Journal of *Cybersecurity and Privacy*

MDPI

Article

Mitigating Malicious Insider Threats to Common Data Environments in the Architecture, Engineering, and Construction Industry: An Incomplete Information Game Approach

KC Lalropuia [1,*], Sanjeev Goyal [2,3], Borja García de Soto [1,4], Dongchi Yao [1,4] and Muammer Semih Sonkor [1,4]

[1] S.M.A.R.T. Construction Research Group, Division of Engineering, New York University Abu Dhabi (NYUAD), Experimental Research Building, Saadiyat Island, Abu Dhabi P.O. Box 129188, United Arab Emirates; garcia.de.soto@nyu.edu (B.G.d.S.); dy2037@nyu.edu (D.Y.); semih.sonkor@nyu.edu (M.S.S.)

[2] Division of Social Science, New York University Abu Dhabi (NYUAD), Saadiyat Island, Abu Dhabi P.O. Box 129188, United Arab Emirates; sg472@cam.ac.uk

[3] Faculty of Economics, University of Cambridge, Cambridge CB3 9DD, UK

[4] Department of Civil and Urban Engineering, Tandon School of Engineering, New York University (NYU), 6 MetroTech Center, Brooklyn, NY 11201, USA

[*] Correspondence: kclalropuia@gmail.com or kcl7487@nyu.edu

Abstract: Common data environments (CDEs) are centralized repositories in the architecture, engineering, and construction (AEC) industry designed to improve collaboration and project efficiency. However, CDEs hosted on cloud platforms face significant risks from insider threats, as stakeholders with legitimate access may act maliciously. To address these vulnerabilities, we developed a game-theoretic framework using Bayesian games that account for incomplete information, modeling both simultaneous and sequential interactions between insiders and data defenders. In the simultaneous move game, insiders and defenders act without prior knowledge of each other's decisions, while the sequential game allows the defender to respond after observing insider actions. Our analysis used Bayesian Nash Equilibrium to predict malicious insider behavior and identify optimal defense strategies for safeguarding CDE data. Through simulation experiments and validation with real project data, we illustrate how various parameters affect insider–defender dynamics. Our results provide insights into effective cybersecurity strategies tailored to the AEC sector, bridging theoretical models with practical applications and supporting data security within the increasingly digitalized construction industry.

Keywords: AEC industry; Bayesian game theory; common data environment (CDE); cybersecurity insider threats; Monte Carlo simulation

check for updates

Academic Editor: Danda B. Rawat

Received: 5 November 2024

Revised: 16 December 2024

Accepted: 10 January 2025

Published: 31 January 2025

Citation: Lalropuia, K.; Goyal, S.; García de Soto, B.; Yao, D.; Sonkor, M.S. Mitigating Malicious Insider Threats to Common Data Environments in the Architecture, Engineering, and Construction Industry: An Incomplete Information Game Approach. *J. Cybersecur. Priv.* **2025**, *5*, 5. https://doi.org/10.3390/jcp5010005

1. Introduction

The utilization of robotics, the adoption of various communication technologies, and the integration of building information modeling (BIM) processes into construction tasks are accelerating the digital transformation of the architecture, engineering, and construction (AEC) industry [1]. This transformation has resulted in an increased amount of data stored in digital formats, including sensitive information (e.g., design files, intellectual property, bid documents) that are prone to cyberattacks [1]. Despite the increasing reliance on digital tools, the importance of robust security measures to protect construction projects has been overlooked, leaving the industry exposed to various cyber threats [2]. The complex nature of construction projects' supply chains and the involvement of many stakeholders (e.g., owner, contractors, engineers, suppliers) from different disciplines (e.g., structural, architectural, mechanical) further increase the challenge of providing secure and efficient data exchange.

The risks associated with these vulnerabilities are evident in recent cyber incidents targeting construction companies. These include data breaches (i.e., theft, modification, and exposure of sensitive data), fraudulent wire transfers, and property damages [1]. For example, hackers stole the design files of the Australian Intelligence Service's headquarters during its construction in 2013 [2]. This proves that design documents can also be valuable for malicious actors when a constructed building is of strategic importance to the government. A white paper prepared by the security software company FinalCode also presented the risks of insider threats targeting CAD files in design-centric businesses [3]. In addition, employees' and other stakeholders' personal information can be a target of attackers. For instance, Turner Construction was targeted by a phishing attack in 2016, exposing the tax information and social security numbers of its employees [4]. Similar attacks also damage the reputation of the targeted companies and can cause disruptions to business operations.

Common data environments (CDEs), introduced as centralized data repositories (see Figure 1) to enhance collaboration among stakeholders in BIM-enabled projects, aim to improve data security and management [1]. However, the reliance on centralized CDEs has introduced a single point of failure, as highlighted by several studies proposing decentralized alternatives utilizing blockchain and the interplanetary file system (IPFS) [5,6]. Protection against data theft becomes a significant challenge as the information exchange reaches its peak with the increasing use of BIM/CDE tools, particularly in design–build and integrated project delivery (IPD) projects [7].

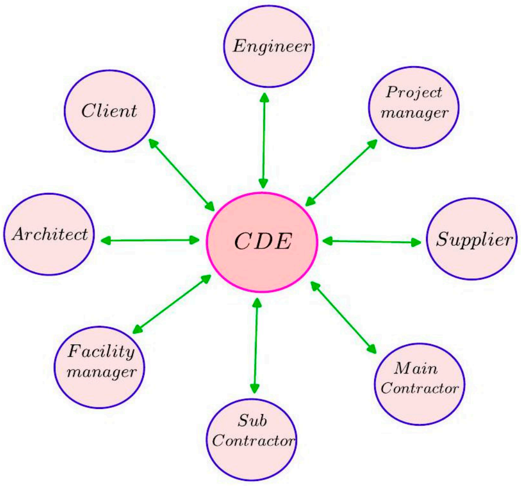


Figure 1. Common data environment (CDE).

Several document types can be sensitive depending on the project type. For example, the cost and profitability calculations and financial forecast files of large-scale projects are considered confidential. Such documents typically include the unit cost of constructing different elements of the structure, procurement and subcontract details for different materials and services, and the project's cash flow. Therefore, a potential leakage of such documents would give a competitive advantage to the rivals of the construction company, resulting in financial loss. Another sensitive document would be design files, especially considering the construction of buildings such as embassies, prisons, military bases, and critical government buildings.

Even though the provided examples of cyberattacks were conducted by external actors, the motivation and consequences would be similar in case of insider threat. Turk et al. [8]

and Mantha et al. [1] pointed out that various stakeholders involved in construction projects might be motivated to act as malicious insiders for various reasons, including financial gain and espionage. These motivations are aligned with the previous examples of external cyberattacks targeting construction companies. Supporting these claims, a recent survey on cybersecurity in the construction industry reported that 20% of the respondents considered malicious insider threats the highest-level concern [9]. Moreover, considering that the insiders might have legitimate access to the CDE and the mentioned sensitive documents, detection can be more complicated and the outcomes can be more devastating.

Addressing insider threats within CDEs is paramount for safeguarding sensitive construction project data, which constitutes the primary motivation of this study. Mitigating these risks requires proactive strategies beyond traditional cybersecurity measures to encompass insider threat detection and response. To this end, we propose game-theoretic models to analyze and predict malicious insider behavior and devise optimal strategies for protecting sensitive data within CDEs. This paper contributes to the ongoing efforts to enhance cybersecurity in the AEC industry by (1) developing simultaneous and sequential game-theoretic models to understand insider threat dynamics, (2) verifying the proposed models through simulations and hypothetical scenarios, and (3) validating the applicability of the models using real project data.

The remainder of this paper is structured as follows. Section 2 outlines the related work, identifies drawbacks in the existing literature, and discusses the motivations behind this research. Section 3 presents the methodology, introduces the proposed simultaneous and sequential move game models, and provides their solutions. Section 4 verifies the proposed models through simulations, hypothetical scenarios, and real project data. Section 5 discusses the results and limitations and Section 6 concludes this paper.

2. Related Work

Research has been conducted to deal with cybersecurity issues in critical infrastructures [10]. Various approaches have also been used to mitigate insider threats [11]. Hu et al. [12] addressed the joint threat from an advanced persistent threat (APT) attacker and insiders targeting a resource defender employing a differential game approach. The scenario in [12] considered a malicious insider who collaborates with the APT attacker by exchanging sensitive information, such as passwords, to help them achieve their malicious goals. Meanwhile, the defender employs countermeasures to regain control of the compromised resources. In the attack process, however, the defender does not consider any prior beliefs about an insider as to whether he/she would act as a regular or malicious one, which is necessary to respond to the possible threats caused by the insider. In addition, how the data/information is obtained by the malicious insider is not specified [12]. Ni et al. [13] discussed malicious insider attacks in a nuclear power plant based on an evolutionary game model. In this model, a malicious insider has two options, i.e., to perform or not perform the adversarial attacks. At the same time, the plant's defender can implement either a severe punishment scheme or a less strict penalty for malicious insiders. Their proposed game solutions show how insiders would behave concerning their emotions. Kim et al. [14,15] also proposed a Stackelberg game model of defender–adversary interactions along with the possibility of various insiders being involved in a nuclear facility attack. Their analyses identified which insider threat was more critical concerning the facility's security. In the models proposed by Ni et al. [13] and Kim et al. [15], the defender/security department has no preconceived idea about how its employees will behave towards sensitive resources. Furthermore, the authors in [13,15] did not specify how the malicious goal is achieved; in other words, whether authentication or cyberattack is to be launched against the resources to obtain access/steal the resources or sabotage the facilities. Liu et al. [16] presented a model to detect malicious insider threats using a zero-sum stochastic game assuming partially observable states. Kantzavelou et al. [17] also proposed a repeated game model in which insiders interact with the system defender, an intrusion detection system (IDS). Their model predicts future interactions between insiders and the system defender. In addition, Elmrabit et al. [18] developed a model based on a Bayesian network to predict insider threats prior to a data breach, taking into account various aspects such as technological, organizational, and human factors. The model draws on various components to predict the probability of insider threat risk. However, in these works [16–18], no penalty for malicious insiders is imposed, which is a crucial demotivating factor as to whether or not an insider would commit malicious acts to optimize his/her gain or benefits. Laszka et al. [19] introduced a secure team selection framework where the team manager has a secret to share with her team, whereas an insider attacker wants to learn the secret by bribing one of the potential team members. The scenario is analyzed using a stochastic game. Feng et al. [20] and Cansever [21] discussed a game model in which an insider can take part in the game between an attacker and the system defender. The insider can help achieve the attacker's goal while sharing the revenue. In addition, an incentive-based model was introduced by Liu et al. [22] to mitigate malicious insider threats.

The concept of synergy has been explored in game theory to understand how collaboration among players can enhance outcomes through mutual assistance and interdependence. Cooperative game theory introduces measures like the Shapley value to assess individual contributions within coalitions and identify scenarios where synergetic effects yield greater collective benefits than independent actions [23]. These insights are particularly relevant for designing strategies that align the interests of diverse stakeholders in cybersecurity contexts, including insider threat scenarios.

An adversarial risk analysis approach was adopted by Joshi et al. [24] to analyze malicious insider threats and tackle the traceability issue of adversarial insider attacks. A traceability system with respect to insider attackers was proposed by Hu et al. [25] using blockchain. Moreover, machine learning techniques were used to detect malicious insider threats [26–31], where most of the work focused on reactive measures failing to counter proactive challenges. It can be observed that the existing literature does not consider several aspects (see Table 1) that are necessary for predicting malicious insider behaviors and deriving the best defense strategies against such attacks. It is clear that modeling malicious insider threats without considering all of these aspects has drawbacks in capturing the realistic situation. Notably, previous studies on the behavior of malicious insiders assume complete information about the game structure. However, this assumption is unrealistic since insiders' intentions, such as being malicious or honest, are not entirely known to the data defender. Moreover, to the best of the authors' knowledge, no study has discussed insider threat modeling considering the construction industry. Therefore, in this paper, we propose novel incomplete information game models in the context of the construction industry incorporating the following aspects:

- Aspect 1 (A1): The value of information/data/resources to an insider.
- Aspect 2 (A2): Penalty to a malicious insider when his/her activity and identity are exposed.
- Aspect 3 (A3): How the sensitive information/data are compromised (e.g., through authentication or cyberattack).
- Aspect 4 (A4): The probability of discovering the malicious activities and the insider's identity.
- Aspect 5 (A5): The prior belief/information that the data defender has about an insider.

Table 1. Different aspects considered (yes) or not considered (no) in the literature.

Authors	Approach	Aspects Considered				
		A1	A2	A3	A4	A5
Liu et al. [16]	Stochastic game	yes	no	yes	yes	no
Laszka et al. [19]	Stochastic game	yes	no	yes	no	no
Liu et al. [22]	Static game	yes	yes	no	no	no
Hu et al. [12]	Differential game	yes	yes	no	yes	no
Feng et al. [20]	Sequential game	yes	yes	no	yes	no
Cansever et al. [21]	Stackelberg game	yes	yes	no	yes	no
Kim et al. [14]	Stackelberg game	yes	no	yes	yes	no
Kantzavelou et al. [17]	Repeated game	yes	no	yes	yes	no
Ni et al. [13]	Evolutionary game	yes	yes	no	yes	no
Hu et al. [25]	Blockchain	yes	no	yes	yes	no
Elmrabit et al. [18]	Bayesian network	yes	no	no	yes	yes
Joshi et al. [24]	Adversarial risk analysis	yes	no	no	yes	yes
Azaria et al. [29]	Machine learning	yes	no	yes	yes	no
Hall et al. [27]	Machine learning	yes	no	yes	yes	no
Kim et al. [26]	Machine learning	yes	no	yes	yes	no
Al-Shehari et al. [28]	Machine learning	yes	no	yes	yes	no
Brdiczka et al. [31]	Graph learning	yes	no	yes	yes	no
Chattopadhyay et al. [30]	Time-series classification	yes	no	yes	yes	no

The main contributions of this paper are highlighted below:

i. The existing literature predominantly examines malicious attacks executed via cyberattacks, often neglecting the potential for insider threats initiated through legitimate authentication processes. This oversight is particularly relevant for the AEC industry, where stakeholders have legitimate access to data within CDEs but may misuse this access for malicious purposes. Our research fills this gap by modeling insider threats that can arise through cyberattacks and authorized access, presenting a more comprehensive view of vulnerabilities in CDEs.

ii. The existing literature often assumes complete information regarding insider behavior types, overlooking the ambiguity of legitimate versus malicious intentions within the AEC environment. Our research introduces a Bayesian game model that incorporates incomplete information, accurately reflecting the real-world complexity of insider motivations. By considering both types of insiders, our model offers a novel approach to predicting insider behavior under conditions of uncertainty, enhancing the development of targeted defense strategies against insider threats in CDEs.

iii. The rise of digitalization, BIM, and CDEs in the AEC sector has introduced unique cybersecurity challenges that current generalized insider threat models do not sufficiently address. To our knowledge, our research is the first to address insider threats to CDEs in the AEC industry.

iv. We validate our models using real project data and simulations, which demonstrate the models' practical applicability in real-world AEC projects. This validation not only supports the theoretical framework but also provides actionable insights that can directly inform threat mitigation strategies within the industry. By bridging theoretical development with empirical testing, our research offers an applied contribution to the field, enhancing the reliability of the proposed defense mechanisms for practical cybersecurity applications.

Game theory is a mathematical study of strategic interactions of agents or players. Every player has a set of possible actions, and payoffs (i.e., cost/penalty or gain/reward) are assigned to each player based on the collective action. A common assumption is that players are rational and, thus, would want to optimize their payoffs. The solution of a game provides each player with the best strategies for making decisions or actions and no one can be better off by deviating from the strategies obtained in the solution (or equilibrium point). A game is considered a complete information model if all the components of the game, such as actions, payoffs, and types, are common knowledge among the players. In contrast, an incomplete information game is where some players do not know the payoff of the other players [32]. Game theory has been employed successfully to address various issues related to cybersecurity [33]. In this study, we also developed incomplete information games to study malicious insider behavior and obtain the best strategies to respond to insider threats.

3. Methodology

3.1. Defining the Data Defender

Two parties are involved in the proposed game-theoretic models: the malicious insider and the data defender. While the former is self-explanatory and has similar meanings in different contexts, the latter should be defined considering its roles before going into the details of the model. In the context of this paper, the defender has two primary roles: (1) access control and (2) intrusion detection. The defender is assumed to perform both roles even though they are handled by different mechanisms in a construction network. Both roles are detailed in the following subsections, together with construction-related examples and the assumptions made.

The malicious insider aims to access sensitive information, which is granted by the access control mechanism explained below in detail. The insider can then use this access to leak sensitive information, make changes, or render it unavailable. However, the malicious insider should stay as stealthy as possible while performing these actions since the IDS is also a part of the data defender, affecting the decisions of the access control system. As elaborated upon in the following sections, the IDS provides feedback to the access control system based on the activities of the insider. This collaboration of the IDS and access control system, which forms the data defender, is crucial to combat insider threats since the malicious actor authorizes access to sensitive data. Therefore, different from external threats, utilizing typical systems such as firewalls, antivirus software, and the IDS as data defenders is insufficient. Including the access control system as a part of the defender is necessary to make the decision of granting or rejecting authorized users' requests. However, the suggested data defender can still be inadequate to combat insider threats if the malicious insider can perform its actions stealthily enough. In this case, the feedback from the IDS would be misleading.

