb}(t) + p_{Tc}(t)}{p_{Ta}(t) + p_{Tb}(t) + p_{Tc}(t) + p_{Va}(t) + p_{Vb}(t) + p_{Vc}(t) + p_{Za}(t) + p_{Zb}(t) + p_{Zc}(t)} \tag{4}$$

$$p(V|H_{(t-1)}) = \frac{p_{Va}(t) + p_{Vb}(t) + p_{Vc}(t)}{p_{Ta}(t) + p_{Tb}(t) + p_{Tc}(t) + p_{Va}(t) + p_{Vb}(t) + p_{Vc}(t) + p_{Za}(t) + p_{Zb}(t) + p_{Zc}(t)} \tag{5}$$

$$p(Z|H_{(t-1)}) = \frac{p_{Za}(t) + p_{Zb}(t) + p_{Zc}(t)}{p_{Ta}(t) + p_{Tb}(t) + p_{Tc}(t) + p_{Va}(t) + p_{Vb}(t) + p_{Vc}(t) + p_{Za}(t) + p_{Zb}(t) + p_{Zc}(t)} \tag{6}$$

Equations (4)–(6) mimic the guessing of the strategies played based on the observed properties. For example, suppose most observed properties are assigned to strategy T. In that case, the ratio of the probabilities assigned to those properties (the numerator in 4) and the probabilities assigned to all properties belonging to all strategies (the denominator in 4) will be the highest, and the manager assesses that it is most likely that the hacker played strategy T. However, while such an update directs the awareness toward one subset of the hacker's strategies, signaling his/her type (assuming the hacker's specialization in a kind of attack vector), a further update involves knowledge about frequencies of all attack types. That allows for the assumption that one subset of the hacker's available strategies may be most likely without disregarding the other subsets.

The update of the probability of choosing strategy $M1$ in time t (which is the best response to the hacker's choice of strategy T from subset S_{t-1}) comprises previous knowledge about frequencies of the attack types, the hacker's strategy chosen at the previous stage, and awareness about the likelihood that strategy T has been selected (4) based on the perceived properties:

$$\begin{aligned} p_{M1}(t) &= p(M1|M_t, H_{t-1}, F) = p(T|S_{t-1}, H_{t-1}, F) \\ &= \frac{p(T|H_{t-1}) \cdot p(F|T, M_{t-1})}{\Sigma a' \; p(a'|T, H_{t-1}) \cdot p(T|H_{t-1}) \cdot p(F|T, M_{t-1}) + \Sigma b' \; p(b'|T, H_{t-1}) \cdot p(T|H_{t-1}) \cdot p(F|T, M_{t-1}) + \Sigma c' \; p(c'|T, H_{t-1}) \cdot p(T|H_{t-1}) \cdot p(F|T, M_{t-1})} \end{aligned} \tag{7}$$

The update is similarly defined for $p_{M2}(t)$ and $p_{M3}(t)$:

$$\begin{aligned} p_{M2}(t) &= p(M2|M_t, H_{t-1}, F) = p(V|S_{t-1}, H_{t-1}, F) \\ &= \frac{p(V|H_{t-1}) \cdot p(F|V, M_{t-1})}{\Sigma a' \; p(a'|V, H_{t-1}) \cdot p(V|H_{t-1}) \cdot p(F|V, M_{t-1}) + \Sigma b' p(b'|V, H_{t-1}) \cdot p(V|H_{t-1}) \cdot p(F|V, M_{t-1}) + \Sigma c' \; p(c'|V, H_{t-1}) \cdot p(V|H_{t-1}) \cdot p(F|V, M_{t-1})} \end{aligned} \tag{8}$$

$$\begin{aligned} p_{M3}(t) &= p(M3|M_t, H_{t-1}, F) = p(Z|S_{t-1}, H_{t-1}, F) \\ &= \frac{p(Z|H_{t-1}) \cdot p(F|Z, M_{t-1})}{\Sigma a' p(a'|Z, H_{t-1}) \cdot p(Z|H_{t-1}) \cdot p(F|Z, M_{t-1}) + \Sigma b' \; p(b'|Z, H_{t-1}) \cdot p(Z|H_{t-1}) \cdot p(F|Z, M_{t-1}) + \Sigma c' \; p(c'|Z, H_{t-1}) \cdot p(Z|H_{t-1}) \cdot p(F|Z, M_{t-1})} \end{aligned} \tag{9}$$

where $\Sigma a'$, $\Sigma b'$, and $\Sigma c'$ denote the sum over all possible values of properties a, b, and c, respectively. F represents the frequencies of a certain type of attack in the past that is common knowledge between the manager and the hacker, estimated based on public reports. The final update reflects a manager's belief about the subset of strategies that the

hacker used. While this resembles the notion of guessing the hacker's type, a hacker might be versatile and mix the applied strategy over the stages.

Equations (7)–(9) further update the probabilities of the manager's strategy. In that sense, the manager uses his/her updated awareness about the opponent's strategy and extends its meaning to his/her choice of strategy in the next stage. These functions update the manager's awareness about the hacker's strategy and properties based on the previous awareness, the frequencies of the attack, and the hacker's strategy at the last stage. The manager can then use his/her updated awareness to assign probabilities to each strategy and choose his/her strategy based on expected payoffs.

Including F in the manager's awareness update functions allows the manager to incorporate his/her knowledge of the past frequency of attacks into his/her current beliefs about the hacker's strategies and properties. It also denotes the minimal awareness that an attack is possible. This can be particularly important when the manager's prior beliefs may be biased or incomplete, and the past frequency of attacks provides additional information to update the manager's beliefs. This is also important at the initial stages of the game, especially if the manager does not have prior experience with cybersecurity. However, it can be noticed that F will skew the manager's probabilities of choosing strategies toward the one that counters the most common type of attack and might hinder his/her ability to adapt the strategies promptly. This detailed approach to modeling awareness provides a foundation for exploring the effectiveness of different managerial strategies in the face of evolving cybersecurity threats.

5. Reasoning about Strategies

First, we need to determine the probability that the hacker will choose a strategy from each of the subsets, T, V, and Z, given the manager's awareness at time t. We can use Bayesian updating to update the manager's awareness at each stage of the game based on his/her observations.

Let $p_T(t)$, $p_V(t)$, and $p_Z(t)$ denote the probabilities that the hacker will choose a strategy from subsets T, V, and Z, respectively, at time t, given the manager's strategy at time $t-1$. Then, we have the following:

$$p_T(t) = p(T|H_{(t-1)}, M_{(t-1)}, F) = \frac{p(T|H_{(t-1)}))\cdot p(M_{(t-1)}.|T)\cdot p(F)}{\Sigma T' p(T'|H_{(t-1)}))\cdot p(M_{(t-1)}.|T')\cdot p(F)} \tag{10}$$

where $p(T|H_{(t-1)}))$ is the probability that the hacker will choose a strategy from subset T given his/her strategies at the time $t-1$, $(p(M_{(t-1)})|T).$ is the probability that the manager will chose strategy M_1 given the hacker's choice of subset T at time $t-1$, and $p(F)$ is the probability of observing the frequencies of a certain type of attack in the past.

Similarly, we can define the probabilities $p_V(t)$ and $p_Z(t)$ as follows:

$$p_V(t) = p(V|H_{(t-1)}, M_{(t-1)}, F) = \frac{p(V|H_{(t-1)}))\cdot p(M_{(t-1)}.|V)\cdot p(F)}{\Sigma V' p(V'|H_{(t-1)}))\cdot p(M_{(t-1)}.|V')\cdot p(F)} \tag{11}$$

$$p_Z(t) = p(Z|H_{(t-1)}, M_{(t-1)}, F) = \frac{p(Z|H_{(t-1)}))\cdot p(M_{(t-1)}.|Z)\cdot p(F)}{\Sigma Z' p(Z'|H_{(t-1)}))\cdot p(M_{(t-1)}.|Z')\cdot p(F)} \tag{12}$$

Additional reasoning about the strategies is introduced to add to the heuristic approach to model the manager's choices. The update is further governed by reasoning about the manager's strategies, implying a set of rules based on the assumption that strategies in subsets T and V partially share property c, and strategies in subsets V and Z partially share property b, as well as the overlaps in the corresponding manager's best responses. That reasoning results in probabilities p'_{M1}, p'_{M2}, and p'_{M3}, such that we can observe the following:

If $p_{Ta} > p_{Va}$ and $p_{Ta} > p_{Za}$ and $p_{Tb} > p_{Vb}$ and $p_{Tb} > p_{Zb}$ and $p_{Tc} \geq p_{Vc}$ and $p_{Tc} > p_{Zc}$, then the manager chooses strategy $M1$ with probability $p'_{M1} = 1$.