3.1.1. Access Control

The defender's first role is to manage data access by accepting or rejecting data access requests. Since this paper considers construction projects that utilize CDEs, access control is implemented on the data stored in a CDE. As mentioned earlier, CDEs are widely used for storing, viewing, and exchanging data due to the increasing use of BIM technologies in construction projects. The CDE utilized by the project may either be cloud-based or hosted on the in-house servers of a project. Companies from different sectors increasingly rely on cloud computing technologies for storage due to their advantages, such as no upfront cost, location flexibility for employees, and pay-as-you-go pricing models [34]. This transition also applies to the construction sector, with the increasing number of off-the-shelf cloud platforms that make cloud implementation more effortless. Some examples of cloud platforms offered by leading construction software development companies are Autodesk Construction Cloud, Graphisoft BIMcloud, and Trimble Connect.

This paper assumes the use of one of the cloud-based platforms (e.g., Autodesk Construction Cloud) offered by a construction software development company, considering their widespread use in the industry, especially by small and medium-sized enterprises (SMEs), which constitute more than 95% of construction supply chains [35]. The CDE platform selection in construction projects depends on the software packages used for various tasks, such as design authoring, clash detection, structural analysis, energy analysis, and reality capture. The platform developed by the software company commonly used in the project is prioritized for improved interoperability. This paper assumes a generic cloud platform without selecting a specific one.

The access control mechanism of the cloud platform that handles accepting and rejecting data access requests is considered a part of the data defender in this paper. There are three major access control models widely used in computer systems: role-based access control (RBAC) (i.e., non-discretionary access control), mandatory access control (MAC), and discretionary access control (DAC) [36]. In this paper, RBAC is assumed to be implemented in the cloud platform with the least privilege design principle in mind, similar to Autodesk Construction Cloud [37]. Therefore, individual users and user groups are given privileges based on their roles in the project. The BIM manager of the project is assumed to function as the administrator of the cloud platform, responsible for assigning roles and defining privileges for each role. It should be noted that assigning roles is not a one-time task but rather an ongoing process in a typical construction project due to the changing roles and new employees joining the project.

3.1.2. Intrusion Detection

The second role of the data defender is to detect potential intrusions and cyberattacks. Consequently, the IDS is also considered a part of the defender in this paper. The role of the IDS is crucial for the game-theoretic model presented in this study, as the data defender is assumed to make data access decisions while experiencing cyberattacks in specific instances. Therefore, the first role of the defender is contingent on the intrusion detection role. This paper does not make any assumptions regarding the type of IDS, such as signature-based (knowledge-based) or anomaly-based (behavior-based), as the technical aspects of the IDS fall beyond the scope of this paper.

As mentioned earlier, an external cloud platform is assumed to be utilized as the CDE. However, the IDS can only be implemented on the internal network of the project. Hence, it is assumed that the cloud platform used as the CDE accepts input from the IDS, allowing the IDS to dictate the decisions of the access control mechanism. This interaction between the access control mechanism and the IDS is presented in detail in the following sections of this paper. Lastly, it is assumed that being connected to the project network is necessary to access the CDE to effectively achieve IDS–access control collaboration. The stakeholders within the project perimeter can connect to the network through a wireless access point (WAP) or wired connection. On the other hand, a virtual private network (VPN) is mandatory to connect to the project network for stakeholders outside the project area.

3.2. Simultaneous Move Game Model

Insider threats are difficult to deal with in comparison to external threats due to the privilege that insiders have. An insider is motivated to compromise data for different purposes (e.g., financial gain, espionage). A malicious insider can achieve this activity by using his/her privilege through authentication to gain access to the data. This is termed as the misuse of access [38]. In this case, however, there is a probability that the malicious act and his/her identity are discovered because all the detailed information of the insider who has accessed the data is revealed to the data defender during the authentication process. As a result, the malicious insider can face a heavy penalty (cost) if his/her activity and identity are revealed. Thus, to prevent his/her identity and malicious activity from being known, the insider can make use of a cyberattack technique such as defense bypass [38] (e.g., SQL injection attack [39]) to access the data. We assume that the probability of exposing the malicious activity and insider's identity under authentication (misuse of data) is greater than that of malicious action/identity being discovered under cyberattack. However, launching a cyberattack to obtain the data is costly compared to a misuse of access attack through an authentication process.

Therefore, there are two schemes for a malicious insider to implement this activity: gain access to the data through authentication or a cyberattack. An insider can exploit his/her privilege to obtain important information, such as vulnerabilities of the computing facilities (e.g., cloud computing used to host the CDE), by scanning, reconnaissance, or infiltration. The data defender believes that there is a malicious insider in the project team with a positive probability. This shows that releasing data to authorized insiders whenever a data access request is made can cause data compromise (e.g., tampering, theft, leakage).

Therefore, when an insider (whose type can be legitimate or malicious) sends a data access request, the data defender is faced with a situation as to whether to accept the request and release the data or reject the request and not release the data. As a result, the following two cases arise:

i. If the data are released to an insider who happens to be malicious, the data will be misused (e.g., trading them for financial purposes, sending them to the enemy) by the malicious insider.
ii. On the other hand, if the data request is rejected, there is a probability of rejecting a legitimate insider request. Though the data are protected in this situation, the project team would be unable to achieve the expected outcome/goal in the project work due to the information (data) necessary for the project being withheld. That is, the workflow will be interrupted, for example, during the design phase.

Thus, considering the above scenario, the questions that need to be addressed are as follows: What will be the best strategies for the defender to protect the data in the scenario of incomplete information about an insider who can act as legitimate or malicious? How likely is it that an attack is being carried out by an insider of the project team or, equivalently, how secure are the data stored in the database of the CDE/BIM? To address this problem, we formulated an incomplete information game model to capture the interactions between an insider (legitimate or malicious) and the defender. The analysis of the proposed model will give us insights into how an insider in the project would behave as the game solutions predict the behavior of an insider and the best decisions for the defender.

Now, we consider the interactions between insiders (stakeholders) of a construction project and the data defender who defends data stored in a CDE. In this model, an insider sends a data access request to the defender. The defender is not certain about whether the request comes from a legitimate or malicious insider. To capture the interactions, we propose a simultaneous move incomplete information game model in this section and solve the game model to perceive the behavior of the insiders and know how to respond to malicious insider threats. For this, we define the notations and terminologies that are used in the proposed game model (which is denoted as $\mathit{\Gamma}$) as follows: R_{aut} (request data access through authentication), R_{cyb} (request data access through cyberattack), D_{accept} (accept data access request and release data), D_{reject} (reject data access request and do not release data), and $C_{cyb} \in (0,1)$ (cost of cyberattack). The action sets of an insider and the defender can be written as $\mathcal{A}_I = \left\{R_{\text{aut}}, R_{\text{cyb}}\right\}, \mathcal{A}_d = \left\{D_{\text{accept}}, D_{\text{reject}}\right\}$. Also, the type set of insiders $\Omega = \{$ malicious (M), legitimate (L)$\}$. The pure strategy set of an insider is given by $S_I = \left\{R_{aut}^M R_{aut}^L, R_{cyb}^M R_{aut}^L\right\}$, where $R_{cyb}^M R_{aut}^L$ is the strategy with which the insider would launch a cyberattack if he/she is malicious (M). On the other hand, if he/she is legitimate (L), he/she would take the authentication process to access the data. Similarly, the other strategy, $R^M_{\text{aut}}\ R^L_{\text{aut}}$, can be defined. In addition, the pure strategy set of the defender is given by $S_D = \{D_{\text{accept}}\ , D_{\text{reject}}\ \}$. That is, the defender can respond to the data access request by either accepting or rejecting it.

Nature's probability distribution on insider's type space is given by $\Phi : \Omega \mapsto [0,1]$, such that $\Phi(M) = \delta$ and $\Phi(L) = 1-\delta$. That is, the probability that an insider is malicious is δ, whereas the insider is legitimate with a probability of $1-\delta$. This is common knowledge among the two players—the insider and the defender. Let $\beta \in (0,1)$ denote the payoff assigned to a malicious insider and $\omega \in (0,1)$ denote the payoff to the defender due to the discovery of a malicious insider identity or the protection of data (and $-\omega$ reflects the loss as a result of data compromise or not detecting a malicious insider identity). In the case of identity detection, for example, the defender can improve the data security by removing the malicious insider from the project team. Furthermore, p_1 is used to denote the probability that the identity of the malicious insider and his/her activity are discovered in the case of proper authentication. Let $V_i(a, b \mid \theta), i = 1,2$, denote the payoffs of player $i \in \mathcal{N} = \{1 \text{ (insider)}, 2 \text{ (defender)} \}$ corresponding to an action profile $(a,b) \in \mathcal{A} = \mathcal{A}_I \times \mathcal{A}_d$ and an insider of type $\theta \in \Omega$, i.e., $V_i : \mathcal{A} \times \Omega \mapsto \mathbb{R}$.

The extensive form of the game model is shown in Figure 2. In the payoffs of Figure 2, the subscript a is used to represent authentication or accept as the case may be and r is used to represent reject. $i_0, i_1, \ldots, i_5$ are used to denote different nodes of the game tree. The dotted oval denotes the information set of the defender. Furthermore, notations and their meanings used in the proposed models are given in Table A1 in Appendix D.

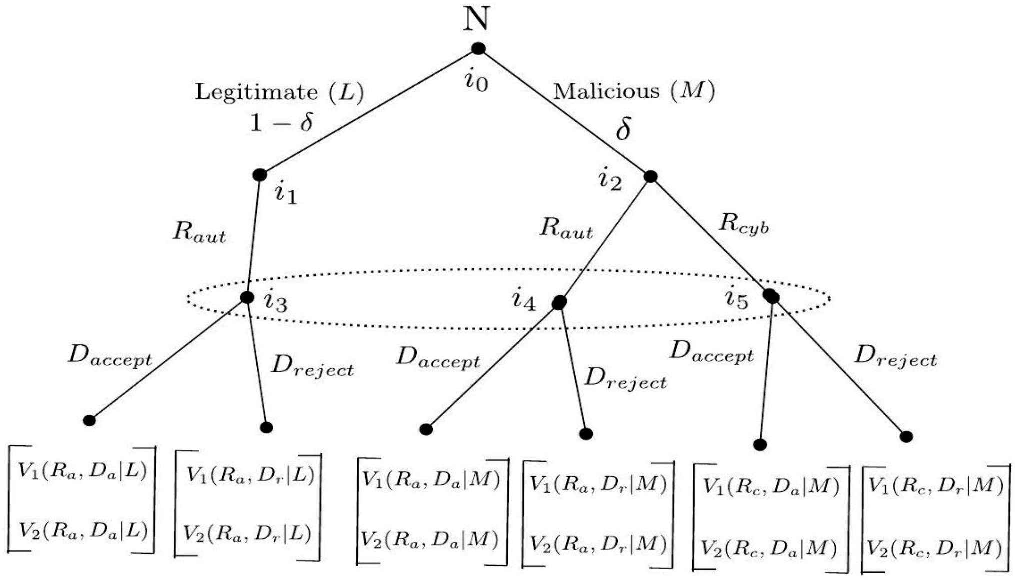

N
i_0
Legitimate (L)
$1-\delta$
Malicious (M)
δ
i_1
i_2
R_{aut}
R_{aut}
R_{cyb}
i_3
i_4
i_5
D_{accept}
D_{reject}
D_{accept}
D_{reject}
D_{accept}
D_{reject}
$V_1(R_a, D_a|L)$ $V_2(R_a, D_a|L)$
$V_1(R_a, D_r|L)$ $V_2(R_a, D_r|L)$
$V_1(R_a, D_a|M)$ $V_2(R_a, D_a|M)$
$V_1(R_a, D_r|M)$ $V_2(R_a, D_r|M)$
$V_1(R_c, D_a|M)$ $V_2(R_c, D_a|M)$
$V_1(R_c, D_r|M)$ $V_2(R_c, D_r|M)$

Figure 2. Extensive form of the simultaneous move game model.

3.2.1. Payoff Functions

Now, we describe the payoff functions of the game model. Consider a strategy profile $(R_{\text{aut}}\ , D_{\text{accept}}\ )$ for $i \in \mathcal{N}$ given an insider is of legitimate type L. In this case, a legitimate insider sends a data access request and the defender accepts it. As a result, both the insider and the defender receive a certain payoff whose value is normalized to 1, i.e., $V_i(R_{\text{aut}}\ , D_{\text{accept}}\ \mid L) = 1$, whereas a legitimate insider and the defender receive payoff zero if the access request is rejected, i.e., $V_i(R_{\text{aut}}\ , D_{\text{reject}}\ \mid L) = 0$, $i \in \mathcal{N}$. In the case of a malicious insider, if the data access request is accepted, the insider receives payoff β with probability $(1-p_1)$, and this is represented as $V_1(R_{\text{aut}}\ , D_{\text{accept}}\ \mid M) = (1-p_1)\beta$. On the other hand, the defender receives payoff $-\omega$ with probability $(1-p_1)$ and, therefore,

$V_2(R_{\text{aut}}, D_{\text{accept}} \mid M) = (1-p_1)(-\omega)$. In addition, if a malicious insider sends a data request and the request is rejected, both the insider and the defender receive payoff 0, i.e., $V_1(R_{\text{aut}}, D_{\text{reject}} \mid M) = 0$ and $V_2(R_{\text{aut}}, D_{\text{reject}} \mid M) = 0$. However, if a malicious insider launches a cyberattack to access the data and the data are released, the insider receives payoff β at the cost of the cyberattack $C_{cyb} \in (0,1)$, i.e., $V_1\left(R_{cyb}, D_{\text{accept}} \mid M\right) = \beta - C_{cyb}$, whereas the defender receives $-\omega$, i.e., $V_2\left(R_{\text{cyb}}, D_{\text{accept}} \mid M\right) = -\omega$. Furthermore, a malicious insider who sends a data access request through a cyberattack receives $-C_{cyb}$ if the request is rejected and the defender also receives payoff zero, i.e., $V_1\left(R_{cyb}, D_{\text{reject}} \mid M\right) = -C_{cyb}$ and $V_2\left(R_{cyb}, D_{\text{reject}} \mid M\right) = 0$.

Thus, we can express the expected payoff function of $i \in \mathcal{N}$, which is given by $U_i : S_I \times S_D \mapsto \mathbb{R}$, where $U_1(R^M_{\text{aut}} R^L_{\text{aut}}, D_{\text{accept}}) = \delta V_1(R_{\text{aut}}, D_{\text{accept}} \mid M) + (1-\delta)V_1 (R_{\text{aut}}, D_{\text{accept}} \mid L) = \delta[(1-p_1)\beta] + (1-\delta)$. In addition, $U_2(R^M_{\text{aut}} R^L_{\text{aut}}, D_{\text{accept}}) = \delta V_2(R_{\text{aut}}, D_{\text{accept}} \mid M) + (1-\ \delta)V_2(R_{\text{aut}}, D_{\text{accept}} \mid L) = \delta[(1-p_1)(-\omega)] + (1-\delta)$.

Similarly, the other expected payoffs corresponding to different strategy profiles can be expressed as $U_1(R^M_{\text{aut}} R^L_{\text{aut}}, D_{\text{reject}}) = 0, U_2(R^M_{\text{aut}} R^L_{\text{aut}}, D_{\text{reject}}) = 0, U_1\left(R^M_{\text{cyb}} R^L_{\text{aut}}, D_{\text{accept}}\right) = \delta\left[\beta - C_{cyb}\right] + (1-\delta), U_2\left(R^M_{cyb} R^L_{\text{aut}}, D_{\text{accept}}\right) = \delta[(-\omega)] + (1-\delta), U_1\left(R^M_{cyb} R^L_{\text{aut}}, D_{\text{reject}}\right) = \delta\left(-C_{cyb}\right)$ and $U_2\left(R^M_{cyb} R^L_{\text{aut}}, D_{\text{reject}}\right) = 0$.

3.2.2. Solution of the Game: Bayesian Nash Equilibrium (BNE)

Let $x_1 = \frac{1}{1+\omega(1-p_1)}$ and $y_1 = \frac{1}{1+\omega}$. Then, we solve the game model and present the solution in the following proposition.

Proposition 1. *(i) If $C_{cyb} < \beta p_1$, then*

$$BNE(\Gamma) = \begin{cases} \textit{Unique pure strategy } \left(R^M_{cyb} R^L_{aut}, D_{accept}\right) & \textit{if } 0 < \delta < y_1 \\ \textit{Mixed strategy } (\lambda^*, 1-\lambda^*) \textit{ and } (\eta^*, 1-\eta^*) & \textit{if } y_1 < \delta < x_1 \\ \textit{Unique pure strategy } (R^M_{aut} R^L_{aut}, D_{reject}) & \textit{if } x_1 < \delta < 1 \end{cases} \quad (1)$$

Here, η^* and λ^* are given by Equation (A1) and Equation (A2), respectively, in Appendix A.
(ii) If $C_{cyb} > \beta p_1$, then

$$BNE(\Gamma) = \begin{cases} \textit{Unique pure strategy } (R^M_{aut} R^L_{aut}, D_{accept}) & \textit{if } 0 < \delta < x_1 \\ \textit{Unique pure strategy } (R^M_{aut} R^L_{aut}, D_{reject}) & \textit{if } x_1 < \delta < 1 \end{cases} \quad (2)$$

Proof. See Appendix A. □

The results of Proposition 1 provide insights into the optimal strategies of insiders (malicious or legitimate) and defenders based on the probability δ of an insider being malicious. The solutions are categorized based on the relationship between the cost of a cyberattack C_{cyb} and the benefit of the attack βp_1.