If $p_{Va} > p_{Ta}$ and $p_{Va} > p_{Za}$ and $p_{Vb} > p_{Tb}$ and $p_{Vb} \geq p_{Zb}$ and $p_{Vc} \geq p_{Tc}$ and $p_{Vc} > p_{Zc}$, then the manager chooses strategy $M2$ with probability $p'_{M2} = 1$.

If $p_{Za} > p_{Ta}$ and $p_{Za} > p_{Va}$ and $p_{Zb} > p_{Tb}$ and $p_{Zb} \geq p_{Vb}$ and $p_{Zc} > p_{Tc}$ and $p_{Zc} > p_{Vc}$, then the manager chooses strategy $M3$ with probability $p'_{M3} = 1$.

If $p_{Ta} > p_{Za}$ and $p_{Va} \geq p_{Za}$ and $p_{Tb} \geq p_{Zb}$ and $p_{Vb} \geq p_{Zb}$ and $p_{Tc} \geq p_{Zc}$ and $p_{Vc} \geq p_{Zc}$, then the manager chooses between strategies $M1$ and $M2$ with assigned probabilities $p'_{M1}(t) = \frac{p_{M1}(t)}{p_{M1}(t)+p_{M2}(t)}$ and $p'_{M2}(t) = \frac{p_{M2}(t)}{p_{M1}(t)+p_{M2}(t)}$.

If $p_{Ta} > p_{Va}$ and $p_{Za} \geq p_{Va}$ and $p_{Tb} \geq p_{Vb}$ and $p_{Zb} \geq p_{Vb}$ and $p_{Tc} \geq p_{Vc}$ and $p_{Zc} \geq p_{Vc}$, then the manager chooses between strategies M1 and M3 with assigned probabilities $p'_{M1}(t) = \frac{p_{M1}(t)}{p_{M1}(t)+p_{M3}(t)}$ and $p'_{M3}(t) = \frac{p_{M3}(t)}{p_{M1}(t)+p_{M3}(t)}$.

If $p_{Va} > p_{Ta}$ and $p_{Za} \geq p_{Ta}$ and $p_{Vb} \geq p_{Tb}$ and $p_{Zb} \geq p_{Tb}$ and $p_{Vc} \geq p_{Tc}$ and $p_{Zc} \geq p_{Tc}$, then the manager chooses between strategies M2 and M3 with assigned probabilities $p'_{M2}(t) = \frac{p_{M2}(t)}{p_{M2}(t)+p_{M3}(t)}$ and $p'_{M3}(t) = \frac{p_{M3}(t)}{p_{M2}(t)+p_{M3}(t)}$.

Based on the updated probabilities, the manager chooses strategies:

$p'_{M1} = 1$ if $p_{Ta} > p_{Va}$ and $p_{Ta} > p_{Za}$ and $p_{Tb} > p_{Vb}$ and $p_{Tb} > p_{Zb}$ and $p_{Tc} \geq p_{Vc}$ and $p_{Tc} > p_{Zc}$, or else 0.

$p'_{M2} = 1$ if $p_{Va} > p_{Ta}$ and $p_{Va} > p_{Za}$ and $p_{Vb} > p_{Tb}$ and $p_{Vb} \geq p_{Zb}$ and $p_{Vc} \geq p_{Tc}$ and $p_{Vc} > p_{Zc}$, or else 0

$p'_{M3} = 1$ if $p_{Za} > p_{Ta}$ and $p_{Za} > p_{Va}$ and $p_{Zb} > p_{Tb}$ and $p_{Zb} \geq p_{Vb}$ and $p_{Zc} > p_{Tc}$ and $p_{Zc} > p_{Vc}$, or else 0.

The manager's expected payoff for each strategy can be calculated as follows:

$$E(M_1) = p_T(t)\cdot \mathrm{c} + p_V(t)\cdot \mathrm{b} - p_z(t)\cdot \mathrm{c} \tag{13}$$

$$E(M_2) = p_T(t)\cdot \mathrm{b} + p_V(t)\cdot \mathrm{c} + p_Z(t)\cdot \mathrm{b} \tag{14}$$

$$E(M_3) = -p_T(t)\cdot \mathrm{c} + p_Z(t)\cdot \mathrm{b} + p_Z(t)\cdot \mathrm{c} \tag{15}$$

where the probability of the hacker's strategy belonging to subset T is p_T, to subset V is p_V, and to subset Z is p_Z. However, it can be noticed that the manager's reasoning is primarily governed by his/her awareness and reasoning that involves the rules that lead to a higher payoff, but not the expected payoff itself, thus mimicking the unawareness of the payoff. However, the manager must be sensitive to a loss and react to it. In addition, let us assume the manager's reflective awareness about the relevance of prior frequencies in his/her probability assignment and his/her control over his/her beliefs. If the manager did not win at time $(t-1)$, he/she should rethink the prior probabilities and set them to 0.5 in the next stage (thus allowing for maximum uncertainty and loosely mimicking the effect of time [15–17]).

The expected payoff of the hacker for each subset of strategies is as follows:

$$E(T) = -p'_{M1}(\mathrm{t})\cdot \mathrm{c} + p'_{M2}(\mathrm{t})\cdot \mathrm{a} + p'_{M3}(\mathrm{t})\cdot \mathrm{c} \tag{16}$$

$$E(V) = p'_{M1}(\mathrm{t})\cdot a - p'_{M2}(\mathrm{t})\cdot \mathrm{c} + p'_{M3}(\mathrm{t})\cdot \mathrm{a} \tag{17}$$

$$E(Z) = p'_{M1}(\mathrm{t})\cdot \mathrm{c} + p'_{M2}(\mathrm{t})\cdot \mathrm{a} - p'_{M3}(\mathrm{t})\cdot \mathrm{c} \tag{18}$$

where p'_{M1}, p'_{M2}, and p'_{M3}, are the probabilities that the manager will choose strategies $M1$, $M2$, and $M3$, respectively.

To maximize their expected payoff, the manager should assign probabilities as follows:

$p'_{M1} = 1$ if $p_{Ta} > p_{Va}$ and $p_{Ta} > p_{Za}$ and $p_{Tb} > p_{Vb}$ and $p_{Tb} > p_{Zb}$ and $p_{Tc} \geq p_{Vc}$ and $p_{Tc} > p_{Zc}$ or if $E(M1)_{t-1}$ is the highest, or else 0.

$p'_{M2} = 1$ if $p_{Va} > p_{Ta}$ or if $p_{Va} > p_{Za}$ and $p_{Vb} > p_{Tb}$ and $p_{Vb} \geq p_{Zb}$ and $p_{Vc} \geq p_{Tc}$ and $p_{Vc} > p_{Zc}$ and if $E(M2)_{t-1}$ is the highest, or else 0.

$p'_{M3} = 1$ if $p_{Za} > p_{Ta}$ and $p_{Za} > p_{Va}$ and $p_{Zb} > p_{Tb}$ and $p_{Zb} \geq p_{Vb}$ and $p_{Zc} > p_{Tc}$ and $p_{Zc} > p_{Vc}$ or if $E(M3)_{t-1}$ is the highest, or else 0.

The strategic considerations discussed here are instrumental in developing a robust defense mechanism, guiding managers in SMEs to make informed decisions based on updated awareness and strategic reasoning.

6. The Role of (Un)Awareness in Equilibrium

The game can be analyzed using the best-response strategies, equilibrium analysis, and sequential decision-making. An equilibrium analysis examines stable states in a game where no player can benefit by changing his/her strategy, while the other players keep theirs unchanged. Identifying equilibrium helps predict the likely outcomes of strategic interactions. Conversely, sequential decision-making refers to making decisions one after another, where each decision may depend on the outcome of previous decisions. In cybersecurity management, this involves adapting defenses based on the evolving threat landscape and past attack experiences.

Stage 1: The manager chooses the strategy to counter the most common attack. In this stage, the manager's best response is to choose $M1$ if the hacker's strategy belongs to subset T, $M2$ if it belongs to subset V, and $M3$ if it belongs to subset Z. To maximize his/her expected payoff, the manager should assign probabilities as described in the previous chapter.

Stage t (t > 1): The manager updates his/her awareness based on the observed properties and chooses a strategy. In this stage, the manager updates his/her awareness by calculating the probabilities, $p(T)$, $p(V)$, and $p(Z)$, based on the observed properties, using Equations (1)–(3). Using the updated probabilities, the manager then updates the probabilities assigned to their strategies, $p_{M1(t)}$, $p_{M2(t)}$, and $p_{M3(t)}$, based on the updated awareness and past frequencies, F (Equations (4)–(6)).

The manager's expected payoffs for each strategy at this stage are the same as in Stage 1, but with the updated probabilities, $p(T)$, $p(V)$, and $p(Z)$; and the updated probabilities, $p'_{M1}(t)$, $p'_{M2}(t)$, and $p'_{M3}(t)$ (13)–(15). The manager then chooses the strategy with the highest expected payoff and continues to the next stage.

Repeat Stage t until convergence or a maximum number of iterations. The manager repeats Stage t, updating his/her awareness and probabilities and choosing strategies based on expected payoffs until a convergence point or a maximum number of iterations is reached. Convergence can be defined based on a predetermined threshold for the differences between consecutive iterations or by reaching a stable set of probabilities. Nevertheless, the manager's goal is anticipating the hacker's behavior and successful defense, implying that meaningful convergence occurs only when the manager's awareness of the hacker's strategies distribution aligns with the hacker's strategies distribution.

Suppose we disregard the reasoning about the strategies by iteratively updating their awareness and strategy. In that case, the manager should reach a perfect Bayes equilibrium, where the manager's strategy maximizes his/her expected payoff, given the probabilities assigned to the hacker's strategies and the observed properties. This equilibrium allows the manager to make informed decisions based on the available information and the historical frequencies of different strategies and outcomes. If the probabilities reach a convergence, it can be written in Bayes' perfect equilibrium formula:

$$(M^*, S^*) = argmax_{M,T} p(M, \mathrm{S}|H_{(t-1)}, F) / \Big[p(M|T, H_{(t-1)}, F) + p(M|V, H_{(t-1)}, F) + p(M|Z, H_{(t-1)}, F)\Big] \quad (19)$$

where $p(M, S|H_{(t-1)}, F)$ is the joint probability of the manager's action and the hacker's subset being chosen given the history, $H_{(t-1)}$, and the awareness of the prior frequencies of attacks, F; and $p(M|T, H_{(t-1)}, F)$ is the probability of the manager choosing action M given that the hacker chose subset T and the manager-observed history, $H_{(t-1)}$, with prior knowledge, F. Moreover, $p(M|V, H_{(t-1)}, F)$ and $p(M|Z, H_{(t-1)}, F)$ are defined similarly.

The role of the manager's awareness in the solution is to affect the conditional probabilities, $p(M|T, H_{(t-1)}, F)$, $p(M|V, H_{(t-1)}, F)$, and $p(M|Z, H_{(t-1)}, F)$, which govern the probability of the manager choosing action M given that the hacker chose subset T, V, or Z, respectively. The manager's observed history, $H_{(t-1)}$, leads to gaining full awareness. Until

reaching full awareness, the manager makes decisions based on his/her best guess about the situation. That best guess will be determined by the manager's prior experience (or lack thereof) or the common knowledge (public reports) he/she relies on initially. Moreover, the manager can quickly reach convergence if the observed hacker chooses the most common attack vector repeatedly. However, in any other case, learning and gaining awareness will take more time.

The manager's awareness depends on the perceived properties of the attack. To become aware of the attack, the manager should recognize and identify its properties and assign those properties to the correct hacker's strategy. The manager may misjudge a property or a strategy, especially in the game's early stages, leading to slower convergence and more stages with a loss as a payoff.

The manager's awareness update affects these probabilities because it changes the manager's perception of the likelihood of each subset being chosen by the hacker based on past experiences or knowledge. Therefore, the manager's awareness can impact the manager's strategy by changing the relative weights assigned to each possible action based on their perceived effectiveness against each subset.

The mathematical modeling constructs a dynamic game between a manager and a hacker, incorporating the concept of (un)awareness and iterative Bayesian updating to simulate the manager's evolving awareness of cybersecurity threats. Through this analysis, the pivotal role of awareness in achieving equilibrium is demonstrated, offering valuable insights into the development of adaptive and effective cybersecurity strategies.

7. Algorithm for Strategic Interaction Simulation

Based on the theoretical framework and the game complexity, the Bayesian awareness updating is further assessed through the simulation. The objective is to simulate the decision-making process of a hacker and a manager over a series of interactions, incorporating strategy updates based on observed outcomes. Notation is available in Appendix A, and an outline of the simulation process is presented in Figure 2.

The simulation outlined in Figure 2 unfolds as follows:

Initialization
Input:
Number of simulation rounds, T; initial frequencies; and probabilities.
Define the players and strategies:
Players: $P = \{Hacker, Manager\}$;
Hacker's strategies: $S = \{T, V, Z\}$;
Manager's strategies: $M = \{M_1, M_2, M_3\}$;
Payoff matrices: hacker's payoff, $U_H(S, M)$; manager's payoff, $U_M(S, M)$.

- Initial strategy probabilities:
  - Hacker's strategy probabilities: $P_H = \{p_{HT}, p_{HV}, p_{HZ}\}$;
  - Manager's strategy probabilities: $P_M = \{p_{M1}, p_{M2}, p_{M3}\}$.
- Historical data initialization:
  - Historical frequencies of attack types: $F = \{F_T, F_V, F_Z\}$;
  - Probabilities of hacker's choices based on hacker's type: $H = \{H_T, H_V, H_Z\}$.
- Variables for tracking frequencies:
  - Frequencies of strategies: $F_S = \{\frac{\sum_{k=1}^{t} T}{t}, \frac{\sum_{k=1}^{t} V}{t}, \frac{\sum_{k=1}^{t} Z}{t}, t\}$;
  - Outcomes tracking: $O = \{\frac{O_H(t)}{\max O}, \frac{O_M(t)}{\max O}, \mathrm{t}\}$;
  - Simulation loop (for each iteration t from 1 to T):

    Hacker strategy probability determination:

    - Calculate the hacker's strategy probabilities based on the initial hacker's strategy probabilities.

    Hacker strategy choice:

- Selection based on max probability: $S_t = argmax P_{H(t)}$.

Property observation probability update (awareness update):

- Updated probabilities, $P_{obs}(S, M)$ based on $P_H(t)$ and $P_M(t)$; for each property p in S: $P_{obs}(p|S_t, M) = f(P_H(t, S_t), P_M(t, M))$.

Manager strategy probability update:

- Update based on observed properties, historical data, and outcome of the previous round: $P_M(t+1, M) = g(P_{obs}(p \mid S_t, M), F(S), H(S))$.

Manager strategy choice:

- Selection based on max probability: $M_t = argmax P_M(t+1)$.

Payoff calculation:

- $U_H(S_t, M_t) = Lookup(U_H, S_t, M_t)$.
- $U_M(S_t, M_t) = Lookup(U_M, S_t, M_t)$.

Frequency and history update:

- Update historical frequencies for strategies and types of attacks: $F_S(S_t) + 1$, $O(U_H, U_M) = O(U_H, U_M) + 1$.
- Update the historical frequency of the manager's strategies.

Awareness and strategy correction:

- Adjust probabilities if the payoff is below a certain threshold. That is, if $U_M(S_t, M_t) < threshold_M$, adjust P_M accordingly.

Store iteration results:

- Store $S_t, M_t, U_H, U_M, P_{H(t+1)}, P_{M(t+1)}$ for analysis.

Loop continuation check:
If 'I' is less than 'T', then t = t + 1 and repeat steps in 2.

After loop completion:
Output: A data frame containing the results of each round.

- Collect and format the simulation results from all iterations for analysis.

End of algorithm.

The simulation algorithm outlined here eases our understanding of the complex dynamics and awareness evolution in the interplay of cybersecurity threats and defenses. It bridges theoretical models with real-world applicability and allows for examinations of different settings.