When $C_{cyb} < \beta p_1$,

- If $0 < \delta < y_1$, the unique pure strategy equilibrium suggests that malicious insiders opt for cyberattacks $\left(R^M_{cyb}\right)$, while legitimate insiders choose authentication (R^L_{aut}). The defender, in response, accepts the data access request (D_{accept}).

- If $y_1 < \delta < x_1$, a mixed strategy equilibrium emerges, with malicious insiders alternating between cyberattacks and authentication (λ^* and $1-\lambda^*$) and legitimate insiders also using authentication with probability λ^*. The defender adapts probabilistically.
- If $x_1 < \delta < 1$, both malicious and legitimate insiders choose authentication $\left(R_{\text{aut}}^{M}\ R_{\text{aut}}^{L}\right)$ but the defender rejects the access request $\left(D_{\text{reject}}\right)$.

This scenario illustrates the increasing cautiousness of the defender as the probability of an insider being malicious (δ) rises. For lower values of δ, the defender prefers to grant access, balancing potential risks. For intermediate values, the strategies diversify, reflecting uncertainty. For high δ, a strict rejection policy dominates, protecting sensitive data.

When $C_{cyb} > \beta p_1$,

- If $0 < \delta < x_1$, the unique pure strategy equilibrium involves all insiders choosing authentication (R_{aut}^{M}, R_{aut}^{L}), and the defender grants access $\left(D_{\text{accept}}\right)$.
- If $x_1 < \delta < 1$, the strategy shifts, with all insiders continuing to authenticate, but the defender now rejects access (D_{reject}).

Higher costs of launching a cyberattack discourage malicious insiders from pursuing such strategies. The defender's responses align with the increasing probability of malicious intent, transitioning from acceptance to rejection as δ grows.

The results demonstrate how the interplay between attack cost, benefit, and malicious probability (δ) governs the strategic behavior of both insiders and the defender.

3.2.3. Extended Simultaneous Move Game Model

In the previous game model, the probability that a malicious insider who launches a cyberattack is detected is not considered. Therefore, the game model is insufficient to capture the behavior of malicious insiders who can carry out a cyberattack to gain data access. Hence, we consider this aspect and discuss the extended model (denoted by Γ_1) by incorporating this probability. To this end, let p_2 denote the probability that the identity of the malicious insider and his/her activity are discovered and assume that $p_1 > p_2$. Recall that β is the payoff (or gain) to the attacker due to the data compromised and $-\beta$ measures the intensity of penalty to the attacker if detected, i.e., the higher the value of β, the greater the severity of the penalty, and $\omega \in (0,1)$ is the payoff to the defender due to the discovery of a malicious insider identity or the protection of data. Additionally, $-\omega$ measures the loss due to data compromise or failure to discover the malicious insider identity. Furthermore, corresponding to the proper/smooth functioning of the project work, payoff 1 is assigned. In contrast, penalty 0 is assigned to both the legitimate insider and the defender for rejecting a legitimate data access request. In this case, the data are withheld, causing inefficiency in the project work.

Now, suppose that an insider of the legitimate type sends a data access request to the data defender. This request is responded to by the defender using accept $\left(D_{\text{accept}}\right)$. Therefore, the corresponding payoff functions can be written as $V_i\left(R_{\text{aut}}, D_{\text{accept}} \mid L\right) = 1, i \in \mathcal{N}$. On the other hand, rejecting the request results in the payoff function $V_i\left(R_{\text{aut}}, D_{\text{reject}} \mid L\right) = 0, i \in \mathcal{N}$.

Consider that a malicious insider sends a data access request through authentication, and this is accepted by the defender; the payoff of the malicious insider can be written as $V_1\left(R_{\text{aut}}, D_{\text{accept}} \mid M\right) = p_1(-\beta) + (1-p_1)\beta$. On the other hand, if the request is accepted, the payoff to the defender is given by $V_2\left(R_{\text{aut}}, D_{\text{accept}} \mid M\right) = p_1\omega + (1-p_1)(-\omega)$. Also, consider that a malicious insider sends a data request through authentication and the request is rejected by the defender. In this case, both the malicious insider and the defender receive the payoff 0. Therefore, the insider's payoff function is given by $V_i\left(R_{\text{aut}}, D_{\text{reject}} \mid M\right) = 0, i \in \mathcal{N}$.

Furthermore, if an insider makes a data access request through a cyberattack and the request is accepted, then the corresponding payoff functions can be written as $V_1\left(R_{cyb}, D_{\text{accept}} \mid M\right) = p_2(-\beta) + (1-p_2)\beta - C_{cyb}$. Moreover, as for the defender, the payoff function is $V_2\left(R_{\text{cyb}}, D_{\text{accept}} \mid M\right) = p_2(\omega) + (1-p_2)(-\omega)$. Also, when the malicious insider request is rejected by the defender, we have $V_1\left(R_{cyb}, D_{\text{reject}} \mid M\right) = -C_{cyb}$ and $V_2\left(R_{\text{cyb}}, D_{\text{reject}} \mid M\right) = 0$.

Thus, we can write the expected payoff function of $i \in \mathcal{N}, U_i : S_I \times S_D \mapsto \mathbb{R}$, where

$$U_1\left(R^M_{aut}\, R^L_{aut}, D_{accept}\right) = \delta V_1\left(R_{aut}, D_{accept} \mid M\right) + (1-\delta)V_1\left(R_{aut}, D_{accept} \mid L\right).$$
$$or\ U_1\left(R^M_{aut}\, R^L_{aut}, D_{accept}\right) = \delta[p_1(-\beta) + (1-p_1)\beta] + (1-\delta).$$

Also, $U_2\left(R^M_{\text{aut}}\, R^L_{\text{aut}}, D_{\text{accept}}\right) = \delta V_2\left(R_{\text{aut}}, D_{\text{accept}} \mid M\right) + (1-\delta)V_2\left(R_{\text{aut}}, D_{\text{accept}} \mid L\right)$ or $U_2\left(R^M_{\text{aut}}\, R^L_{\text{aut}}, D_{\text{accept}}\right) = \delta[p_1\omega + (1-p_1)(-\omega)] + (1-\delta)$. The expected payoff functions corresponding to the other strategy profiles can be obtained similarly.

3.2.4. Solution of the Extended Simultaneous Move Game Model

Let $x^* = \frac{1}{1+\omega(1-2p_1)}$ and $y^* = \frac{1}{1+\omega(1-2p_2)}$. We have the following proposition:

Proposition 2. *(i) If $C_{cyb} < 2\beta(p_1 - p_2)$, then*

$$BNE(\Gamma_1) = \begin{cases} \textit{Unique pure strategy } \left(R^M_{cyb}R^L_{aut}, D_{accept}\right) & \textit{if } 0 < \delta < y^* \\ \textit{Mixed strategy } \left(\lambda^*_1, 1-\lambda^*_1\right) \textit{ and } \left(\eta^*_1, 1-\eta^*_1\right) & \textit{if } y^* < \delta < x^* \\ \textit{Unique pure strategy } \left(R^M_{aut}R^L_{aut}, D_{reject}\right) & \text{if } x^* < \delta < 1 \end{cases} \quad (3)$$

The mixed strategies η^*_1 and λ^*_1 are given by Equation (A13) and Equation (A16), respectively, in Appendix B.

(ii) If $C_{cyb} > 2\beta(p_1 - p_2)$, then

$$BNE(\Gamma_1) = \begin{cases} \textit{Unique pure strategy } \left(R^M_{aut}\, R^L_{aut}, D_{accept}\right) & \textit{if } 0 < \delta < x^* \\ \textit{Unique pure strategy } \left(R^M_{aut}\, R^L_{aut}, D_{reject}\right) & \textit{if } x^* < \delta < 1 \end{cases} \quad (4)$$

Proof. See Appendix B. □

The results of Proposition 2 extend the analysis by considering two probability parameters, p_1 and p_2, representing the likelihoods of malicious behavior by insiders under different conditions. The equilibrium strategies are influenced by the relationship between the cost of a cyberattack $\left(C_{cyb}\right)$ and the threshold value $2\beta(p_1 - p_2)$.

When $C_{cyb} < 2\beta(p_1 - p_2)$,

- If $0 < \delta < y^*$, the unique pure strategy equilibrium indicates that malicious insiders launch cyberattacks $\left(R^M_{cyb}\right)$, legitimate insiders authenticate $\left(R^L_{\text{aut}}\right)$, and the defender accepts the access request $\left(D_{\text{accept}}\right)$.
- If $y^* < \delta < x^*$, t mixed strategy equilibrium arises, with malicious insiders mixing between cyberattacks and authentication strategies $\left(\lambda^*_1 \text{ and } 1-\lambda^*_1\right)$ and legitimate insiders also adopting a probabilistic authentication strategy $\left(\eta^*_1 \text{ and } 1-\eta^*_1\right)$. The defender adjusts probabilistically.
- If $x^* < \delta < 1$, both malicious and legitimate insiders select authentication $\left(R^M_{aut}, R^L_{aut}\right)$ but the defender rejects the access request $\left(D_{\text{reject}}\right)$.

For $C_{cyb} < 2\beta(p_1 - p_2)$, the defender's strategies shift dynamically as δ (the probability of a malicious insider) increases:

- At low δ, the defender is inclined to accept requests, reflecting a trust-oriented strategy when the malicious probability is low.
- For intermediate δ, mixed strategies dominate, reflecting the defender's uncertainty and the malicious insider's strategic adaptation.
- At high δ, rejection becomes the optimal strategy to mitigate the risk posed by potentially malicious insiders.

When $C_{cyb} > 2\beta(p_1 - p_2)$,

- If $0 < \delta < x^*$, the unique pure strategy equilibrium involves all insiders selecting authentication $\left(R_{aut}^M, R_{aut}^L\right)$ and the defender accepts the request $\left(D_{\text{accept}}\right)$.
- If $x^* < \delta < 1$, the strategy shifts, with all insiders continuing to authenticate, but the defender rejects the access request (D_{reject}).

Higher costs of launching a cyberattack (C_{cyb}) discourage malicious insiders from attacking, leading to more consistent behavior. The defender's response aligns with the increasing probability of malicious insiders, transitioning from acceptance to rejection as δ grows.

The results illustrate how the interplay between attack cost, insider probabilities, and the likelihood parameters p_1 and p_2 governs the strategic behavior of insiders and defenders. These findings provide a theoretical foundation for designing adaptive defense mechanisms that respond to varying insider threat scenarios.

3.3. Sequential Move Game Model

In the previous section, we considered a simultaneous move game model in which each of the players takes an action simultaneously without knowing the actions taken by the other player. In this section, we consider the attack dynamics where an insider makes a data access request, which is observed by a data defender who has prior beliefs about the insider and responds to the request based on the updated beliefs of the insider type.

Let us recall that a malicious insider can request data access in two ways: (i) authentication (misuse of privilege) and (ii) cyberattack, such as defense bypass, to evade detection from the IDS [38]. When an insider makes a data request through authentication, the defender observes this activity. Although the defender perceives that the request is made using an authentication, he/she has prior beliefs that the access request comes from a malicious insider with probability δ. Hence, for the defender, accepting a request that comes from authentication is not always optimal. Moreover, when an insider tries to gain access to data through a cyberattack, another challenging decision problem faced by the defender would be whether it is always optimal to reject the suspicious request. This might not always be optimal because a malicious insider's identity cannot be discovered by rejecting the access request, thereby providing him/her with another opportunity to launch attacks in the future. In fact, accepting a suspicious request at the cost of data security can lead to the detection of malicious activity as well as the discovery of a malicious insider's identity. As a result, the project team can get rid of the malicious insider to enhance data security. However, at the same time, accepting a suspicious request is not always optimal, as there is a probability that the malicious insider identity might not be discovered at all. Thus, we develop a sequential move Bayesian game model (which is denoted as Γ_2) to capture this scenario and predict a malicious insider's behavior as well as the best strategies to respond to the attack.

We assume that the defender employs an IDS to monitor access requests. When an insider (legitimate/malicious) makes a data access request through authentication, no alarm is triggered by the IDS for the request since the necessary authentication process is performed by the insider. However, when a malicious insider makes a data access request utilizing a cyberattack to gain access to data, an alarm is triggered by the IDS. The extensive form of the game model is shown in Figure 3. Note that in the sequential game model, the defender has two information sets denoted by a dotted oval. In contrast, in the simultaneous move game model, the defender has only one information set (see Figure 2).

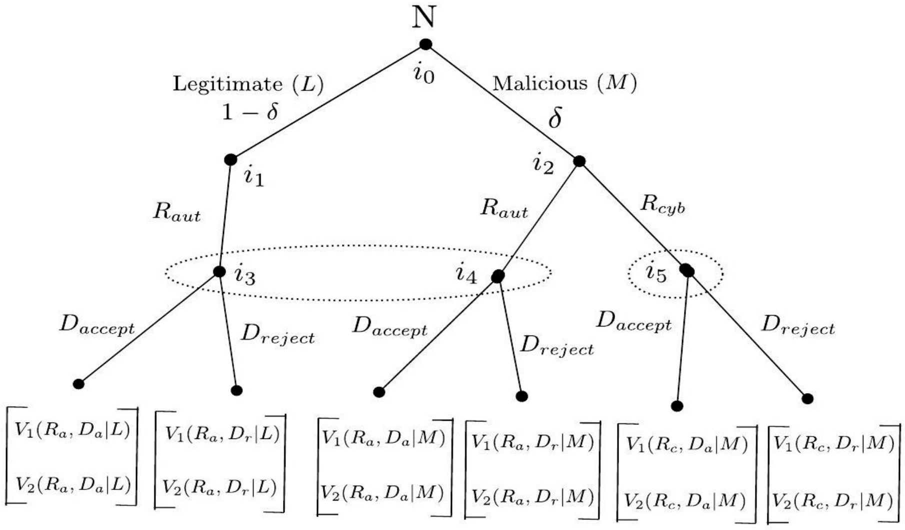

N
i_0
Legitimate (L)
$1-\delta$
Malicious (M)
δ
i_1
i_2
R_{aut}
R_{aut}
R_{cyb}
i_3
i_4
i_5
D_{accept}
D_{reject}
D_{accept}
D_{reject}
D_{accept}
D_{reject}
$V_1(R_a, D_a|L)$ $V_2(R_a, D_a|L)$
$V_1(R_a, D_r|L)$ $V_2(R_a, D_r|L)$
$V_1(R_a, D_a|M)$ $V_2(R_a, D_a|M)$
$V_1(R_a, D_r|M)$ $V_2(R_a, D_r|M)$
$V_1(R_c, D_a|M)$ $V_2(R_c, D_a|M)$
$V_1(R_c, D_r|M)$ $V_2(R_c, D_r|M)$

Figure 3. Extensive form of the sequential move game model.

Now, the strategy sets of an insider and defender can be written as

$$\begin{aligned} S_I' &= \left\{ R^M_{aut}\;R^L_{aut}\,, R^M_{cyb}\;R^L_{aut} \right\}. \\ S_D' &= \left\{ D^{aut}_{accept}\;D^{cyb}_{accept}\,, D^{aut}_{accept}\;D^{cyb}_{reject}\,, D^{aut}_{reject}\;D^{cyb}_{accept}\,, D^{aut}_{reject}\;D^{cyb}_{reject} \right\}. \end{aligned}$$

The meaning of elements in $S_I^{'}$ can be interpreted as in the case of the elements of S_1 of the simultaneous move game model. The elements of $S_D^{'}$, however, have different interpretations. That is, $D^{\text{aut}}_{\text{accept}}\;D^{cyb}_{\text{reject}}$ denotes the defender's strategy, in which the defender accepts the data request if he/she observes that it comes from an authentication process, whereas he/she rejects the access request if it comes through a cyberattack. The other strategies can be interpreted similarly.

Thus, the payoff matrix of the game model can be written as

$$R^M_{aut}\;R^L_{aut}\;R^M_{cyb}\;R^L_{aut} \begin{bmatrix} D^{aut}_{accept}\;D^{cyb}_{accept} & D^{aut}_{accept}\;D^{cyb}_{reject} & D^{aut}_{reject}\;D^{cyb}_{accept} & D^{aut}_{reject}\;D^{cyb}_{reject} \\ (x_{11}, y_{11}) & (x_{12}, y_{12}) & (x_{13}, y_{13}) & (x_{14}, y_{14}) \\ (x_{21}, y_{21}) & (x_{22}, y_{22}) & (x_{23}, y_{23}) & (x_{24}, y_{24}) \end{bmatrix}$$

Here, $x_{11} = U_1^{'}\left(R^M_{\text{aut}}\;R^L_{\text{aut}}\,, D^{\text{aut}}_{\text{accept}}\;D^{cyb}_{\text{accept}}\right)$ and $y_{11} = U_2^{'}\left(R^M_{\text{aut}}\;R^L_{\text{aut}}\,, D^{\text{aut}}_{\text{accept}}\;D^{cyb}_{\text{accept}}\right)$. Similarly, the other x_{ij} and y_{ij} s have their corresponding values. The x_{ij} and y_{ij} s can be expressed as

$$\begin{aligned} x_{11} &= U_1'\left(R^M_{aut}\;R^L_{aut}\,, D^{aut}_{accept}\;D^{cyb}_{accept}\right) = \delta V_1\left(R_{aut}\,, D_{accept}\;\mid M\right) + (1-\delta)V_1\left(R_{aut}\,, D_{accept}\;\mid L\right). \\ y_{11} &= U_2'\left(R^M_{aut}\;R^L_{aut}\,, D^{aut}_{accept}\;D^{cyb}_{accept}\right) = \delta V_2\left(R_{aut}\,, D_{accept}\;\mid M\right) + (1-\delta)V_2\left(R_{aut}\,, D_{accept}\;\mid L\right). \end{aligned}$$

Similarly, we can write the expressions for the other payoffs.