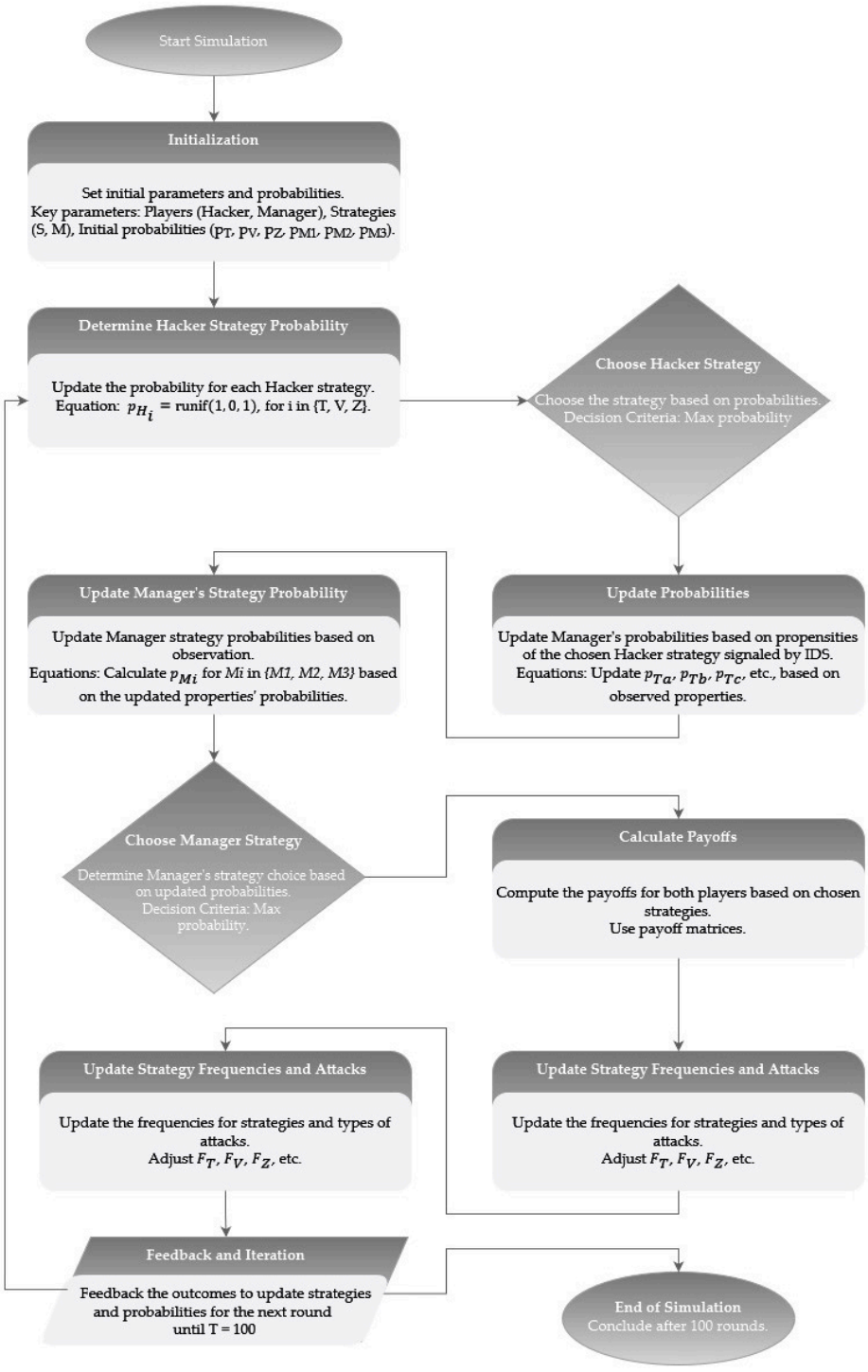

Figure 2. Simulation-process diagram. Note: The diagram was created using drawio.com.

7.1. An Example of a Use-Case Scenario

To illustrate the application of the game-theory approach in a cybersecurity context, consider the following hypothetical scenario involving a small company specializing in cloud-based services for small businesses. The company has recently expanded its customer base and holds sensitive data in its cloud storage. The company has a basic cybersecurity infrastructure but lacks a dedicated cybersecurity team. The manager is aware of the cybersecurity threats but has limited knowledge of anticipating or responding to sophisticated cyber-attacks.

One Monday morning, the manager receives an alert from their rudimentary Intrusion Detection System (IDS) about unusual email activities. The manager recalls the game-theory framework for cybersecurity decision-making introduced in the company's recent cybersecurity-awareness training.

The manager reviews the historical data on cyber-attacks and notices that phishing attacks (T) have been the most common, followed by software-vulnerability exploits (V) and DDoS attacks (Z). This prior information forms the basis for the manager's initial strategy probabilities.

Using the Bayesian updating approach, the manager considers the properties of the unusual email activities, such as suspicious attachments and links, which are indicative of a phishing attack (strategy T in the model), and assigns the highest probability to the hacker's strategy T. Based on the Bayesian updating model, the manager recalculates the probabilities of facing each type of cyber-attack. Given the current alert and historical data, the likelihood of a phishing attack is deemed highest. The manager decides that implementing stricter email filtering and enhancing employee awareness (strategy M1) make for the best immediate response.

The manager initiates a quick cybersecurity briefing for all employees, emphasizing the signs of phishing emails and the importance of not clicking on unknown links or attachments. Simultaneously, the manager updates the email filtering rules to catch and quarantine suspicious emails.

Over the next few days, the manager monitors the situation closely. The number of suspicious email activities decreases significantly, indicating that the phishing attack has been successfully mitigated. Based on this successful outcome, the manager updates the company's cybersecurity strategy probabilities, enhancing the company's preparedness for future attacks.

This use-case scenario demonstrates how a small company without a dedicated cybersecurity team can apply a game-theory framework to make informed decisions and effectively respond to cybersecurity threats. By incorporating Bayesian updating, the company can dynamically adjust its strategies based on evolving threats and historical data, enhancing its cybersecurity posture over time.

7.2. Simulation Data Generation and Assumptions

The dataset for our simulations was generated synthetically to explore the strategic interactions between managers and hackers within the game-theory framework established in this study. This approach allowed us to create a controlled environment where the impact of various strategies and awareness levels could be systematically analyzed.

The primary real-world information integrated into our simulations was the shares of different types of attacks, as referenced from the CERT annual report 2022 [45]. This empirical grounding provided a realistic backdrop against the strategic interactions between hypothetical managers and hackers. Each simulated interaction was predicated on a set of assumptions reflective of real-world cybersecurity management scenarios and awareness: managers and hackers choose from a finite set of strategies, with the effectiveness of each managerial strategy varying according to the assessed type of attack employed by the hacker. The evolution of managerial awareness and strategic adaptation was modeled using Bayesian updating, based on the observed outcomes of interactions and informed by the initial attack type shares from the referenced report.

The simulation environment was custom designed to facilitate this complex interplay of strategies, outcomes, and learning processes, ensuring a rigorous yet flexible framework for analyzing our study's theoretical propositions. The simulation environment parameters, including the number of rounds and the impact of different strategies on payoffs, were chosen based on the literature to ensure a balance between realism and analytical tractability. The results are then compared to similar theoretical models and case studies.

8. Results and Discussion

8.1. Different Hacker Types

The awareness update is imperfect because the inexperienced manager updates his/her initial probabilities roughly, considering only the game history and prior frequencies. This is enough when the hacker's type (or strategy choices, i.e., his/her specialization) aligns with the initial frequencies and game history (the hacker's choices are consistent). That can be seen in the first two graphs in Figure 3.

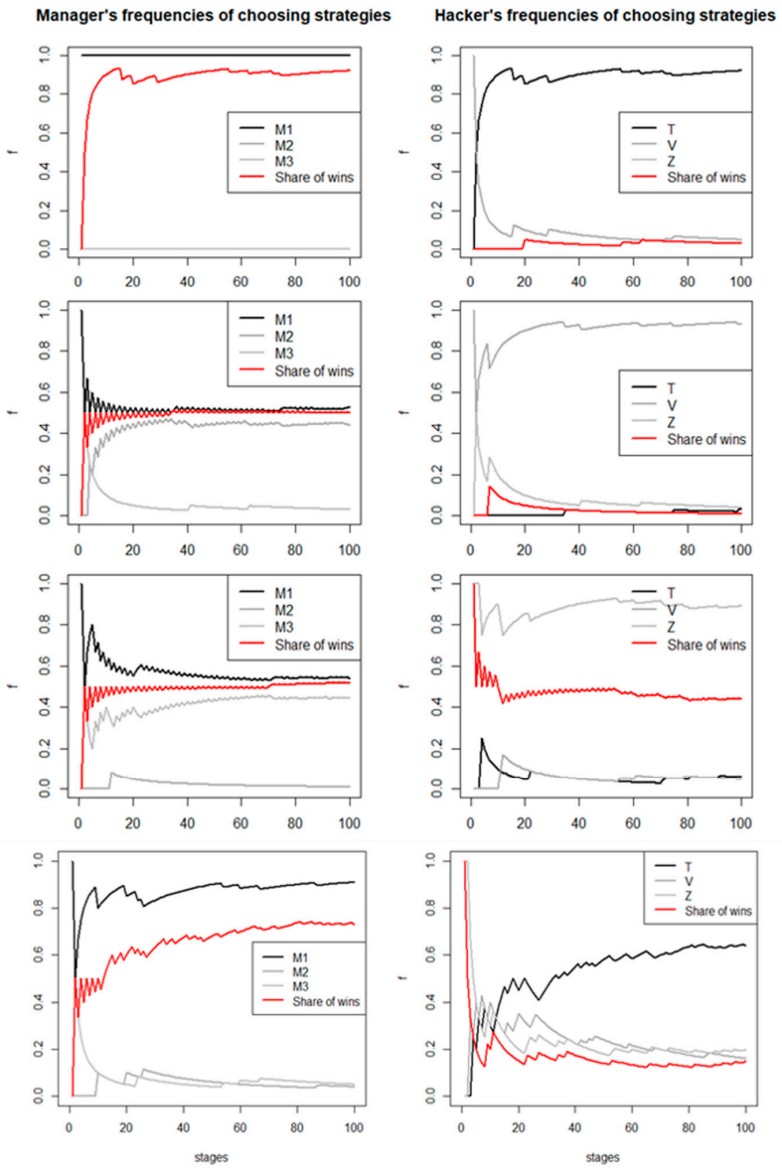

Figure 3. Manager's (**left**) and hacker's (**right**) frequencies of choosing strategies and shares of wins with different hacker types. Notes: Hacker types are predominantly T, V, and Z and versatile, respectively; wins are calculated based on the number of payoffs of c for both players (managers on the left and hackers on the right).

Figure 3 illustrates the frequencies with which strategies are chosen by the manager (left) and hacker (right). Strategies are selected based on the highest probability in each round, allowing these selections to be interpreted as strategies chosen at each stage. The red line in each graph represents the cumulative share of wins (calculated only by the rounds where they achieved the highest payoff). The pairs of figures depicting the frequencies of strategy choices by both managers and hackers result from various scenarios defined by

the hacker's type, specifically those predominantly using strategies T, V, and Z and those employing a versatile approach, respectively.

The two graphs in the second row in Figure 3 depict a situation where the hacker predominantly chooses strategy V, and the manager responds with strategies M1 and M2. That allows the manager to win in approximately half of the interactions, with only a few successful hacker attacks. The two graphs in the third row in Figure 3 involve a hacker who predominantly chooses strategy Z, allowing the manager to win 50% of the time and with the same percentage of completely successful attacks. The reason for this lies in the initial frequencies, which reinforce the manager's choice of strategy M1. While the situation may not seem dire because the manager defends the company in at least 50% of situations, each loss could be the last one for the company.

The last two graphs in the fourth row in Figure 3 are based on a simulation with a versatile hacker who chooses each strategy with equal probability. Interestingly, that allows a higher share of manager's wins because there are more cases where the role of initial frequencies points to the optimal choice. Likewise, the hacker's attacks are completely successful in approximately 20% of the rounds.

The simulation results highlight the challenges managers face with imperfect awareness in adapting to cybersecurity threats. The initial successes observed in the simulations, where the manager's strategies align with the hacker's predominant choices, underscore the importance of matching defensive strategies to the most likely attack vectors, as emphasized by Leng et al. [13] in their exploration of strategic interactions between software manufacturers and hackers. This alignment between defensive strategies and attack probabilities mirrors the game-theory models' predictions, where the awareness of attack frequencies informs optimal defensive strategies.

However, the hacker's versatility, as shown in the remaining graphs of Figure 3, further demonstrates managers' need to adapt their strategies beyond historical data. Aggarwal et al. [15] and their discourse on using deception as a strategic countermeasure support this concept. This adaptability is crucial for effectively managing the evolving nature of cyber threats.

Moreover, these findings resonate with the importance of situational awareness in cybersecurity management, as highlighted by Aggarwal et al. [18], who emphasized the role of Intrusion Detection Systems (IDSs) in augmenting cyber situational awareness. By integrating Bayesian updating mechanisms, this model reflects the continuous learning and adaptation process in response to observed cyber threats, akin to the Instance-Based Learning Theory (IBLT) discussed by [19]. This approach allows us to model the manager's decision-making process as a function of accumulated experiences and the adaptation to new information, thereby bridging the gap between theoretical constructs and practical applications in cybersecurity defense strategies.

Furthermore, the simulation results presented through figures underscore the criticality of aligning managerial actions with the probabilistic nature of cyber threats, as suggested by the equilibrium analysis. This alignment is paramount for crafting effective defense mechanisms, underpinning the theoretical discourse on innovative defense strategies beyond traditional security solutions, as explored by [15–17]. By providing a nuanced understanding of how managers can leverage their awareness and strategic insights to counteract diverse cyber threats, this study contributes to the broader cybersecurity literature, offering empirical evidence to support theoretical assertions and highlighting the dynamic interplay between attacker strategies and defensive responses within the cybersecurity domain.

Simplified, an inexperienced manager armed only with a national cybersecurity report should adopt a strategy of vigilant awareness and adaptive defense. They should start by understanding and prioritizing threats identified in the report, focusing on the most common attacks. Implementing fundamental cybersecurity practices and continuously updating their knowledge and strategies in response to new information are crucial steps. The manager should also actively engage in awareness efforts, tailoring employee training to

address the specific threats highlighted in the report. This approach, grounded in Bayesian updating and strategic adaptation, will enable even those with limited cybersecurity expertise to effectively mitigate risks if they face a typical attacker. In other instances, they could face a loss before their experience allows for the accumulation of enough knowledge. One way to counteract that is to learn from other people's experiences. The other possibility surpasses the scope of this model but can involve a retrospective based primarily on the recent opponent's activities [17–19].

While the initial presentation of our game-theory framework illustrates cyber-attacks through specific examples, such as social engineering, vulnerability exploits, and DDoS attacks, it is crucial to understand that these categories serve as archetypes to demonstrate the model's functionality rather than limit its applicability. Indeed, the nuanced landscape of cybersecurity threats often sees attacks not as isolated incidents but as components of a more sophisticated strategy, where one type of attack paves the way for another.

Recognizing this, our framework is designed with the flexibility to model such interdependencies between different attack strategies. Each attack vector—social engineering, a software vulnerability exploit, or a DDoS attack—can be considered both a standalone threat and a precursor to or component of a more complex attack pattern within the game's dynamics. The changes in the hacker's type enable exploration of the manager's updated awareness and reaction to different attack types. For example, the versatile hacker type illustrates the possibility of a series of different attack types.

While the game formulation allows for sequential strategies, further research may explore compound strategies, where the outcome of one move influences the setup and potential success of subsequent strategies. This may also be achieved by dynamically updating the game's state based on the actions taken and the outcomes observed, representing complex attack patterns that reflect real-world cyber threats' iterative nature. For example, the transition from a social-engineering attack to a vulnerability exploit and, subsequently, to a DDoS campaign can be modeled by defining multi-stage strategies within the game, where the success and detection of each stage affect the probabilities and payoffs of the following actions.

Additionally, the model may be expanded in future research to include other categories of cyber-attacks, such as ransomware, which would involve defining the probabilities for this strategy given the hacker's type and potential outcomes associated with such an attack within the game's structure. This would continue to specify how a ransomware attack alters the game state, affects the manager's awareness and strategy choices, and influences the attacker's and defender's payoffs. The modular nature of our game-theory approach facilitates this expansion, allowing for the inclusion of new attack vectors by defining their characteristics and integrating them into the existing framework. Such adaptability underscores the model's capacity to evolve in response to the ever-changing landscape of cybersecurity threats.

8.2. Different Prior Frequencies

The results in the previous section were derived using initial frequencies from the report ([45], 0.7875, 0.1947, and 0.0178). However, the report does not involve only the companies and refers to the past year, so it might not reflect the real picture. Cybercrime is quickly evolving, and the frequency of attack types could change rapidly. So, the simulation is also conducted using altered frequencies, and the hacker's type is versatile. Similar to the previous figure, Figure 4 also shows the frequencies of the manager's (left) and hacker's (right) strategy probabilities. The red line in each graph represents the cumulative share of wins.

Using initial frequencies from past reports [45] as a basis for Bayesian updating in the simulations reveals the critical role of accurate and timely intelligence in cybersecurity management. The evolving nature of cyber threats, as indicated by the need to adjust frequencies in the simulations, aligns with the observations made by Aggarwal et al. [18] regarding the importance of cyber situational awareness. It is relevant to note a practical

application of these concepts. A case study from Princeton University highlights the transformative impact of a security culture through user awareness [46]. This example shows that prior knowledge, when strategically leveraged through targeted communication and community engagement, can play a crucial role in addressing cybersecurity threats in complex organizational environments. This underscores the tangible benefits of informed strategy choices and the implementation of awareness-driven cybersecurity measures. Drawing on prior knowledge and awareness has proven critical in various real-world social-engineering attacks. For instance, notable incidents like the phishing scam that fooled a Shark Tank judge in 2020, the loss suffered by Toyota Boshoku Corporation due to a business email compromise attack in 2019, or the Ethereum Classic website hack in 2017 underscore the necessity of recognizing cybersecurity threats [47,48]. While acquiring knowledge about cyber-attacks is essential for developing baseline awareness and enhancing defensive strategies, there is a valid concern that disseminating such information could inadvertently aid attackers by providing them with insights into vulnerabilities and potential targets [49]. Another venue relies on cyber–physical systems or intrusion detection and prevention systems [50]. However, the authors [50] highlight the importance of the human factor in the context of securing IoT ecosystems by emphasizing that as these devices become more integrated into our daily lives, it is critical to address not just the technical but also the psychological vulnerabilities associated with human interaction with these systems. They argue that human psychological flaws are an intrinsic part of the security challenges facing IoT ecosystems. This perspective acknowledges that, alongside the technical, economic, and regulatory hurdles, the human element plays a pivotal role in the overall security posture. These cases highlight the significance of being aware of potential attack vectors, as it is a baseline for further assessment.