3.3.1. Solution of the Sequential Move Game Model

Let $x^* = \frac{1}{1+\omega(1-2p_1)}$. Then, we have the following proposition:

Proposition 3. *When* $p_2 < \frac{1}{2}$,

(i) If $\delta < x^*$

$$BNE(\Gamma_2) = \begin{cases} \left(R_{aut}^M\ R_{aut}^L\ , D_{accept}^{aut}\ D_{reject}^{cyb}\right) & \text{if } C_{cyb} > \beta(2p_1 - 1) \\ \left(R_{cyb}^M\ R_{aut}^L\ , D_{accept}^{aut}\ D_{reject}^{cyb}\right) & \text{if } C_{cyb} < \beta(2p_1 - 1) \end{cases} \quad (5)$$

(ii) If $\delta > x^*$,

$$BNE(\Gamma_2) = \begin{cases} \text{No equilibria} & \text{if } C_{cyb} < \beta(2p_1 - 1) \\ \left(R_{aut}^M\ R_{aut}^L\ , D_{reject}^{aut}\ D_{reject}^{cyb}\right) & \text{if } C_{cyb} > \beta(2p_1 - 1) \end{cases} \quad (6)$$

Proof. See Appendix C. □

Proposition 4. *When* $p_2 > \frac{1}{2}$,

(i) If $\delta < x^*$*, then*

$$BNE(\Gamma_2) = \begin{cases} \left(R_{cyb}^M\ R_{aut}^L\ , D_{accept}^{aut}\ D_{accept}^{cyb}\right) & \text{if } C_{cyb} < 2\beta(p_1 - p_2) \\ \left(R_{aut}^M\ R_{aut}^L\ , D_{accept}^{aut}\ D_{accept}^{cyb}\right) & \text{if } C_{cyb} > 2\beta(p_1 - p_2) \end{cases} \quad (7)$$

(ii) If $\delta > x^*$*, then*

$$BNE(\Gamma_2) = \left\{ \text{No equilibria} \quad \text{for } C_{cyb} \in (0,1) \right. \quad (8)$$

Proof. See Appendix D. □

BNE of the sequential move game can be represented by a flowchart based on Propositions 3 and 4, as shown in Figure 4.

Propositions 3 and 4 provide insights into optimal strategies under different conditions for p_1, p_2, δ, and C_{cyb}. Here, p_1 represents the probability that a malicious insider launching authentication (R_{aut}^M) to commit malicious acts is detected, while p_2 represents the probability that a malicious insider launching a cyberattack $\left(R_{cyb}^M\right)$ is detected. When the probability that a malicious insider using a cyberattack is detected is smaller than $\frac{1}{2}$, i.e., $p_2 < \frac{1}{2}$, two cases arise:

Case (i): $\delta < x^*$ (i.e., the probability that an insider is malicious is less than the value x^*).

If $C_{cyb} > \beta(2p_1 - 1)$,

- *Insider Strategy*: Both malicious and legitimate insiders choose authentication $(R_{aut}^M R_{aut}^L)$.
- *Defender Strategy:* The defender accepts authentication requests (D_{accept}^{aut}) but rejects cyberattacks $\left(D_{\text{reject}}^{cyb}\right)$.

If $C_{cyb} < \beta(2p_1 - 1)$,

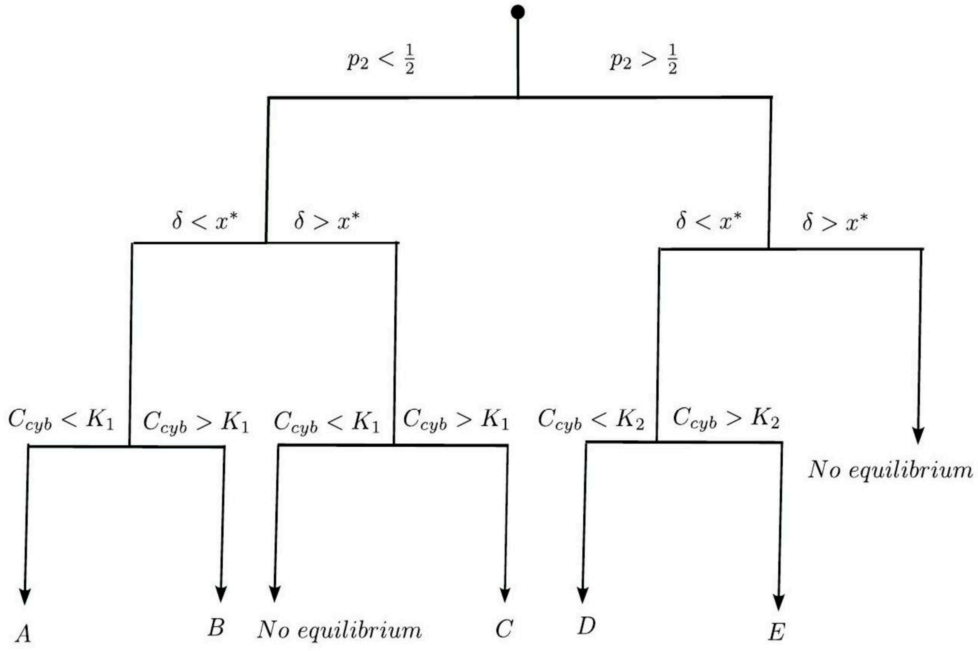
- *Insider Strategy*: Malicious insiders choose cyberattack and legitimate insiders choose authentication $\left(R^{M}_{cyb}R^{L}_{aut}\right)$.
- *Defender Strategy:* The defender accepts authentication requests $\left(D^{\text{aut}}_{\text{accept}}\right)$ but rejects cyberattacks $\left(D^{cyb}_{\text{reject}}\right)$.

Case (ii): $\delta > x^{*}$ (i.e., the probability that an insider is malicious is greater than x^{*}).
If $C_{cyb} < \beta(2p_1 - 1)$,

- *Outcome:* No equilibrium exists because the defender cannot effectively balance the cost of rejecting requests and the risk of allowing malicious activity.

If $C_{cyb} > \beta(2p_1 - 1)$,

- *Insider Strategy:* Both malicious and legitimate insiders choose authentication ($R^{M}_{\text{aut}}\ R^{L}_{\text{aut}}$).
- *Defender Strategy:* The defender rejects both authentication requests and cyberattacks $\left(D^{aut}_{\text{reject}}\ D^{cyb}_{\text{reject}}\right)$.



where $x^* = \frac{1}{1+\omega(1-2p_1)}$, $A = (R^M_{cyb}R^L_{aut}, D^{aut}_{accept}D^{cyb}_{reject})$, $B = (R^M_{aut}R^L_{aut}, D^{aut}_{accept}D^{cyb}_{reject})$,
$K_1 = \beta(2p_1 - 1)$, $C = (R^M_{aut}R^L_{aut}, D^{aut}_{reject}D^{cyb}_{reject})$, $D = (R^M_{cyb}R^L_{aut}, D^{aut}_{accept}D^{cyb}_{accept})$,
$K_2 = 2\beta(p_1 - p_2)$, $E = (R^M_{aut}R^L_{aut}, D^{aut}_{accept}D^{cyb}_{accept})$.

Figure 4. Flowchart of BNE.

For $p_2 < \frac{1}{2}$, the defender's strategy depends on the cost of the cyberattack $\left(C_{cyb}\right)$ and the probability of discovering a malicious insider. At lower values of δ, when the probability of malicious insiders is low, the defender is more likely to accept authentication requests while rejecting cyberattacks. At higher δ, the defender increasingly rejects all requests to safeguard sensitive data.

In addition, when the probability that a malicious insider using a cyberattack is detected is greater than $\frac{1}{2}$, *i.e.*, $p_2 > \frac{1}{2}$, two cases arise:

Case (i): $\delta < x^{*}$ (i.e., the probability that an insider is malicious is less than x^{*}).
If $C_{cyb} < 2\beta(p_1 - p_2)$,

- *Insider Strategy:* Malicious insiders choose cyberattack and legitimate insiders choose authentication $\left(R_{cyb}^{M} R_{aut}^{L}\right)$.
- *Defender Strategy:* The defender accepts all requests $\left(D_{\text{accept}}^{aut}\ D_{\text{accept}}^{cyb}\right)$.

  If $C_{cyb} > 2\beta(p_1 - p_2)$,
- *Insider Strategy:* Both malicious and legitimate insiders choose authentication $(R_{aut}^{M} R_{\text{aut}}^{L})$.
- *Defender Strategy:* The defender accepts all requests $\left(D_{\text{accept}}^{aut}\ D_{\text{accept}}^{cyb}\right)$.

  Case (ii): $\delta > x^*$ (i.e., the probability that an insider is malicious is greater than x^*). For $C_{cyb} \in (0,1)$,
- *Outcome:* No equilibrium exists because the defender cannot formulate a consistent response strategy for high δ.

For $p_2 > \frac{1}{2}$, the defender's acceptance of cyberattacks increases because the high likelihood of detecting malicious insiders diminishes the risks associated with granting access. However, when δ is high, the absence of equilibria underscores the challenges of managing insider threats under uncertain conditions.

These findings provide actionable insights for dynamically adjusting defense strategies based on observed actions and varying probabilities of insider behavior. The results demonstrate that sequential-move games introduce strategic complexity, where the defender must adapt to observed insider actions. The balance between the acceptance and rejection of requests is influenced by factors such as the cost of cyberattacks, the likelihood of detecting malicious insiders, and the probability of malicious behavior.

3.3.2. Perfect Bayesian Nash Equilibrium (PBE)

Sometimes, players are not sequentially rational in their behavior in the BNE strategies. Therefore, we explore the players' behavior in the game model to determine whether their behavior predicted by the equilibrium solutions is consistent. If it is consistent, the strategy is called perfect Bayesian Nash equilibrium (PBE).

(i) Now, we verify that the BNEs given by Equation (5) are the PBEs.

Let $\mu(i_3 \mid R_{\text{aut}})$ and $\mu(i_4 \mid R_{\text{aut}})$ denote the posterior beliefs that an insider is legitimate (L) and malicious (M), respectively, given that the insider takes action R_{aut}. In addition, let $\mu\left(i_5 \mid R_{cyb}\right)$ denote the posterior belief that an insider is malicious (M), conditional on the insider choosing action R_{cyb}.

The posterior belief is updated based on the Bayes' rule:

$$\mu(i_3 \mid R_{\text{aut}}) = \frac{P(\text{ Insider is legitimate and chooses } R_{\text{aut}})}{P(\text{ Insider is legitimate and chooses } R_{\text{aut}}) + P(\text{ Insider is malicious and chooses } R_{\text{aut}})}$$

or $\mu(i_3 \mid R_{\text{aut}}) = \frac{(1-\delta)\phi_L}{(1-\delta)\phi_L + \delta\phi_M}$,

where $\phi_L = P(\text{ Insider chooses } R_{\text{aut}} \mid \text{ Insider is legitimate (L)})$ and

$\phi_M = P(\text{ Insider chooses } R_{\text{aut}} \mid \text{ Insider is malicious (M)})$. Note that $\phi_L = 1$.

Thus, we can write the other posterior beliefs as below:

$$\mu(i_4 \mid R_{aut}) = \frac{\delta\phi_M}{\delta\phi_M + (1-\delta)\phi_L)}$$

$$\mu\left(i_5 \mid R_{cyb}\right) = \frac{\delta(1-\phi_M)}{\delta(1-\phi_M) + (1-\delta)(1-\phi_L)},$$

$$\text{or } \mu\left(i_5 \mid R_{cyb}\right) = 1 \text{ since } \phi_L = 1.$$

From Figure 3, we have two information sets of the defender: $H_1 = \{i_3, i_4\}$ and $H_2 = \{i_5\}$.

To see that $\left(R_{\text{aut}}^{M}\, R_{\text{aut}}^{L}\,, D_{\text{accept}}^{\text{aut}}\, D_{\text{reject}}^{cyb}\right)$ is a PBE of the game Γ_2, we consider the posterior beliefs $\mu \equiv \left[\mu(i_3 \mid R_{\text{aut}}\,), \mu(i_4 \mid R_{\text{aut}}\,), \mu\left(i_5 \mid R_{\text{cyb}}\,\right)\right]$.

The strategy $R_{\text{aut}}^{M}\, R_{\text{aut}}^{L}$ corresponds to $\phi_M = 1$ and $\phi_L = 1$ so that the posterior beliefs in H_1 become $\mu(i_3 \mid R_{\text{aut}}\,) = 1 - \delta, \mu(i_4 \mid R_{\text{aut}}\,) = \delta$. Therefore, the information set H_1 is reached with positive probability. However, H_2 is reached with zero probability for this strategy so that we can assign any posterior belief $\mu\left(i_5 \mid R_{cyb}\right) \in [0,1]$ [32]. Now, let us consider the expected payoffs to the defender due to the action D_{accept} in H_1, denoted by ψ,

$$\begin{aligned}&\psi = V_2\left(R_{\text{aut}}\,, D_{\text{accept}}\, \mid L\right)\mu(i_3 \mid R_{\text{aut}}\,) + V_2\left(R_{\text{aut}}\,, D_{\text{accept}}\, \mid M\right)\mu(i_4 \mid R_{\text{aut}}\,)\\ &\text{or } \psi = V_2\left(R_{\text{aut}}\,, D_{\text{accept}}\, \mid L\right)(1-\delta) + V_2\left(R_{\text{aut}}\,, D_{\text{accept}}\, \mid M\right)\delta.\end{aligned}$$

Now, the expected payoff to the defender due to the action D_{reject} denoted by $\psi^{'}$ in H_1 is given by

$$\begin{aligned}&\psi^{'} = V_2\left(R_{\text{aut}}\,, D_{\text{reject}}\, \mid L\right)\mu(i_3 \mid R_{\text{aut}}\,) + V_2\left(R_{\text{aut}}\,, D_{\text{reject}}\, \mid M\right)\mu(i_4 \mid R_{\text{aut}}\,)\\ &\text{or } \psi^{'} = V_2\left(R_{\text{aut}}\,, D_{\text{reject}}\, \mid L\right)(1-\delta) + V_2\left(R_{\text{aut}}\,, D_{\text{reject}}\, \mid M\right)\delta.\end{aligned}$$

It can be noticed that $\psi = y_{12}$ and $\psi^{'} = y_{14}$. Moreover, if $\delta \in \Delta_3$, we know that $y_{12} > y_{14}$, i.e., $\psi > \psi^{'}$. This implies that D_{accept} is the best response to R_{aut} in H_1. Furthermore, we need to show that D_{reject} is also the best response to R_{cyb} in H_2. Let ζ and $\zeta^{'}$ denote the expected payoffs due to the actions D_{accept} and D_{reject}, respectively, in H_2. Therefore, we can write

$$\begin{aligned}&\zeta = V_2\left(R_{\text{cyb}}\,, D_{\text{accept}}\, \mid M\right)\mu\left(i_5 \mid R_{\text{cyb}}\,\right) \text{ and}\\ &\zeta^{'} = V_2\left(R_{\text{cyb}}\,, D_{\text{reject}}\, \mid M\right)\mu\left(i_5 \mid R_{\text{cyb}}\,\right), \text{ where } \mu\left(i_5 \mid R_{\text{cyb}}\,\right) \in [0,1].\end{aligned}$$

It can be seen that $\zeta^{'} > \zeta$ when $p_2 < \frac{1}{2}$. Thus, we know that the defender plays the best response in each of the information sets H_1 and H_2. Hence, the strategy profile $\left(R_{\text{aut}}^{M}\, R_{\text{aut}}^{L}\,, D_{\text{accept}}^{\text{aut}}\, D_{\text{reject}}^{cyb}\right)$ is a PBE of Γ_2.