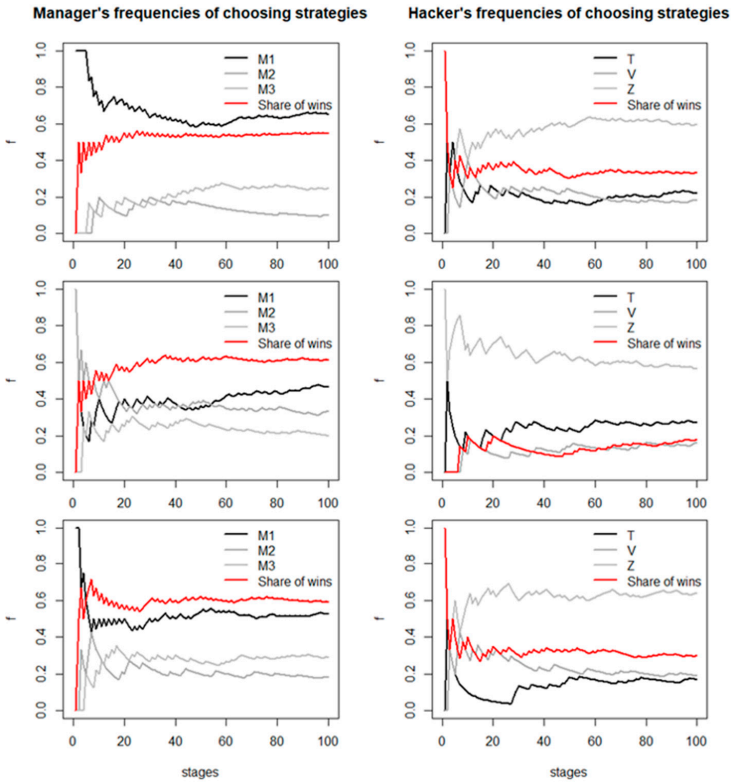

Figure 4. Manager's (**left**) and hacker's (**right**) frequencies of choosing strategies and shares of wins with different initial frequencies (common knowledge). Notes: The initial frequencies for each attack are equal in the first two graphs; 0.2, 0.7, and 0.1 in the second two graphs; and 0.1, 0.2, and 0.7 in the third two graphs. Wins are calculated based on the number of payoffs of c for both players (manager on the left and hacker on the right). The hacker's type is versatile (chooses each strategy with an initial equal probability).

The graphs in the first row show a situation where the manager initially anticipates each type of attack with equal probability. That leads to the manager's winning in about 50% of the cases. The initial frequencies are augmented for the second and third simulation run but allow the manager to win in approximately 60% of the cases. The comparison of the graphs shows that even inaccurate information on prior frequencies can be better than complete uncertainty. However, the accurate initial frequencies, in the sense that they align with the attacker's type, lead to the best results for the managers and build their awareness through Bayesian updating.

Nevertheless, the findings suggest that reliance on outdated or inaccurate frequency data can hinder the effectiveness of cybersecurity strategies, underscoring the need for ongoing intelligence gathering and analysis. This requirement for accurate threat intelligence and adaptability in response strategies is further supported by the literature on Intrusion Detection Systems (IDSs) and their contribution to situational awareness [18]. The simulations demonstrate that even imperfect awareness can lead to improved defensive outcomes when updated through Bayesian methods. This concept resonates with the Instance-Based Learning Theory (IBLT) [19] and its application in cybersecurity decision-making.

Future enhancements of the model can aim to incorporate more granular representations of SME characteristics, such as varying levels of IT competence and resource-allocation preferences, to refine our understanding of SMEs' cybersecurity challenges and resilience strategies further. These refinements could involve other aspects of awareness, such as response time, threat assessment accuracy, or learning rate.

The findings advocate for a nuanced approach to cybersecurity management, where ongoing learning, adaptability, and the strategic use of intelligence are paramount. Moreover, they highlight the potential for future research to explore alternative models of awareness and decision-making that can accommodate the rapid evolution of cyber threats and the diverse tactics employed by attackers.

The Bayesian awareness updating that involves prior frequencies of the attacks works well in the cases of the most common attack types. However, it may not allow enough agility and adaptiveness to the manager when prior frequencies do not reflect the immediate attacker's type. While this emphasizes the importance of intelligence about cyber-attacks, it also calls for other awareness modeling approaches.

To address emerging cyber threats, including AI-driven attacks and sophisticated phishing schemes, the model could be expanded to incorporate adaptive learning mechanisms that account for the evolving nature of these threats. Specifically, the model could integrate a machine learning component where the manager's awareness and strategy adaptation are not solely based on historical data but also on predictive analytics that consider trends and patterns in cyber threats. This enhancement would enable the model to dynamically adjust to new types of attacks, even those that have not been widely observed in the past. For instance, incorporating a neural network that analyzes patterns in attack vectors and predicts potential future threats could improve the model's predictive capability. This approach would allow SME managers to anticipate and prepare for emerging threats more effectively, making the cybersecurity management process more proactive rather than reactive.

8.3. Theoretical Contributions

Our research introduces a novel methodological approach for quantifying the theoretical aspect of awareness in game theory in line with theoretical propositions by [23,25], tailored to the cybersecurity context and leveraging insights by [19]. While this initiative primarily focuses on methodological innovation in awareness quantification, it naturally extends its utility to enhancing the understanding of strategic interactions in cybersecurity.

The game captures the dynamic nature of cybersecurity, where the manager continually adapts his/her strategies based on observed actions and threat landscapes. Based on Bayesian inference, the manager's awareness update functions allow the manager to update his/her beliefs about the hacker's strategies based on observed properties and prior

knowledge. The probabilities assigned to the hacker's strategies by the manager reflect their subjective assessment of the likelihood of each strategy being chosen by the hacker.

Moreover, the manager's awareness update functions mimic and simulate the process of learning and gaining awareness of the hackers' strategies and their properties over time. By incorporating information about the frequencies of past attacks, the manager can update his/her beliefs and assign probabilities to the hacker's strategies, which reflects the evolving threat environment.

The manager's awareness of the hacker's potential strategies built upon the observed properties helps him/her make informed decisions about which countermeasures to employ. Through awareness, the manager can update his/her understanding of the situation and assign probabilities to different strategies and subsets. The updating process allows the manager to refine his/her awareness of the hacker's potential strategies based on the available information.

The simulations demonstrate how the manager's awareness and his/her choices of strategies are influenced by the hacker's behavior, prior frequencies, and game history, similar to the approach of [16,17]. The accuracy of the initial frequencies plays a significant role in the manager's success, with aligned frequencies leading to optimal results. Inaccurate information on prior frequencies still outperforms complete uncertainty, emphasizing the value of any available knowledge. Based on expected payoffs and updated awareness, the manager's strategy choices demonstrate the importance of adaptive defense mechanisms in cybersecurity. However, the results suggest that other awareness modeling approaches are necessary to enhance the manager's agility and adaptiveness when the prior frequencies do not reflect the immediate attacker's type, indicating the need for improved intelligence about cyber-attacks and examinations of different awareness modeling approaches.

This study enhances the existing body of knowledge by elucidating the intricate dynamics between managers and hackers through a comprehensive game-theory framework incorporating Bayesian updating for dynamic awareness. Incorporating Bayesian updating for dynamic awareness into our model represents a significant departure from traditional static awareness approaches in cybersecurity, similar to the dynamic game settings discussed by [23], but specifically tailored to the complex, evolving nature of cyber threats faced by SMEs. This novel adaptation demonstrates the need for a more nuanced, proactive response to cybersecurity management, aligning with the continuous learning process inherent in real-world cybersecurity operations and significantly advancing the theoretical framework within which cybersecurity strategies are developed and implemented. By simulating the iterative updating of awareness based on observed outcomes and historical data, we provide a nuanced understanding of how managers can adjust their strategies to counteract an ever-changing array of cyber threats.

8.4. Practical Implications and Future Directions

In cybersecurity management, awareness is vital for effectively managing and mitigating security risks. Cybersecurity threats and attacks are constantly evolving and becoming more sophisticated. Organizations must keep track of the latest attack vectors, vulnerabilities, and techniques that malicious actors employ. Understanding an attacker's potential strategies and capabilities is crucial for designing effective defense mechanisms [8]. When an attack occurs, recognizing it and categorizing the attacker's strategies and techniques can help organizations respond effectively, mitigate the impact, and prevent future incidents.

Investigating the game-theory aspects of cybersecurity awareness and decision-making highlights significant advancements in comprehending these complex domains. By delving into the nuanced interplay between hackers and managers, particularly within the context of SMEs, we not only elucidate the strategic underpinnings of cybersecurity threats but also chart a path toward more informed and effective defensive strategies. The game provides insights into decision-making processes for cybersecurity managers, highlighting the need to consider probabilistic assessments of threats and the effectiveness of countermeasures. Complementing the conclusions of [6,18], the developed model offers SME managers a the-

oretical foundation upon which to base their cybersecurity decisions, fostering a proactive rather than reactive approach to digital threats.