Also, consider the pure-strategy BNE $\left(R_{cyb}^{M} R_{\text{aut}}^{L}\,, D_{\text{accept}}^{\text{aut}}\, D_{\text{reject}}^{cyb}\right)$ given by Equation (5). This strategy corresponds to $\phi_M = 0$ and $\phi_L = 1$. This leads to the posterior beliefs $\mu(i_3 \mid R_{\text{aut}}\,) = 1, \mu(i_4 \mid R_{\text{aut}}\,) = 0$ and $\mu\left(i_5 \mid R_{\text{cyb}}\,\right) = 1$. It can be seen that with this strategy, the two information sets H_1 and H_2 are reached with positive probabilities. Furthermore, the defender plays the best response D_{accept} in H_1 with the updated posterior beliefs as the expected payoffs $\psi = V_2\left(R_{\text{aut}}\,, D_{\text{accept}}\,\right) \mid L)$ and $\psi^{'} = V_2\left(R_{\text{aut}}\,, D_{\text{reject}}\, \mid L\right)$ are such that $\psi > \psi^{'}$. Also, the defender plays the best response D_{reject} in H_2, i.e., $\zeta < \zeta^{'}$, where $\zeta = V_2\left(R_{\text{cyb}}\,, D_{\text{accept}}\, \mid M\right)$ and $\zeta^{'} = V_2\left(R_{\text{cyb}}\,, D_{\text{reject}}\, \mid M\right)$ and Equation (5) is derived subject to the constraint $p_2 < \frac{1}{2}$. Therefore, the defender plays the best response in both the information sets H_1 and H_2 and, hence, the strategy $\left(R_{cyb}^{M} R_{\text{aut}}^{L}\,, D_{\text{accept}}^{\text{aut}}\, D_{\text{reject}}^{cyb}\right)$ is a PBE.

(ii) The BNE of Equation (6) is a PBE. To see this, consider the strategy $\left(R_{\text{aut}}^{M}\, R_{\text{aut}}^{L}\,, D_{\text{reject}}^{\text{aut}}\, D_{\text{reject}}^{cyb}\right)$. For this strategy, $\phi_M = 1$ and $\phi_L = 1$. This implies that $\mu(i_3 \mid R_{\text{aut}}\,) = 1 - \delta$ and $\mu(i_4 \mid R_{\text{aut}}\,) = \delta$. Thus, the two information sets H_1 and H_2 are reached with positive probabilities. Moreover, the defender plays the best response D_{reject} in each of the information sets as $\psi^{'} > \psi$ and $\zeta^{'} > \zeta$ for $p < \frac{1}{2}$. Hence, the strategy $\left(R_{\text{aut}}^{M}\, R_{\text{aut}}^{L}\,, D_{\text{reject}}^{\text{aut}}\, D_{\text{reject}}^{cyb}\right)$ is a PBE.

(iii) Similar to the above discussion, it can be shown that the BNEs given by Equation (7) are PBEs.

4. Verification and Validation

One of the methods in scientific research involves first verifying a proposed mathematical model before its application and then validating its applicability [40]. Accordingly, we use the terms 'verification' and 'validation' in this work to refer to the correctness of the proposed model and its applicability in real-world scenarios, respectively. We employ Monte Carlo simulation experiments to verify the proposed model in Section 4.1, show their implementation using hypothetical scenarios in Section 4.2, and utilize real project data to validate the applicability of the proposed model in Section 4.3. Thus, verifying the model through simulation experiments ensures that the theoretical results align with the outcomes obtained from the simulations. Conversely, validating its applicability involves assessing whether the proposed model accurately represents real-world phenomena and scenarios.

4.1. Verification of the Proposed Models

One way to verify a mathematical model is to perform empirical analysis using actual data. In this study, the actual data required to verify the model are the details of a previous cyber incident involving malicious insiders. However, organizations usually prefer not to publish insider attack incidents for various reasons, such as reputation damage, loss of trust, legal and regulatory concerns, competitive disadvantage, and contractual considerations. Therefore, the unavailability of actual data necessitated using the Monte Carlo simulation to verify our proposed model. In fact, in the absence of actual data, simulation is a valuable tool to analyze mathematical models, as demonstrated by Ni et al. [13] and Kim et al. [15]. The authors [15] used Monte Carlo simulations to analyze their game models. Ni et al. [13] also performed simulations to analyze their game model due to the challenges in obtaining actual data for input parameters. Similarly, in this research, we used the Monte Carlo simulation to verify our proposed model.

For each game model, we analyzed the basic parameters β, ω, C_{cyb} and the probabilities p_1, p_2, and δ for both the simultaneous move and sequential move game models. In this experiment, we employed a Monte Carlo simulation, generating multiple parameter combinations to identify those that satisfied the constraints for each game model, where each parameter was normalized and, hence, randomized from $(0, 1)$. Regarding sampling techniques, we employed random sampling to generate parameter combinations across the defined parameter space. Each parameter was sampled from a uniform distribution within theoretically justified bounds, ensuring a comprehensive exploration of the game's strategic landscape. This approach was chosen for its simplicity and effectiveness in covering a wide range of scenarios without prior assumptions about parameter distributions.

The ranges for each parameter were determined based on theoretical considerations within the construction cybersecurity field. For instance, the parameter δ, which is the probability that an insider is malicious, was varied between 0 and 1 to cover all possible weights, reflecting a wide spectrum of game dynamics; p_1 (the probability that the identity of the malicious insider and his/her activity is discovered in the case of proper authentication) needed to be greater than p_2 (the probability that the identity of the malicious insider and his/her activity is discovered in the case of a cyberattack). We conducted many simulation runs for each parameter set to ensure the robustness and reliability of our results. This large number of runs leveraged the law of large numbers, allowing us to approximate the expected outcomes of strategies with high confidence.

The decision to randomize and normalize parameters within the 0 to 1 range is grounded in both theoretical considerations and practical assumptions. Specifically, parameters such as p_1, p_2, and δ represent probabilities, inherently necessitating their values to fall within the 0 to 1 interval. This ensures that their interpretation remains consistent with probabilistic theory. For parameters like C_{cyb}, ω, and β, which are related to costs and payoffs, normalizing their values to a 0 to 1 scale is a strategic choice aimed at establishing a universal and consistent framework for comparison. In real-world scenarios, absolute values of costs and payoffs can vary significantly across different contexts, such as varying scales of projects or financial capacities of companies. Normalizing these values facilitates a more generalized and adaptable model application.

For each parameter exploration, we conducted numerous simulations, approximately 10,000, which leveraged the law of large numbers to ensure the robustness of our model. Therefore, the simulation process adhered to the law of large numbers. This approach guaranteed the robustness and generalizability of our model. This approach allowed us to systematically sample and evaluate different parameter settings, ensuring the credibility of our simulation results. Once we found a parameter combination that met the constraints, we focused on visualizing and analyzing the mixed strategy probabilities $\lambda^*, 1-\lambda^*, \eta^*$, and $1-\eta^*$. To understand the impact of a particular parameter, we plotted the corresponding mixed strategy probabilities. We observed the resulting changes in the mixed strategy equilibrium probabilities by systematically varying the fixed parameters. Our experiments show that the simulation results are consistent with the theoretical results obtained based on the proposed models, and the simulation code is available on GitHub [41].

We plotted different graphs, such as Figures 5–8, based on the basic simultaneous move game model for numerical illustration purposes. From Figure 5, it can be observed that the mixed strategy equilibrium probability λ^* (this corresponds to an insider using authentication if malicious) increased as the probability that an insider was malicious (δ) increased. Moreover, as the probability of detecting an insider under authentication (p_1) increased, the probability that an insider used an authentication process, characterized by λ, decreased. In addition, in Figure 6, the probability that a malicious insider launched a cyberattack (i.e., $1-\lambda^*$) decreased as the probability of being malicious δ increased and the probability of carrying out a cyberattack $\left(1-\lambda^*\right)$ increased as the detection probability p_1 under authentication increased. Furthermore, Figure 7 shows that the equilibrium probability of accepting the request increased as the cost of the cyberattack increased, whereas the probability of rejecting the access request $1-\eta^*$ decreased as the cost of the cyberattack increased.

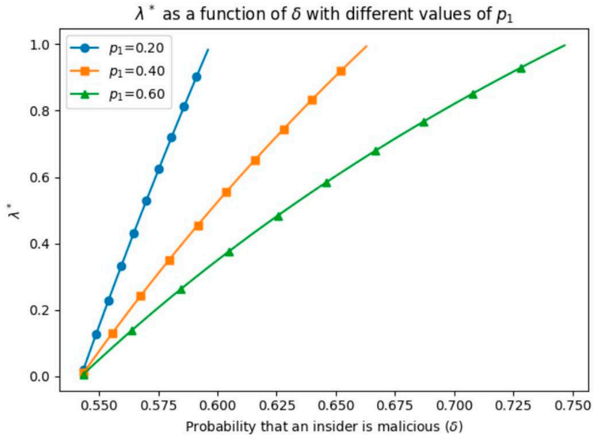


Figure 5. λ^* versus δ.

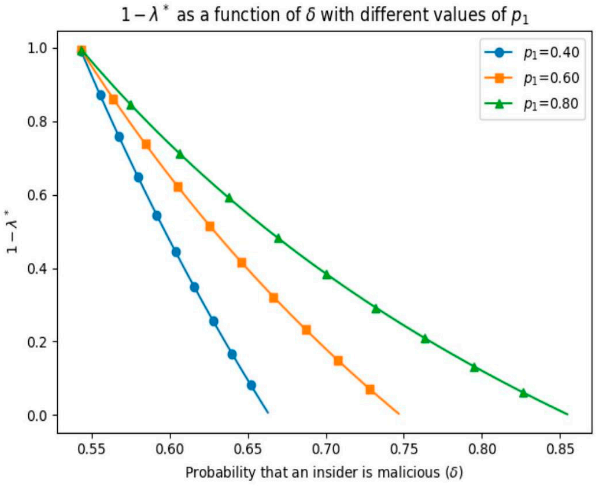


Figure 6. $1-\lambda^*$ versus δ.

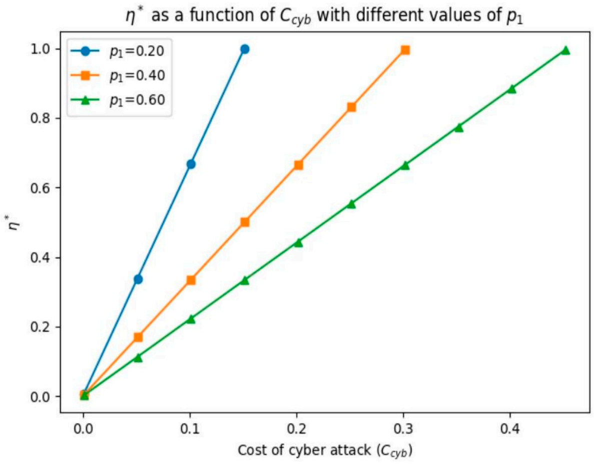


Figure 7. η versus C_{cyb}.

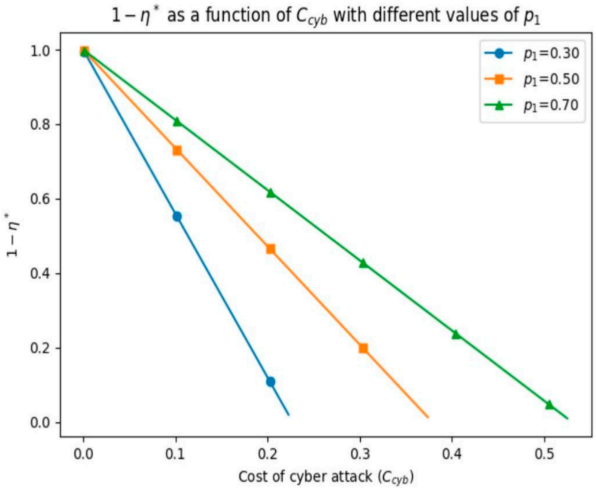


Figure 8. $1-\eta^*$ versus C_{cyb}.

4.2. Implementation of the Proposed Model in a Construction Example

This section illustrates the practical implementation of the proposed sequential game-theoretical model in the context of a construction project. Showing the implementation and presenting different scenarios are crucial for contextualizing the theory presented in Sections 4 and 5. The proposed models involve an insider with a parameter directly related to its characteristics: the probability that an insider is malicious (δ). The other party involved in the game-theoretic models is the data defender. Considering that the data defender manages the access control using a role-based method, the role of the insider in the project mainly defines the initial δ value. Therefore, understanding different possible roles in a construction project is essential before showing the proposed models' implementation. A high-level list of roles in a construction project using BIM is presented in Table 2. Most roles shown below were taken from Hughes and Murdoch [42], and BIM- and IT-related roles were added to the list to make it up-to-date and more relevant to this study. Moreover, a procurement method with separate design and construction responsibilities was assumed. Only the roles that were assumed to have access to the project IT network were included.

Table 2. Different categories and roles.

Categories	**Sub-Categories**	**Sample Roles**
Client	(i) Client	Client
	(ii) Client's representative	Client project manager Client liaison officer
Advisor/Consultant	(i) Management	Project manager Construction manager Design coordinator Design manager BIM coordinator BIM manager
	(ii) Design	Architectural designer Civil and structural engineer Geotechnical engineer Mechanical and electrical engineer Fire engineer
	(iii) Financial	Cost consultant Cost planner Quantitative surveyor
Builders and contractors	(i) Constructor	Project manager Construction manager Construction scheduler Construction cost estimator Contract manager Site manager Site engineer Quantitative surveyor BIM manager BIM coordinator BIM specialist IT manager IT specialist Business manager Human resource manager Administrator
	(ii) Partial responsibility	Sub-contractor

The list of roles in Table 2 can be extended or reduced depending on project characteristics. However, it is clear that not all roles have the same initial probability of being a malicious insider δ_{initial} in a project. For example, the initial probability of a client being malicious should not be assumed to be the same as the initial probability of a sub-contractor being malicious. Therefore, while implementing the proposed model, different δ_{initial} values should be considered for different roles. However, δ values of each user in the network should be dynamic throughout the project and change based on feedback from the IDS. In this paper, the probability of an insider being malicious at any given time is annotated as δ_{current} . For example, if a user with a low δ_{initial} value starts having suspicious activity (e.g., unexpected traffic from its devices), its δ_{current} value is revised and relatively increased.

The access control manages the access requests of subjects to different objects in the network. While the subjects refer to project participants with various roles, the object can be a file or device. In this paper, the object is assumed to be a digital file stored in the centralized repository (i.e., CDE). Since the sensitivity of each file in a project is different, all parameters related to data defined in the previous sections should also be different. One of these parameters is the defender's payoff due to the discovery of a malicious insider identity or data protection $\omega \in (0, 1)$. It represents the importance of protecting the data to the project or defender. It can also be considered as the criticality of the data for the proper functioning of the project (i.e., avoiding project disruption and maintaining business continuity). Moreover, $-\omega$ reflects the loss to the defender as a result of not detecting a malicious insider or exposing data to a malicious insider. As the criticality of a file for the project increases, this parameter should also increase (i.e., a high ω means that it is important to the defender). Therefore, it is crucial to understand different file types in a construction project to identify their sensitivity levels for different types of projects during different phases. A high-level and non-exhaustive list of file types used in BIM projects is as follows: BIM execution plan (BEP), 3D models—architectural, 3D models—structural, 3D models—MEP, coordination models, cost estimation documents, construction schedules, cost and schedule forecasts, quantity takeoff files, specifications, clash detection reports, bills of quantities (BoQs), requests for information (RFIs), requests for change (RFCs), quality control/quality assurance documents, bidding documents, payment certificates, progress reports, risk assessment documents, autonomous or semi-autonomous machinery control system files, testing and inspection reports, contracts, and other legal documents.

The parameter ω values for different criticality levels were assigned based on inspiration from the qualitative severity rating scale in the Common Vulnerability Scoring System (CVSS) v3.1 [43]. Since the ω value was normalized within the range of $(0, 1)$ and the original values from CVSS were within the range of $[0, 10]$, the ratings were multiplied by 0.1 to obtain the ω values. A stacked bar chart showing different criticality levels for data and the corresponding ω values are shown in Figure 9.

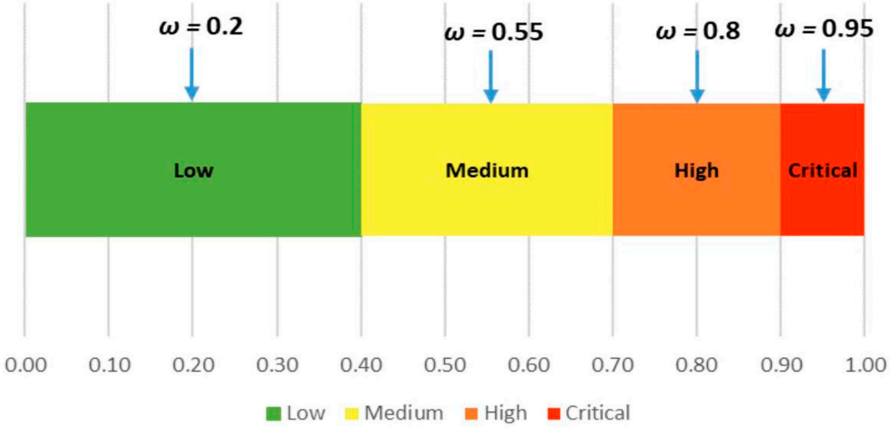


Figure 9. Criticality levels for data and the corresponding ω values.

Different document types might have different sensitivities based on the type and phase of the project. Therefore, assuming fixed values for each one regardless of the characteristics of the project would be inaccurate. For example, while the design documents might have high sensitivity in a critical project such as a military base construction during all the phases, they might have much lower sensitivity in a residential project regardless of the project phase. Mantha et al. [1] summarized some of the critical assets that can be targeted by attackers in construction projects. They mentioned that during the design phase, proprietary information, such as the details of the operational procedures, could be stolen and sold to other parties for financial gain.

The other parameter, the malicious insider's payoff corresponding to the compromising of data (β), presents the importance of the data to the attacker (i.e., the malicious insider). The value of this parameter should be considered independent of the ω value since it is determined based on the attacker's motivation rather than the project's priorities. Similar to ω, β was also normalized between 0 and 1. As its value approached 1, the benefit of compromising data was maximized for the attacker. The same qualitative categorization for the criticality of data and the corresponding values shown in Figure 9 were used for the β value. Therefore, the value of data to the attacker could be low, medium, high, or critical, with β values of 0.2, 0.55, 0.8, and 0.95, respectively. The attackers could have various motivations that determined their targets in the project. In general, cyber attackers can be classified into different categories based on their motivations, such as the ones listed below [44]:

- Pranksters are the attackers who perform attacks without serious intentions, mostly for fun.
- Hacksters are the ones hacking to improve their skills and out of curiosity.
- Malicious hackers are cyber actors who desire destruction and cause damage for self-pleasure.
- Personal problem solvers commit their activities to gain personal benefit. They cannot solve their issues through legal ways and use cyberattacks for that purpose.
- Career criminals have pure financial motivations.
- Extreme advocates perform their activities due to social movements, religious reasons, or political motivations. They have also been called hacktivists.
- Malcontents, addicts, and individuals are attackers mostly with psychological problems, such as antisocial personality disorder.

The last parameter to consider for the implementation of the model was the cost of a cyberattack $\left(C_{cyb}\right)$. This parameter depends on the malicious insider's expertise level and the targeted file's security level. Moreover, the targeted file's security level depends on the project security level and the targeted file's accessibility level. For the malicious insider's expertise level, the Dreyfus model [45] was employed. This model defines five levels of expertise: novice, advanced beginner, competent, proficient, and expert. For the project security level, five qualitative levels (very low, low, medium, high, very high) and corresponding values (0.1, 0.3, 0.5, 0.7, 0.9) were defined. The project security level is characterized by the security measures employed by the project/defender, such as the IDS, a multi-factor authentication system, firewalls, and software patch management. If all the security measures suggested by cybersecurity standards are employed, then the project security level can be considered "very high". Finally, for the targeted file's accessibility level, the same five qualitative levels as the project security level were used. However, the corresponding values for different levels were in the opposite order since increasing accessibility decreases the security level of a file. For example, if a file was very sensitive and accessible to a few people in the project, then the file accessibility level could be considered "very low", with a value of 0.9.

The file security level was calculated by multiplying the project security level and the file accessibility level to incorporate the overall security measures employed in the project and the number of people who can access the file, i.e.,

$$\textit{File security level} = (\textit{Project security level}) * (\textit{File accessibility level}).$$

The qualitative values for each expertise, project security, and accessibility level are shown in Table 3. The cost of cyberattack $\left(C_{cyb}\right)$, normalized within the range of (0,1), was calculated by subtracting the average value of malicious insider expertise level from the average value of file security level, i.e.,

$$\textit{Cost of cyberattack} = max\{\textit{File security level} - \textit{Malicious insider expertise level},\ 0\}.$$

Table 3. Expertise, security, and accessibility levels and the corresponding qualitative values.

Malicious Insider Expertise Level	Project Security Level	File Accessibility Level	Rating Scale		Rating Average
Novice	Very low	Very high	0	0.2	**0.1**
Advanced beginner	Low	High	0.2	0.4	**0.3**
Competent	Medium	Medium	0.4	0.6	**0.5**
Proficient	High	Low	0.6	0.8	**0.7**
Expert	Very high	Very low	0.8	1	**0.9**

If the expertise level value is higher than or equal to the file security level value, the cost of cyberattack $\left(C_{cyb}\right)$ is assumed to be zero. This means that if the attacker has the required expertise level to compromise the targeted data, he/she should not need additional resources. If not, the attacker should use extra resources that will make the cyberattack cost more than zero. The following scenario, where an insider requests access to a file, is presented to understand the mentioned parameters and their roles in determining the best strategies by the insider and defender and show the practical implementation of the proposed model.

4.2.1. Overview of the Hypothetical Scenarios

In these scenarios, a construction cost estimator from the main contractor, who is a malicious insider, requests access to two different files stored in the centralized repository (i.e., CDE) of the project during the construction phase. The project is a smart hospital building construction project, and the cost estimator typically has access to both files. Since the project is a smart building, it will be equipped with IoT devices once the construction is completed. Moreover, medical equipment will be installed at the last stage of the construction phase as it is a hospital building. The details of the IoT devices and medical equipment are stored in the CDE of the project. The two files requested by the cost estimator (i.e., insider) are the cost and schedule forecast file and the structural design file.

To demonstrate the impact of different security levels of projects on the best strategies of the insider and defender, two different scenarios assuming two different overall security levels for the same project are considered. In Scenario 1, the security level of the project was assumed to be "high" (see Table 3). As mentioned in the previous sections, two probability values were used while computing the Bayesian Nash Equilibrium (BNE): the probability that a malicious insider who launches authentication is detected (p_1) and the probability that the malicious insider who launches a cyberattack is detected (p_2). Since the probability that the malicious insider who launches a cyberattack is detected (p_2) is dependent on the overall security level of the project, p_2 was chosen as the corresponding value for "high" in Table 3, which was 0.7. Moreover, since p_1 is assumed to be always higher than p_2 in the proposed game models, p_1 was assumed to be 0.8 for Scenario 1. In Scenario 2, the overall security level of the project was assumed to be "medium" (see Table 3). Therefore, p_2 was assumed to be 0.49 (nearly equal to 0.5) based on the qualitative rating corresponding to "medium" in Table 3. Similar to the first scenario, p_1 was assumed to be slightly higher than p_2, which was 0.55 in this case. A summary of both scenarios for the same smart hospital construction project is presented in Table 4.

Table 4. Characteristics related to the projects for scenarios 1 and 2.

Project Type **Project Phase**	**Smart Hospital Building** **Construction Phase**	
Scenarios	**Characteristic**	**Value**
Scenario 1	The overall security level of the project	High (0.7) (See Table 3)
	The probability that the malicious insider who launches a cyberattack is detected (p_2)	0.7
	The probability that the malicious insider who uses authentication is detected (p_1)	0.8
Scenario 2	The overall security level of the project	Medium (0.5) (See Table 3)
	The probability that the malicious insider who launches a cyberattack is detected (p_2)	0.49
	The probability that the malicious insider who uses authentication is detected (p_1)	0.55

At the beginning of the project, the initial probability of being a malicious insider (δ_{initial}) for the cost estimator was assumed to be 0.2 since it is a trusted role in the project. However, at the time of the data request, the probability of being a malicious insider (δ_{current}) was assumed to be higher, 0.8, due to unusual traffic from the cost estimator's computer detected by the IDS. The unusual traffic shows that high volumes of data were transferred from the project repository to an unknown IP address. In this scenario, the cost estimator who requests access to the files is a malicious insider with financial motivation. He/she is a career criminal, based on Parker's [44] cyber attacker categories previously presented, and is assumed to have an expertise level of advanced beginner, based on the Dreyfus model [45]. These characteristics related to the malicious insider are summarized in Table 5.

Table 5. Characteristics of the malicious insider.

Characteristic	**Value**
Type of malicious insider	Career criminal
The motivation of the malicious insider	Financial gain
Insider's expertise level	Advanced beginner (0.3) (See Figure 3)
The initial probability of being a malicious insider (δ_{initial})	0.2
The probability of being a malicious insider at the time of the access request (δ_{current})	0.8

Table 6 (for Scenario 1) and Table 7 (for Scenario 2) show the two different files requested by the malicious insider, the criticality of each file for the project considering different cybersecurity attributes, the corresponding ω values, the value of each file to the malicious insider, the corresponding β values, the accessibility levels of each file, the project security level, file security levels, malicious insider's expertise level, the cost of cyberattack $\left(C_{cyb}\right)$, and the Bayesian Nash Equilibrium (BNE) that shows the best strategy for the insider and the defender. The criticality levels of each file were determined based on the CIA triad [46] (i.e., confidentiality, integrity, and availability). The details of each file requested by the malicious insider and their importance from the project's and insider's perspectives were as follows:

- The cost and schedule forecast file shows the details of the contractor's cost calculations for various tasks, the internal schedule for the remaining work, the profitability analysis of the contractor, and the risk register of the project. The file is "critical" in terms of confidentiality since it includes the financial details of the project, such as the cost of various tasks, the profitability of the project, and the cost of materials and services. Since this information is only available to a few people in the project, the accessibility level of the file is "very low" (Table 6). The file's integrity has a "medium" criticality since the data alterations might mislead the project management and cause wrong decisions to be made. However, it is not as critical as the confidentiality aspect. Lastly, the availability of the file has low criticality since its unavailability does not disrupt the business functions or site operations. Since the malicious insider has a financial motivation, the file is of "critical" value. He/she can potentially sell the sensitive content of the file to competitors or ask for a ransom in exchange for not leaking the data. Therefore, the insider primarily targets this file.
- The structural design file includes all the details regarding the structural elements, such as the reinforcement details, concrete and other structural material characteristics, and the connection details of each element. Since it is a building information model, all details, including the exact locations of the structural elements, are included in the file. The file has a "medium" criticality in terms of confidentiality since it includes intellectual property. The most critical aspect of the file is its integrity since a stealthy attacker could tamper with the structural design details and mislead the site teams about the execution. This could potentially cause a reduction in the strength of the structural elements, which might cause a catastrophic failure of the building during the operational phase. Considering that the building is a hospital, the criticality of properly implementing the correct structural design further increases. Finally, the availability of the file has "medium" importance since the unavailability might cause disruptions to site activities, which might indirectly lead to financial loss. The accessibility of the file is "medium" as there are a considerable number of project participants, such as the structural design team, quantity surveyor, and cost estimator, who need this information to perform their tasks. From the malicious insider's perspective, the file is not as valuable as the cost and schedule forecast file. However, he/she can attack the file with ransomware and threaten the project by permanently destroying it or leaking its content. Considering that the file has medium-level sensitivity in terms of confidentiality and availability, it is also of medium importance to the malicious insider.

The ω values for each cybersecurity attribute of each file were assigned based on Figure 9 and the average ω was the arithmetic mean of the three different ω values. The cost of cyberattack $\left(C_{cyb}\right)$ was calculated using the method presented previously. For the cost and schedule forecast file in Scenario 1, the file security level was calculated by multiplying the project security level, 0.7, by the file accessibility level, 0.9, which resulted in 0.63. Since the malicious insider had an expertise level of "Advanced beginner", which corresponded to a value of 0.3 (see Table 3), subtracting this from the file security level, 0.63, gave us the value for the cost of the cyberattack $\left(C_{cyb}\right)$, 0.33. This means that the malicious insider will need additional resources to compromise the cost and schedule forecast file in Scenario 1. The values for the structural design file in Scenario 1 are given in Table 6 and the values for both files in Scenario 2 are presented in Table 7. The BNE corresponding to these scenarios were computed based on the flowchart of BNE (see Figure 4) and are also presented in Tables 6 and 7.

Table 6. Parameters and BNE for scenario 1.

File Type	Criticality of the File (for the Project)		Payoff Due to Discovery of Malicious Insider Identity or Data Protection (ω)		Value of the File to the Malicious Insider	Payoff Corresponding to Compromised Data (β)	File Accessibility Level	Project Security Level	File Security Level	Malicious Insider's Expertise Level	Cost of Cyberattack (C_{cyb})	Bayesian Nash Equilibrium (BNE)
	Cybersecurity Attribute	Criticality	ω	Average ω								
Cost and Schedule Forecast File	Confidentiality	Critical	0.95	0.57	Critical	0.95	Very low: 0.9	High: 0.7	(0.9 × 0.7) = 0.63	Advanced beginner: 0.3	(0.63 − 0.3) = 0.33	E
	Integrity	Medium	0.55									
	Availability	Low	0.2									
Structural Design File	Confidentiality	Medium	0.55	0.68	Medium	0.5	Medium: 0.5		(0.5 × 0.7) = 0.35		(0.35 − 0.3) = 0.05	D
	Integrity	Critical	0.95									
	Availability	Medium	0.55									

Table 7. Parameters and BNE for scenario 2.

File Type	Criticality of the File (for the Project)		Payoff Due to discovery of Malicious Insider Identity or Data Protection (ω)		Value of the File to the Malicious Insider	Payoff Corresponding to Compromised Data (β)	File Accessibility Level	Project Security Level	File Security Level	Malicious Insider's Expertise Level	Cost of Cyberattack (C_{cyb})	Bayesian Nash Equilibrium (BNE)
	Cybersecurity Attribute	Criticality	ω	Average ω								
Cost and Schedule Forecast File	Confidentiality	Critical	0.95	0.57	Critical	0.95	Very low: 0.9	Medium: 0.5	(0.9 × 0.5) = 0.45	Advanced beginner: 0.3	(0.45 − 0.3) = 0.15	B
	Integrity	Medium	0.55									
	Availability	Low	0.2									
Structural Design File	Confidentiality	Medium	0.55	0.68	Medium	0.5	Medium: 0.5		(0.5 × 0.5) = 0.25		(0.25 − 0.3) < 0	A
	Integrity	Critical	0.95									
	Availability	Medium	0.55									

4.2.2. Discussion of the BNE for Hypothetical Scenarios

In scenario 1 (Table 6), where the project security level is high, we observe that the BNE with respect to the cost and schedule forecast file is E when the cost of cyberattack C_{cyb} is 0.33. The equilibrium E $= \left(R^{M}_{\text{aut}}\ R^{L}_{\text{aut}}\ , D^{\text{aut}}_{\text{accept}}\ D^{cyb}_{\text{accept}}\right)$ (see Figure 4) states that when the cost of the cyberattack is 0.33, a malicious insider whose level is advanced beginner would prefer using authentication to a cyberattack to request the file, and the legitimate insider would also use authentication. The defender observes this, and, in response to that, decides that the best strategy is to accept the access request with the probability $p_1 = 0.8$ of the malicious insider being detected. On the other hand, for the structural design file, the BNE is D, where D $= \left(R^{M}_{\text{cyb}}\ R^{L}_{\text{aut}}\ , D^{\text{aut}}_{\text{accept}}\ D^{cyb}_{\text{accept}}\right)$. This states that when the cost of the cyberattack C_{cyb} is 0.05, a malicious insider would prefer launching a cyberattack to using authentication to request the file. This action is observed by the defender, and the best defense strategy is to accept the request and catch the malicious insider with the probability $p_2 = 0.7$.

In scenario 2 (Table 7), where the project security is medium, we see that the BNE corresponding to the cost and schedule forecast file is B $= \left(R^{M}_{\text{aut}}\ R^{L}_{\text{aut}}\ , D^{\text{aut}}_{\text{accept}}\ D^{\text{cyb}}_{\text{reject}}\right)$. This states that when the cost of the cyberattack is 0.15 and if the insider is a malicious one whose expertise level is advanced beginner, he/she would prefer using authentication to a cyberattack at this cost to request the file. In this case, the best strategy for the defender is to accept the request with the probability $p_1 = 0.55$ of the malicious insider being discovered. In addition, it can be seen from this equilibrium that if the insider is legitimate, he/she would request the data through authentication, and this request would be accepted by the defender. On the other hand, in the case of the structural design file, the BNE is A $= \left(R^{M}_{cyb} R^{L}_{\text{aut}}\ , D^{\text{aut}}_{\text{accept}}\ D^{cyb}_{\text{reject}}\right)$, with the cost of the cyberattack set to $C_{cyb} = 0$. This shows that if the insider is a malicious advanced beginner, he/she would launch a cyberattack at the cost of zero (i.e., $C_{cyb} = 0$) rather than using authentication. To counter this act, the best strategy for the defender is to reject the request, given that the probability of the malicious insider being detected is $p_2 = 0.49$, whereas if the insider is legitimate, he/she would request the file through authentication, and this request would be accepted by the defender.

4.3. Validation of the Applicability of the Proposed Model Using Real Project Data

4.3.1. Interviews with Construction Experts

A model in research can undergo validation through the utilization of an expert panel. This process entails engaging a group of experts to scrutinize the model's elements and assess its efficacy [47]. The usefulness, verifiability, and structure of the model are assessed by the experts to determine if the model meets its objectives [48]. The validation phase enhances practitioners' comprehension and utilization of the model within the field [48]. The assessment conducted by the experts can pinpoint any required adjustments to enhance the model's performance. In line with this, interviews were conducted with two experts working for a large-scale construction company to receive feedback about the usefulness of this study and show the applicability of the proposed model when real project data are used. Their company has been delivering significant landmark projects in the Middle East region, mainly in the United Arab Emirates (UAE), since it was founded in 1999. The interviewees included an IT expert and a construction innovation expert with more than ten years of experience. The interview had two sessions: (1) the authors presented the proposed game-theoretic model and its implementation for the hypothetical scenario provided in the previous subsections and (2) the experts were asked to give feedback on different elements of the presented model and provide information about two types of files in two of their projects. The experts' responses were collected through a structured, roundtable discussion during the second interview session. The discussion was guided by the prepared questions regarding the experts' opinions on the model and the characteristics of the file types and projects they preferred to share. This information was then used to show the proposed model's implementation using real project data, discussed in the following subsections. The implementation still had a hypothetical component, which was related to the malicious insider, since the interviewees could not provide information regarding this aspect. Therefore, the malicious insider scenario, including the insider's characteristics (see Table 5), job title, and suspicious activities, was kept the same. On the other hand, the characteristics of the files requested by the malicious insider and the construction projects were changed based on the experts' input. The experts shared the required level of information regarding their projects without disclosing the project names for confidentiality purposes.