In translating the theoretical insights of our game-theory framework into practical strategies for SME managers, the actionable steps that can be derived from our findings must be emphasized. Managers should prioritize the development of a dynamic cybersecurity awareness program that educates and continuously updates the team on the latest cyber threats and defense mechanisms. Managers can leverage the Bayesian updating approach to refine their cybersecurity strategies based on real-time data and evolving threat landscapes, ensuring that their defenses are as adaptive and resilient as possible. Furthermore, previous research [46] has already shown that fostering a culture of cybersecurity awareness within the organization can significantly enhance the collective ability to identify and mitigate threats. By implementing these strategic measures, SMEs can bolster their cybersecurity posture, reducing their vulnerability to cyber-attacks and enhancing their capacity to respond effectively to the complex and ever-changing cyber threat environment.

Applying our model across various industry sectors in future research could unveil sector-specific strategic interactions and defensive postures, offering a more granular understanding of cybersecurity challenges and mitigation strategies. Such explorations would expand our findings' applicability and contribute to developing more nuanced, adaptive cybersecurity strategies tailored to different sectors' unique vulnerabilities and threat profiles.

Further research should validate the practical usefulness of our game-theory framework for cybersecurity in SMEs in real-world testing and implementation. While recognizing the complexity of translating theoretical models into actionable cybersecurity strategies, we propose a phased approach for testing our system in real-world settings. Initially, this could involve a pilot study with a small group of SMEs willing to integrate our model into their cybersecurity decision-making processes. The study would monitor the model's effectiveness in enhancing the participants' cybersecurity awareness and strategic adaptation over time, comparing the incidence and impact of cyber-attacks before and after implementation. Challenges in this endeavor include accurately capturing the dynamic nature of cyber threats, ensuring the model's adaptability to the unique characteristics and constraints of each participating SME, and measuring the model's impact on awareness and cybersecurity outcomes. Qualitative feedback from SME managers and quantitative data on cyber-attack incidences, response times, and mitigation effectiveness can be employed to address these. Such findings would provide valuable insights into the model's relevance for real-world situations and highlight the areas for improvement. Therefore, a line of future research may be dedicated to overcoming these challenges, refining the model based on real-world feedback, and exploring scalable strategies for broader implementation.

9. Conclusions

This analysis underscores the foundational role that the theoretical framework of awareness in game theory plays in strategic interaction. Delving deeper, it explores the essential interplay between awareness and strategic decision-making within game theory. Hence, the primary contribution lies in the utilization of the theoretical foundation of awareness within the realm of game theory to construct an actionable and quantifiable framework tailored to cybersecurity. This framework not only facilitates the application of game theory principles to cybersecurity but also delineates and evaluates the strategic interactions between a manager and a hacker, emphasizing the dynamic process of awareness evolution and strategy adaptation in the face of cyber threats. Through this dual contribution, we aim to bridge theoretical insights with practical applications, providing a novel perspective on managing cybersecurity risks.

By integrating insights from behavioral psychology, information technology management, and even data science, further studies could expand the understanding of strategic decision-making in complex and dynamic threat environments. This cross-disciplinary

approach could not only enrich the theoretical framework but also offer practical insights for developing more resilient and adaptive cybersecurity strategies.

The game-theory contribution is limited to analyzing the interaction between a single defender and an attacker in a dynamic and uncertain environment, while emphasizing the importance of learning and awareness. Future research could enrich this framework by integrating the complexities of emerging cyber threats, such as AI-driven attacks, and by considering multi-attacker scenarios that more accurately reflect the contemporary cyber threat landscape. Moreover, by identifying key areas where further model exploration is possible, such as incorporating adaptive learning mechanisms and exploring multi-attacker scenarios, we pave the way for future studies to enhance the adaptability of cybersecurity awareness in an ever-evolving digital landscape. One critical area involves exploring the scalability of the proposed game-theory model and Bayesian updating approach across different organizational sizes and sectors.

Funding: This research received no external funding.

Data Availability Statement: Simulation and data are available at https://doi.org/10.17605/OSF.IO/Y5R63 (accessed on 29 March 2024).

Conflicts of Interest: The author declares no conflicts of interest.

Appendix A

Notation	
P	Set of players in the game.
S	Set of hacker's strategies.
M	Set of manager's strategies.
U_H	Payoff function for the hacker.
U_M	Payoff function for the manager.
T	Total number of iterations in the simulation.
Hacker	The adversary attempting to compromise the system.
Manager	The defender managing the system's security.
T	A strategy representing a social engineering attack.
V	Another strategy representing software vulnerabilities exploit attack.
Z	Another strategy representing DDOS attack.
$M_1,\ M_2,\ M_3$	Different strategies available to the manager for defending against attacks.
P_H	Initial probability distribution over the hacker's strategies.
P_M	Initial probability distribution over the manager's strategies.
F	Historical frequencies of attack types, indicating how often each type of attack has been used before the game.
$p_{Ta}(t),\ p_{Tb}(t),\ p_{Tc}(t),$ $p_{Va}(t),\ p_{Vb}(t),\ p_{Vc}(t),$ $p_{Za}(t),\ p_{Zb}(t),\ p_{Zc}(t)$	Observed properties of the method (a), target (b), and consequences (c) of hacker's strategies T, V, and Z.
H	Historical probabilities of the hacker's choices, indicating past decision-making trends within the game.
F_S	Frequencies of strategies, tracking how often each strategy is chosen.
O	Outcomes tracking, recording the results of interactions for historical analysis.
$P_H(t)$	Probability distribution over the hacker's strategies at iteration t.
$P_M(t)$	Probability distribution over the manager's strategies at iteration t.
S_t	The hacker's chosen strategy at iteration t.
M_t	The manager's chosen strategy at iteration t.
P_{obs}	Probabilities of property observations, reflecting the likelihood of detecting specific attack properties.
$U_H(S_t, M_t)$	The hacker's payoff given the chosen strategies at iteration t.
$U_M(S_t, M_t)$	The manager's payoff given the chosen strategies at iteration t.
$F_S(t+1),\ O(t+1)$	Updated frequencies of strategies and outcomes after iteration t.