4.3.2. Evaluation of the Proposed Models

The experts were asked to evaluate the proposed models during the second interview session. Two questions were directed to the interviewees to receive their feedback, and their answers were requested using the Likert scale (1–5), along with any comments they had. The questions and provided answers were as follows:

Question 1) Do you think the parameters below (see Table 8) were included in the model in a reasonable way? Please rank from 1 to 5 (5 being the most reasonable).

Table 8. Parameters used in the proposed model and the experts' feedback.

No.	Parameters	Experts' Rankings (1–5)
1.	δ (The initial probability of being a malicious insider)	5
2.	p_1 and p_2 (The probability that the malicious insider is detected)	4
3.	ω (Payoff/reward to the data defender due to detection of the malicious insider)	5
4.	β (Payoff/reward to malicious insider due to stolen data/compromised data)	5
5.	C_{cyb} (Cost of cyberattack)	5

Answer 1)

As the rankings in Table 8 indicate, the experts found the parameters used in the model reasonable. They only had a comment about the assumption of p_1 being always higher than p_2. They mentioned that this assumption is reasonable when the detection and identification of a malicious insider is considered. However, they suggested that this study could also consider the probability of detecting malicious activity. They indicated that the probability of detecting malicious activity when the insider is using a cyberattack would be higher than the probability of detecting malicious activity when the insider is using authentication.

Question 2) The file security level and cost of cyberattack (C_{cyb}) are estimated as follows:

File security level = (Project security level) x (File accessibility level)

$$C_{cyb} = \max\{\textit{File security level} - \textit{malicious insider expertise level},\ 0\}$$

Are the formulae used to estimate the file security level and $\mathrm{C}_{\mathrm{cyb}}$ reasonable?

Answer 2) After a round of discussion, the experts agreed that the provided formulae used in the model are reasonable. They could understand the logic behind the formulae and did not have further suggestions to improve them.

4.3.3. Overview of the File Types

The experts were asked to provide two types of files commonly used in their projects that could be valuable to attackers. The experts agreed on discussing the following file types:

File type 1—Structural design file: Similar to the hypothetical example in this study, the experts suggested that the structural design files would be valuable to potential attackers. They mentioned that their company utilizes BIM; therefore, the structural design files are developed and stored in digital environments. Structural design files include all relevant details, such as material lists, structural element details, load analysis, connection details, and specifications.

File type 2—Resource management file (for labor): This type of file includes all details about the labor used in a project, such as the detailed list of labor, distribution of worker types required for different tasks, total manhours required for each task, and unit labor cost for different worker types. The experts mentioned that these files are also created in digital environments and stored in the CDE of the project.

4.3.4. Overview of Projects

The interviewed experts were asked to provide the details of two projects of their company with different characteristics. The projects chosen by the experts were as follows:

Project 1—High-rise building: This project was delivered by the experts' company in Dubai, UAE. The project included constructing a complex high-rise commercial building equipped with IoT devices. It was a design–bid–build (DBB) project. Therefore, the construction company was not responsible for the design development. Their scope only included the construction phase. The project utilized BIM technologies, and project stakeholders collaborated via a CDE.

Project 2—Theme park: The second project provided by the interviewees was a horizontal construction project for a theme park in Abu Dhabi. The project utilized advanced construction technologies, such as virtual reality for collaborating over building information models, augmented reality onsite for visualizing building elements using tablet PCs, and robots to collect data for assessing site conditions. The theme park included various state-of-the-art IoT devices for automation during the operation and maintenance phase.

Moreover, the experts mentioned that this project's client had strict measures regarding the confidentiality of project information.

The summary of the project-related information, including the security level of the projects, is presented in Table 9. The project phase for both examples is construction since the company was only responsible for construction works in both cases. Moreover, the experts indicated the project security level as "medium" and mentioned that they had similar cybersecurity measures in both projects.

Table 9. Characteristics of projects 1 and 2.

Project Phase	**Construction Phase**	
Scenarios	**Characteristic**	**Value**
Project 1 (High-rise building)	The overall security level of the project	Medium (0.5) (See Table 3)
	The probability that the malicious insider who launches a cyberattack is detected (p_2)	0.49
	The probability that the malicious insider who uses authentication is detected (p_1)	0.55
Project 2 (Theme park)	The overall security level of the project	Medium (0.5) (See Table 3)
	The probability that the malicious insider who launches a cyberattack is detected (p_2)	0.49
	The probability that the malicious insider who uses authentication is detected (p_1)	0.55

4.3.5. Implementation of the Model

The experts were asked to provide the relevant characteristics of both file types in two different projects for the implementation of the game-theoretic model. When the file accessibility levels were assessed, the experts mentioned that structural design files were much less accessible in both projects than resource management files. Moreover, they indicated that the second project's client had a higher priority for confidentiality. Therefore, the accessibility of both files was lower in project 1 compared to project 2. For resource management files, the experts indicated that even though they were accessible to most project employees, the files' cost-related columns were only accessible to a small group. For this reason, they did not assign "very high" accessibility for this file type, even for project 1. All file accessibility levels are summarized in Table 10.

Table 10. File accessibility levels for projects 1 and 2.

File Type	**File Accessibility Level (Project 1)**	**File Accessibility Level (Project 2)**
Structural design file	Low	Very low
Resource management file	High	Medium

The experts were asked to provide their opinion about the value of the provided file types to a potential malicious insider with a financial motivation—the same malicious insider as the hypothetical scenario. They argued that the structural design files would be "critical" to potential malicious insiders since they are considered intellectual property with high financial value. They mentioned that the resource management file would have a "medium" value in project 1 and a "high" value in project 2 since they included cost information. Since this file type included labor cost and project 2 had higher commercial value, its value to a potential malicious insider in project 2 was considered higher by the experts. These values are shown in Table 11.

Table 11. Value of the files to potential malicious insiders in projects 1 and 2.

File Type	Value of the File to a Potential Malicious Insider (Project 1)	Value of the File to a Potential Malicious Insider (Project 2)
Structural design file	Critical	Critical
Resource management file	Medium	High

Finally, the experts were asked about the criticality of the given file types in both projects considering different cybersecurity attributes (i.e., confidentiality, integrity, availability). They mentioned that in both projects, the confidentiality and integrity of the structural design files were "critical". They emphasized the financial value of the structural design files, which increased the importance of confidentiality. From the integrity perspective, they agreed that a potential unauthorized change in structural design files could lead to a catastrophic outcome if not discovered quickly. They considered the availability of the design files to have a "medium" level of importance in both projects since their unavailability would cause a minor delay in the project and require additional resources to recover. However, they did not think that it would have a significant impact on both projects.

For resource management files, the experts considered confidentiality important for project 2 (theme park) due to the client's effort to keep the internal project information confidential. Therefore, they assigned a level of "high" for this file type's criticality for project 2. Other than this aspect, they did not consider any other cybersecurity attribute of the resource management file type to be of more than "low" criticality for both projects. Therefore, all the remaining values were assigned "low". All cybersecurity attribute values and the other aspects of each file type discussed are summarized in Tables 12 and 13. Based on these values collected from the experts, the file security levels, cost of cyberattack (C_{cyb}) values considering the hypothetical malicious insider, and the BNEs are also presented in these tables.

Table 12. Parameters and BNE for project 1.

File Type	Criticality of the File (for the Project)		Payoff Due to Discovery of Malicious Insider Identity or Data Protection (ω)		Value of the File to the Malicious Insider	Payoff Corresponding to Compromised Data (β)	File Accessibility Level	Project Security Level	File Security Level	Malicious Insider's Expertise Level	Cost of Cyberattack (C_{cyb})	Bayesian Nash Equilibrium (BNE)
	Cybersecurity Attribute	Criticality	ω	Average ω								
Structural Design File	Confidentiality	Critical	0.95	0.82	Critical	0.95	Low: 0.7	Medium: 0.5	$(0.5 \times 0.7) = 0.35$	Advanced beginner: 0.3	$\text{Max}\{0.35 - 0.3, 0\} = 0.05$	A
	Integrity	Critical	0.95									
	Availability	Medium	0.55									
Resource Management File	Confidentiality	Low	0.2	0.2	Medium	0.5	High: 0.3		$(0.5 \times 0.3) = 0.15$		$\text{Max}\{0.15 - 0.3, 0\} = 0$	A
	Integrity	Low	0.2									
	Availability	Low	0.2									

Table 13. Parameters and BNE for project 2.

File Type	Criticality of the File (for the Project)		Payoff Due to Discovery of Malicious Insider Identity or Data Protection (ω)		Value of the File to the Malicious Insider	Payoff Corresponding to Compromised Data (β)	File Accessibility Level	Project Security Level	File Security Level	Malicious Insider's Expertise Level	Cost of Cyberattack (C_{cyb})	Bayesian Nash Equilibrium (BNE)
	Cybersecurity Attribute	Criticality	ω	Average ω								
Structural Design File	Confidentiality	Critical	0.95	0.82	Critical	0.95	Very low: 0.9	Medium: 0.5	$(0.5 \times 0.9) = 0.45$	Advanced beginner: 0.3	$\text{Max}\{0.45 - 0.3, 0\} = 0.15$	B
	Integrity	Critical	0.95									
	Availability	Medium	0.55									
Resource Management File	Confidentiality	High	0.8	0.4	High	0.8	Medium: 0.5		$(0.5 \times 0.5) = 0.25$		$\text{Max}\{0.15 - 0.3, 0\} = 0$	A
	Integrity	Low	0.2									
	Availability	Low	0.2									

4.3.6. Discussion of the BNE for Real Project Data

Table 12 presents the BNE corresponding to project 2 (high-rise building) with the project security level of medium. It can be observed from Table 12 that for both the files—the structural design file and the resource management file—the BNE was A $= \left(R^{M}_{cyb} R^{L}_{\text{aut}}, D^{\text{aut}}_{\text{accept}}\ D^{cyb}_{\text{reject}}\right)$, with the cost of cyberattack $C_{cyb} = 0.05$ and 0, respectively. The equilibrium implied that if the insider was malicious, he/she would launch a cyberattack to access the file at a very low cost or no cost at all. The defender would observe this action and respond to it by rejecting the access request. In this situation, the probability of the malicious insider's identity being detected (p_2) would be approximately 0.5, characterized by the project security level of medium. Therefore, the best strategy for the defender would be to reject the file access request. Additionally, the equilibrium stated that if the insider was legitimate, then he/she would launch authentication to obtain access to the file, and the best strategy for the defender would be to accept the access request.

Furthermore, Table 13 presents the BNE calculation for project 2 (theme park). The BNE for the structural design file was B $= \left(R^{M}_{\text{aut}}\ R^{L}_{\text{aut}}, D^{\text{aut}}_{\text{accept}}\ D^{\text{cyb}}_{\text{reject}}\right)$, whereas the BNE for the resource management file was A $= \left(R^{M}_{cyb} R^{L}_{\text{aut}}, D^{\text{aut}}_{\text{accept}}\ D^{cyb}_{\text{reject}}\right)$ (see Table 13). In the case of the structural design file, the cost of cyberattack was 0.15, while, for the resource management file, it was 0. As the cost of cyberattack was relatively high, the malicious insider would prefer authentication over launching a cyberattack for the structural design file. However, for the resource management file, with zero cost, he/she would opt for a cyberattack. After observing the cyberattack, the defender would respond by rejecting the file access request. This decision would be driven by the defender's unwillingness to risk data security due to the low probability of detecting the malicious insider's identity (approximately 0.5 for a medium project security level). Furthermore, the equilibrium for both files dictated that if the insider was legitimate, he/she would perform authentication to request file access. In response, the defender would accept this request and release the file.

5. Discussion and Limitations

The previous section presented the implementation of the proposed game-theoretical models using two scenarios for constructing a smart hospital building. The scenarios differed from each other based on the assumed project security level. In both scenarios, two types of files were considered for the implementation: cost and schedule forecast and structural design files. While the confidentiality of the first file type was assumed to be "high", it was considered "medium" for the second file type due to the nature of the project. If the scenario included a project with high design sensitivity, the second file type's confidentiality would also be "high". For example, if the project were a military base, embassy, or intelligence agency building, the confidentiality of all design files, including the structural ones, would be "critical". Moreover, if the malicious insider's motivation was espionage, the value of the design files of such projects to the malicious insider (see Tables 6 and 7, column "value of the file to malicious insider") would be "critical". If the project type was a residential building, the confidentiality of the design files could be considered even lower than the hospital construction scenario since the design would not have the same criticality level. Therefore, different file types would have different "cybersecurity attribute" (see Tables 6 and 7) values for different project types based on the characteristics of the projects.

While this study presented the implementation of the proposed models in a theoretical scenario, the real-life application might have several constraints and difficulties. The first difficulty in a real-life scenario would be assigning confidentiality, integrity, and availability values for all types of files in the project. Since they have qualitative values, they might change based on the person assigning them. The problem regarding the subjectivity of the values also applies to the other qualitative values in Tables 6 and 7, such as "value of the file to malicious insider" and "malicious insider's expertise level". Another challenge would be identifying the security level of the project. This would require the project to perform security risk assessments regularly. However, even with regular risk assessments, choosing one of the five values for the security level in Table 3 reduces accuracy. The constraints of simplification and reduced accuracy in values also apply to the "malicious insider expertise level" and "file accessibility level". Identifying these values and making them realistic is one of the considerable real-life challenges of this study.

This study also simplified the motivation of the malicious insider. The insider might have several motivations, some not given in this study. Therefore, assigning values for the "Value of the File to Malicious Insider" would be more difficult and complex. Moreover, in this study, the expertise level of the attacker did not affect the values of "the probability of being a malicious insider at the time of the access request $(\delta_{\text{current}})$", "the probability that the malicious insider who launches authentication is detected (p_1)", and "the probability that the malicious insider who launches a cyberattack is detected (p_2)". However, if the attacker is stealthy enough, the IDS might not be able to detect unusual traffic from the insider. Thus, the δ_{current} value would stay low, affecting the best strategy for the defender. Similarly, the stealthiness would significantly affect the probability of being detected, corresponding to the p_1 and p_2 values in this study. The evaluation of the proposed model was made by only two experts from a construction company, which can be considered another limitation of this study. Receiving the feedback of more experts would help improve the study further. Finally, as insider threats are not only concerned with intentional malicious acts but also inadvertent acts, our proposed game models could not capture the scenario of unintentional/inadvertent insider threats, which could be considered a future research direction.

6. Conclusions and Future Work

CDEs have emerged as critical platforms for enhancing collaboration and data management in the AEC industry, particularly with the increasing adoption of BIM. While CDEs have the potential to secure sensitive project information, insider threats—where authorized users misuse their access privileges—remain a significant concern. These threats, which may involve data theft, modification, or leakage, can result in substantial financial losses, intellectual property theft, and strategic disadvantages for construction companies. In this study, we developed game-theoretic models based on Bayesian games, that is a game of incomplete information, to better understand and predict malicious insider behavior within CDEs. These models account for both static and dynamic interactions between insiders, who may act as either malicious or legitimate, and the data defender. Through the application of these models to two real project scenarios (a high-rise building and a theme park), we demonstrated how different project types and sensitivity levels of information (e.g., structural design files and resource management files) affected the interaction between the insiders and the defender. Our models provided insights into how malicious insiders, driven by various motivations such as financial gain or espionage, might behave in these settings and highlighted the corresponding strategies the defender can adopt to mitigate these threats. The findings of this research offer valuable practical guidance for improving CDE security, especially in high-risk construction projects involving sensitive data. By considering various insider threat scenarios, we provide actionable recommendations for enhancing existing cybersecurity protocols in the AEC industry, particularly in response to insider threats, which are often more difficult to detect than external attacks. As the industry continues to digitize, these insights are crucial for securing sensitive construction data and ensuring the success of collaborative, data-driven projects. The proposed models offer a strategic approach for both mitigating insider threats and supporting the ongoing efforts to bolster cybersecurity in the construction sector.

The growing adoption of large language models (LLMs) in cybersecurity is transforming the field by leveraging their abilities, such as in-context learning, instruction following, and step-by-step reasoning, to address complex challenges [49]. These capabilities enable LLMs to solve downstream tasks, such as cryptographic operations and data protection, without extensive retraining, presenting a novel approach to enhancing cybersecurity systems. Moreover, advancements in prompt engineering have further optimized LLM performance, making them effective tools for mitigating evolving cyber threats [49]. Integrating LLMs with game-theoretic models could unlock new opportunities for designing robust, adaptive cybersecurity solutions that address both external and insider threats within the AEC industry. Therefore, the use of LLMs and generative AI will be investigated in future work.