References

1. Berry, C.T.; Berry, R.L. An Initial Assessment of Small Business Risk Management Approaches for Cyber Security Threats. *Int. J. Bus. Contin. Risk Manag.* **2018**, *8*, 1. [CrossRef]
2. Tam, T.; Rao, A.; Hall, J. The Good, The Bad and The Missing: A Narrative Review of Cyber-Security Implications for Australian Small Businesses. *Comput. Secur.* **2021**, *109*, 102385. [CrossRef]
3. Antunes, M.; Maximiano, M.; Gomes, R.; Pinto, D. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *J. Cybersecur. Priv.* **2021**, *1*, 219–238. [CrossRef]
4. Reegård, K.; Blackett, C.; Vikash, K. The Concept of Cybersecurity Culture. In Proceedings of the 29th European Safety and Reliability Conference, Hannover, Germany, 22–26 September 2019; pp. 4036–4043.
5. Hudock, A.; Weidman, J.; Grossklags, J. Security Onboarding: An Interview Study on Security Training for Temporary Employees. In Proceedings of the Conference on Mensch und Computer, Magdeburg, Germany, 6–9 September 2020; ACM: Magdeburg, Germany, 2020; pp. 183–194.
6. Ofte, H.J.; Katsikas, S. Understanding Situation Awareness in SOCs, a Systematic Literature Review. *Comput. Secur.* **2023**, *126*, 103069. [CrossRef]
7. Ključnikov, A.; Mura, L.; Sklenár, D. Information Security Management in SMEs: Factors of Success. *J. Entrep. Sustain. Issues* **2019**, *6*, 2081–2094. [CrossRef] [PubMed]
8. Alahmari, A.; Duncan, B. Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. In Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 15–19 June 2020; IEEE: Dublin, Ireland, 2020; pp. 1–5.
9. Kikerpill, K. *Crime-As-Communication: Detecting Diagnostically Useful Information from the Content and Context of Social Engineering Attacks*; University of Tartu Press: Tartu, Estonia, 2021.
10. Dowd, M.; McDonald, J.; Schuh, J. *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities*; Pearson Education: Upper Saddle River, NJ, USA, 2006; ISBN 0-13-270193-6.
11. Mansfield-Devine, S. The Growth and Evolution of DDoS. *Netw. Secur.* **2015**, *2015*, 13–20. [CrossRef]
12. Trim, P.R.J.; Lee, Y.-I. The Global Cyber Security Model: Counteracting Cyber Attacks through a Resilient Partnership Arrangement. *Big Data Cogn. Comput.* **2021**, *5*, 32. [CrossRef]
13. Leng, Q.; Yang, Y.; Pan, R.; Hu, H. Research of Complete Information Static Game Model for Software Manufacturer, White Hats and Black Hats. *Procedia Comput. Sci.* **2018**, *131*, 832–840. [CrossRef]
14. Robertson, J.; Diab, A.; Marin, E.; Nunes, E.; Paliath, V.; Shakarian, J.; Shakarian, P. Darknet Mining and Game Theory for Enhanced Cyber Threat Intelligence. *Def. Rev.* **2016**, *1*, 95–122.
15. Aggarwal, P.; Gonzalez, C.; Dutt, V. Cyber-Security: Role of Deception in Cyber-Attack Detection. In *Advances in Human Factors in Cybersecurity, Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity, Walt Disney World®, Orlando, FL, USA, 27–31 July 2016*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 85–96.
16. Aggarwal, P.; Gonzalez, C.; Dutt, V. HackIt: A Real-Time Simulation Tool for Studying Real-World Cyberattacks in the Laboratory. In *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 949–959.
17. Aggarwal, P.; Gautam, A.; Agarwal, V.; Gonzalez, C.; Dutt, V. Hackit: A Human-in-the-Loop Simulation Tool for Realistic Cyber Deception Experiments. In *Advances in Human Factors in Cybersecurity, Proceedings of the AHFE 2019 International Conference on Human Factors in Cybersecurity, Washington, DC, USA, 24–28 July 2019*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 109–121.
18. Aggarwal, P.; Moisan, F.; Gonzalez, C.; Dutt, V. Understanding Cyber Situational Awareness in a Cyber Security Game Involving Recommendations. *Int. J. Cyber Situational Aware.* **2018**, *3*, 11–38. [CrossRef]
19. Dutt, V.; Ahn, Y.-S.; Gonzalez, C. Cyber Situation Awareness: Modeling Detection of Cyber Attacks with Instance-Based Learning Theory. *Hum. Factors* **2013**, *55*, 605–618. [CrossRef] [PubMed]
20. Kostelić, K. Implications of (Un) Awareness for Decision-Making in Strategic Interaction: Another Take on the Prisoner's Dilemma. *Decision* **2023**, *50*, 251–268. [CrossRef]
21. Blasch, E.; Shen, D.; Pham, K.D.; Chen, G. *Review of Game Theory Applications for Situation Awareness*; Pham, K.D., Chen, G., Eds.; SPIE: Baltimore, MD, USA, 2015; Volume 9469, pp. 141–150.
22. Franke, M. Pragmatic Reasoning About Unawareness. *Erkenntnis* **2014**, *79*, 729–767. [CrossRef]
23. Halpern, J.Y.; Rêgo, L.C. Extensive Games with Possibly Unaware Players. *Math. Soc. Sci.* **2014**, *70*, 42–58. [CrossRef]
24. Rêgo, L.C.; Halpern, J.Y. Generalized Solution Concepts in Games with Possibly Unaware Players. *Int. J. Game Theory* **2012**, *41*, 131–155. [CrossRef]
25. Halpern, J.Y.; Piermont, E. Dynamic Awareness. *arXiv* **2020**, arXiv:2007.02823.
26. Halpern, J.Y.; Piermont, E. Partial awareness. In Proceedings of the AAAI Conference on Artificial Intelligence, Honolulu, HI, USA, 27 January–1 February 2019; Volume 33, pp. 2851–2858.
27. Endsley, M.R. Situation Awareness Misconceptions and Misunderstandings. *J. Cogn. Eng. Decis. Mak.* **2015**, *9*, 4–32. [CrossRef]
28. Jiang, X.; Gao, G.; Yang, X. Evolutionary Game Analysis on Live Streaming Commerce Considering Brand Awareness and Anchor Influence. *Kybernetes* **2022**, *52*, 6467–6493. [CrossRef]
29. Liu, Z.L.; Anderson, T.D.; Cruz, J.M. Consumer Environmental Awareness and Competition in Two-Stage Supply Chains. *Eur. J. Oper. Res.* **2012**, *218*, 602–613. [CrossRef]

30. Duan, J.; Gao, D.; Yang, D.; Foh, C.H.; Chen, H.-H. An Energy-Aware Trust Derivation Scheme with Game Theoretic Approach in Wireless Sensor Networks for IoT Applications. *IEEE Internet Things J.* **2014**, *1*, 58–69. [CrossRef]
31. Halpern, J.Y. Awareness in Games, Awareness in Logic. In Proceedings of the International Conference on Logic for Programming Artificial Intelligence and Reasoning, Yogyakarta, Indonesia, 10–15 October 2010; Springer: Berlin/Heidelberg, Germany, 2010; p. 15.
32. Feinberg, Y. Subjective Reasoning-Games with Unawareness. 2004. Research Paper No. 1875. Research Paper Series, Stanford Graduate School of Business. Available online: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=d9f4768ecdc72a001a3a192c9b6c28b634e552bf (accessed on 10 February 2019).
33. Feinberg, Y. Games with Unawareness. *B.E. J. Theor. Econ.* **2021**, *21*, 433–488. [CrossRef]
34. Piermont, E. Unforeseen Evidence. *J. Econ. Theory* **2021**, *193*, 105235. [CrossRef]
35. Chen, G.; Shen, D.; Kwan, C.; Cruz, J.; Kruger, M. Game Theoretic Approach to Threat Prediction and Situation Awareness. In Proceedings of the 2006 9th International Conference on Information Fusion, Florence, Italy, 10–13 July 2006; IEEE: Florence, Italy, 2006; pp. 1–8.
36. Von Thadden, E.-L.; Zhao, X. Incentives for Unaware Agents. *Rev. Econ. Stud.* **2012**, *79*, 1151–1174. [CrossRef]
37. Sarcia', S.A. Timed Strategic Games A New Game Theory for Managing Strategic Plans in the Time Dimension. In Proceedings of the 2013 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), San Diego, CA, USA, 25–28 February 2013; IEEE: San Diego, CA, USA, 2013; pp. 187–194.
38. Heifetz, A.; Meier, M.; Schipper, B.C. Dynamic Unawareness and Rationalizable Behavior. *Games Econ. Behav.* **2013**, *81*, 50–68. [CrossRef]
39. Kostelic, K. Guessing the Game: An Individual's Awareness and Assessment of a Game's Existence. *Games* **2020**, *11*, 17. [CrossRef]
40. Sadzik, T. Knowledge, Awareness and Probabilistic Beliefs. *B.E. J. Theor. Econ.* **2021**, *21*, 489–524. [CrossRef]
41. Hiscox Cyber Readiness Report 2023. Available online: https://www.hiscoxgroup.com/sites/group/files/documents/2023-10/Hiscox-Cyber-Readiness-Report-2023.pdf (accessed on 5 April 2024).
42. Chen, D.; Ignatius, J.; Sun, D.; Zhan, S.; Zhou, C.; Marra, M.; Demirbag, M. Reverse Logistics Pricing Strategy for a Green Supply Chain: A View of Customers' Environmental Awareness. *Int. J. Prod. Econ.* **2019**, *217*, 197–210. [CrossRef]
43. Cao, D.; Li, J.; Liu, G.; Mei, R. Can Decentralization Drive Green Innovation? A Game Theoretical Analysis of Manufacturer Encroachment Selection with Consumer Green Awareness. *Processes* **2021**, *9*, 990. [CrossRef]
44. Salehnejad, R. *Rationality, Bounded Rationality and Microfoundations*; Palgrave Macmillan: London, UK, 2007; ISBN 978-1-349-28149-7.
45. CERT Godišnje Izvješće 2022. CARNET. Available online: https://www.cert.hr/wp-content/uploads/2023/02/CERT-G.I.-2022.pdf (accessed on 27 April 2023).
46. Blum, D.; Sherry, D.; Schaufler, T. Case Study: Transforming Princeton's Security Culture Through Awareness. *ISCA J.* **2020**, *1*, 4. Available online: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-1/case-study-transforming-princetons-security-culture-through-awareness (accessed on 15 March 2024).
47. *10 Real and Famous Cases of Social Engineering Attacks, Gafety*. June 2021. Available online: https://gatefy.com/blog/real-and-famous-cases-social-engineering-attacks/ (accessed on 18 March 2024).
48. *15 Examples of Real Social Engineering Attacks, Tessian*. 7 February 2023. Available online: https://www.tessian.com/blog/examples-of-social-engineering-attacks/ (accessed on 18 March 2024).
49. Lallie, H.S.; Shepherd, L.A.; Nurse, J.R.C.; Erola, A.; Epiphaniou, G.; Maple, C.; Bellekens, X. Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. *Comput. Secur.* **2021**, *105*, 102248. [CrossRef]
50. Xenofontos, C.; Zografopoulos, I.; Konstantinou, C.; Jolfaei, A.; Khan, M.K.; Choo, K.-K.R. Consumer, Commercial, and Industrial Iot (in) Security: Attack Taxonomy and Case Studies. *IEEE Internet Things J.* **2021**, *9*, 199–221. [CrossRef]