Author Contributions: Conceptualization, K.L., S.G., B.G.d.S., D.Y. and M.S.S.; methodology, K.L., S.G., B.G.d.S., D.Y. and M.S.S.; software, K.L., D.Y. and M.S.S.; validation, K.L., S.G., B.G.d.S., D.Y. and M.S.S.; formal analysis, K.L., S.G., B.G.d.S., D.Y. and M.S.S.; investigation, K.L., S.G., B.G.d.S., D.Y. and M.S.S.; resources, K.L., S.G., B.G.d.S., D.Y. and M.S.S.; data curation, K.L., B.G.d.S., D.Y. and M.S.S.; writing—original draft preparation, K.L., S.G., B.G.d.S., D.Y. and M.S.S.; writing—review and editing, K.L., S.G., B.G.d.S., D.Y., and M.S.S.; visualization, K.L., S.G., B.G.d.S., D.Y. and M.S.S.; supervision, S.G. and B.G.d.S.; project administration, S.G. and B.G.d.S.; funding acquisition, S.G. and B.G.d.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Center for Cyber Security (CCS) at New York University Abu Dhabi, funded by Tamkeen under the NYUAD Research Institute Award G1104 and in collaboration with the NYUAD Center for Interacting Urban Networks (CITIES), funded by Tamkeen under the NYUAD Research Institute Award CG001.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Acknowledgments: The authors thank ALEC Engineering and Contracting for their valuable input for this study. In particular, we want to thank Sabyasachi Jana and Ali Raza for their time and valuable information provided for the Implementation section of this paper.

Conflicts of Interest: The authors declare that they have no conflicts of interests.

Appendix A

Proof of Proposition 1. (i) If $C_{cyb} < \beta p_1$, then we have $U_1\left(R_{aut}^M R_{aut}^L, D_{\text{accept}}\right) < U_1\left(R_{\text{cyb}}^M\ R_{\text{aut}}^L, D_{\text{accept}}\right)$ and $U_1\left(R_{\text{aut}}^M\ R_{\text{aut}}^L, D_{\text{reject}}\right) > U_1\left(R_{\text{cyb}}^M\ R_{\text{aut}}^L, D_{\text{reject}}\right)$. Additionally, if $\delta > \frac{1}{1+\omega(1-p_1)}$, then $U_2\left(R_{\text{aut}}^M\ R_{\text{aut}}^L, D_{\text{accept}}\right) < U_1\left(R_{\text{aut}}^M\ R_{\text{aut}}^L, D_{\text{reject}}\right)$. Let $x_1 = \frac{1}{1+\omega(1-p_1)}$. Thus, if $\delta > x_1$, then $\left(R_{\text{aut}}^M\ R_{\text{aut}}^L, D_{\text{reject}}\right)$ is a pure-strategy BNE. Also, if $\delta > \frac{1}{1+\omega}$, then $U_2\left(R_{\text{cyb}}^M\ R_{\text{aut}}^L, D_{\text{accept}}\right) < U_2\left(R_{\text{cyb}}^M\ R_{\text{aut}}^L, D_{\text{reject}}\right)$. Let $y_1 = \frac{1}{1+\omega}$. If $\delta > x_1$ and $\delta > y_1$, then $\left(R_{\text{aut}}^M\ R_{\text{aut}}^L, D_{\text{reject}}\right)$ is the unique pure-strategy BNE since $y_1 < x_1$. This implies that if $\delta > x_1$, then $\left(R_{\text{aut}}^M\ R_{\text{aut}}^L, D_{\text{reject}}\right)$ is the unique pure-strategy BNE. Furthermore, if $\delta < y_1$, then $\left(R_{cyb}^M R_{\text{aut}}^L, D_{\text{accept}}\right)$ is a pure-strategy BNE. In addition, if $\delta < y_1$ and $\delta < x_1$, then $\left(R_{cyb}^M R_{\text{aut}}^L, D_{\text{accept}}\right)$ is the unique pure-strategy BNE. Since $y_1 < x_1$, $\left(R_{\text{cyb}}^M\ R_{\text{aut}}^L, D_{\text{accept}}\right)$ is the unique pure-strategy BNE if $\delta < y_1$. If $\delta < x_1$ and $\delta > y_1$, then there exists a mixed-strategy BNE. Let λ denote the probability that an insider chooses the strategy $R_{\text{aut}}^M\ R_{\text{aut}}^L$ and η denote the probability that the defender chooses D_{accept}. Thus, for the expected values with respect to the pure strategies, we must have $\mathbb{E}\left(R_{\text{aut}}^M\ R_{\text{aut}}^L\right) = \mathbb{E}\left(R_{\text{cyb}}^M\ R_{\text{aut}}^L\right)$. Simplifying this, we obtain

$$\eta^* = \frac{C_{cyb}}{p_1 \beta} \tag{A1}$$

Also, we must have $\mathbb{E}(D_{\text{accept}}) = \mathbb{E}(D_{\text{reject}})$. On simplifying this, we obtain

$$\lambda^* = \frac{(1+\omega) - \frac{1}{\delta}}{p_1\omega} \tag{A2}$$

Summarizing the results above, we obtain Equation (1).

(ii) If $C_{cyb} > \beta p_1$, then we have $U_1(R^M_{\text{aut}}\, R^L_{\text{aut}}, D_{\text{accept}}) > U_1\left(R^M_{cyb} R^L_{\text{aut}}, D_{\text{accept}}\right)$ and $U_1(R^M_{\text{aut}}\, R^L_{\text{aut}}, D_{\text{reject}}) > U_1\left(R^M_{\text{cyb}}\, R^L_{\text{aut}}, D_{\text{reject}}\right)$. This shows that the strategy $R^M_{\text{cyb}}\, R^L_{\text{aut}}$ is dominated by the strategy $R^M_{\text{aut}}\, R^L_{\text{aut}}$. Thus, if $\delta > x_1$, $(R^M_{\text{aut}}\, R^L_{\text{aut}}, D_{\text{reject}})$ is the unique pure-strategy BNE, whereas, if $\delta < x_1$, then $(R^M_{\text{aut}}\, R^L_{\text{aut}}, D_{\text{accept}})$ is the unique pure-strategy BNE. Summarizing the results above, we obtain Equation (2). □

Appendix B

Proof of Proposition 2. (i) Consider the insider strategies $R^M_{\text{aut}}\, R^L_{\text{aut}}$ and $R^M_{cyb} R^L_{\text{aut}}$ to respond to the defender strategy D_{accept}.

Let us compare $U_1(R^M_{\text{aut}}\, R^L_{\text{aut}}, D_{\text{accept}})$ with $U_1\left(R^M_{\text{cyb}}\, R^L_{\text{aut}}, D_{\text{accept}}\right)$. If $C_{cyb} < 2(p_1 - p_2)\beta$, it can be seen for $\delta > 0$ that

$$U_1\left(R^M_{\text{aut}}\, R^L_{\text{aut}}, D_{\text{accept}}\right) < U_1\left(R^M_{\text{cyb}}\, R^L_{\text{aut}}, D_{\text{accept}}\right) \tag{A3}$$

Also, consider the insider strategies $R^M_{aut} R^L_{aut}$ and $R^M_{cyb} R^L_{aut}$ to respond to the defender strategy D_{reject}. Now, compare $U_1(R^M_{\text{aut}}\, R^L_{\text{aut}}, D_{\text{reject}})$ with $U_1\left(R^M_{cyb} R^L_{\text{aut}}, D_{\text{reject}}\right)$. For $\delta > 0$, it can be observed that

$$U_1\left(R^M_{\text{aut}}\, R^L_{\text{aut}}, D_{\text{reject}}\right) > U_1\left(R^M_{\text{cyb}}\, R^L_{\text{aut}}, D_{\text{reject}}\right) \tag{A4}$$

Again, consider the defender's strategies D_{accept} and D_{reject} to respond to the insider's strategy $R^M_{\text{aut}}\, R^L_{\text{aut}}$. It can be deduced that if $\delta \in \Delta_1$, where

$$\Delta_1 = \left\{\delta \in [0,1] \middle| \delta > \frac{1}{1+\omega(1-2p_1)}\right\} \tag{A5}$$

then

$$U_2\left(R^M_{\text{aut}}\, R^L_{\text{aut}}, D_{\text{accept}}\right) < U_2\left(R^M_{\text{aut}}\, R^L_{\text{aut}}, D_{\text{reject}}\right) \tag{A6}$$

Furthermore, consider the defender's strategies D_{accept} and D_{reject} to respond to the insider's strategy $R^M_{cyb} R^L_{\text{aut}}$. We have the following: If $\delta \in \Delta_2$, where

$$\Delta_2 = \left\{\delta \in [0,1] \middle| \delta > \frac{1}{1+\omega(1-2p_2)}\right\} \tag{A7}$$

then

$$U_2\left(R^M_{\text{cyb}}\, R^L_{\text{aut}}, D_{\text{accept}}\right) < U_2\left(R^M_{\text{cyb}}\, R^L_{\text{aut}}, D_{\text{reject}}\right). \tag{A8}$$

Since $p_1 > p_2$, from Equations (A5) and (A7), it can be noticed that $\Delta_1 \subset \Delta_2$ and, therefore, Equation (A8) will also hold for $\delta \in \Delta_1$, i.e., $\delta > \frac{1}{1+\omega(1-2p_1)}$. This shows that the profile of strategy $(R^M_{\text{aut}}\, R^L_{\text{aut}}, D_{\text{reject}})$ is the unique pure-strategy Nash Equilibrium (NE) if $\delta > \frac{1}{1+\omega(1-2p_1)}$.

Let $\Delta_3 = \Delta_1^C \setminus \left\{\delta \in [0,1] \middle| \delta = \frac{1}{1+\omega(1-2p_1)}\right\}$ and $\Delta_4 = \Delta_2^C \setminus \left\{\delta \in [0,1] \middle| \delta = \frac{1}{1+\omega(1-2p_2)}\right\}$. Thus, $\Delta_4 \subset \Delta_3$.

Denote $x^* = \frac{1}{1+\omega(1-2p_1)}$ and $y^* = \frac{1}{1+\omega(1-2p_2)}$. Since $p_1 > p_2$, it is clear that $x^* > y^*$. From Equations (A5) and (A6), if $\delta < x^*$, i.e., $\delta \in \Delta_3$, then

$$U_2\left(R_{\text{aut}}^M\, R_{\text{aut}}^L\,, D_{\text{accept}}\right) > U_2\left(R_{\text{aut}}^M\, R_{\text{aut}}^L\,, D_{\text{reject}}\right) \tag{A9}$$

In addition, if $\delta < y^*$, i.e., $\delta \in \Delta_4$, then

$$U_2\left(R_{\text{cyb}}^M\, R_{\text{aut}}^L\,, D_{\text{accept}}\right) > U_2\left(R_{\text{cyb}}^M\, R_{\text{aut}}^L\,, D_{\text{reject}}\right). \tag{A10}$$

As $\Delta_4 \subset \Delta_3$, Equation (A9) also holds for $\delta \in \Delta_4$. Therefore, if $\delta < y^*$, then the profile of strategy $\left(R_{cyb}^M R_{\text{aut}}^L\,, D_{\text{accept}}\right)$ is the unique pure-strategy BNE of the game.

Again, consider Equations (A8) and (A9). We know that if $\delta \in \Delta_2$ and $\delta \in \Delta_3$, i.e., $y^* < \delta < x^*$, then Equations (A8) and (A9) hold. This implies that there exists a mixed-strategy BNE for the game, which is computed as below:

Suppose that the insider randomizes his/her strategies $R_{aut}^M R_{aut}^L$ and $R_{cyb}^M R_{aut}^L$ with the corresponding probabilities λ_1 and $1 - \lambda_1$, respectively. Also, the defender randomizes his/her strategies D_{accept} and D_{reject} with the corresponding probabilities η_1 and $1 - \eta_1$, respectively.

Thus, the expected payoffs of the insider corresponding to his/her strategies are given by

$$\mathbb{E}_1\left(R_{\text{aut}}^M\, R_{\text{aut}}^L\right) = \eta_1 U_1\left(R_{\text{aut}}^M\, R_{\text{aut}}^L\,, D_{\text{accept}}\right) + (1-\eta_1)U_1\left(R_{\text{aut}}^M\, R_{\text{aut}}^L\,, D_{\text{reject}}\right) \tag{A11}$$

$$\mathbb{E}_1\left(R_{\text{cyb}}^M\, R_{\text{aut}}^L\right) = \eta_1 U_1\left(R_{\text{cyb}}^M\, R_{\text{aut}}^L\,, D_{\text{accept}}\right) + (1-\eta_1)U_1\left(R_{\text{cyb}}^M\, R_{\text{aut}}^L\,, D_{\text{reject}}\right) \tag{A12}$$

The insider must be indifferent to choosing between the strategies $R_{aut}^M R_{aut}^L$ and $R_{cyb}^M R_{\text{aut}}^L$ from the expected payoff given by Equations (A11) and (A12). Hence, we must have $\mathbb{E}_1\left(R_{\text{aut}}^M\, R_{\text{aut}}^L\right) = \mathbb{E}_1\left(R_{\text{cyb}}^M\, R_{\text{aut}}^L\right)$. On simplifying this equation, we obtain

$$\eta_1^* = \frac{C_{cyb}}{2\beta(p_1 - p_2)} \tag{A13}$$

Additionally, the expected payoffs of the defender corresponding to his/her strategies are given by

$$\mathbb{E}_2\left(D_{\text{accept}}\right) = \lambda_1 U_2\left(R_{\text{aut}}^M\, R_{\text{aut}}^L\,, D_{\text{accept}}\right) + (1-\lambda_1)U_2\left(R_{\text{cyb}}^M\, R_{\text{aut}}^L\,, D_{\text{accept}}\right) \tag{A14}$$

$$\mathbb{E}_2\left(D_{\text{reject}}\right) = \lambda_1 U_2\left(R_{\text{aut}}^M\, R_{\text{aut}}^L\,, D_{\text{reject}}\right) + (1-\lambda_1)U_2\left(R_{\text{cyb}}^M\, R_{\text{aut}}^L\,, D_{\text{reject}}\right) \tag{A15}$$

The defender would be indifferent to choosing between his/her strategies D_{accept} and D_{reject} and, therefore, we must have $\mathbb{E}_2\left(D_{\text{accept}}\right) = \mathbb{E}_2\left(D_{\text{reject}}\right)$. On simplifying this equation based on Equations (A14) and (A15), we obtain

$$\lambda_1^* = \frac{1 + \omega(1-2p_2) - \frac{1}{\delta}}{2\omega(p_1 - p_2)} \tag{A16}$$

Summarizing the above results, we obtain the solution of the game as given in Equation (3).

(ii) If $C_{cyb} > 2\beta(p_1 - p_2)$, it can be observed that

$$U_1\left(R_{\text{aut}}^M\, R_{\text{aut}}^L\,, D_{\text{accept}}\right) > U_1\left(R_{cyb}^M R_{\text{aut}}^L\,, D_{\text{accept}}\right) \tag{A17}$$

Furthermore, if $\delta \in \Delta_1$ then the defender's strategy D_{reject} is the best response to the insider's strategy $R^M_{\text{aut}}\ R^L_{\text{aut}}$. Thus, from Equations (A4) and (A17), it follows that the profile of strategy $\left(R^M_{\text{aut}}\ R^L_{\text{aut}}, D_{\text{reject}}\right)$ is the unique pure-strategy BNE of the game.

On the other hand, if $\delta \in \Delta_3$, then it can be noticed that D_{accept} is the defender's best response to the insider's strategy $R^M_{\text{aut}}\ R^L_{\text{aut}}$. Hence, the profile of strategy $\left(R^M_{\text{aut}}\ R^L_{\text{aut}}, D_{\text{accept}}\right)$ is the unique pure-strategy BNE of the game.

Also, it can be noticed that under the condition $C_{cyb} > 2\beta(p_1 - p_2)$, there is no mixed-strategy BNE. The above results can be summarized as presented in Equation (4). □

Appendix C

Proof of Proposition 3. (i) $\delta < x^*$, i.e., $\delta \in \Delta_3$ and $p_2 < \frac{1}{2}$.

If $p_2 < \frac{1}{2}$, it can be deduced that $y_{21} < y_{22}$. Since $y_{11} \le y_{12}$ and $y_{21} < y_{22}$, the strategy $D^{\text{aut}}_{\text{accept}}\ D^{cyb}_{\text{accept}}$ is dominated by the strategy $D^{aut}_{\text{accept}}\ D^{cyb}_{\text{reject}}$. To find the corresponding BNEs, let us consider the following payoff matrix:

$$\begin{array}{c} R^M_{\text{aut}}\ R^L_{\text{aut}} \\ R^M_{\text{cyb}}\ R^L_{\text{aut}} \\ \\ \end{array} \begin{bmatrix} D^{\text{aut}}_{\text{accept}}\ D^{\text{cyb}}_{\text{reject}} & D^{\text{aut}}_{\text{reject}}\ D^{cyb}_{\text{accept}} & D^{\text{aut}}_{\text{reject}}\ D^{cyb}_{\text{reject}} \\ (x_{12}, y_{12}) & (x_{13}, y_{13}) & (x_{14}, y_{14}) \\ (x_{22}, y_{22}) & (x_{23}, y_{23}) & (x_{24}, y_{24}) \end{bmatrix}$$

We can show that $y_{13} = y_{14} = 0$. Moreover, if $p_2 < \frac{1}{2}$, then $y_{23} < y_{24}$. Hence, the strategy $D^{\text{aut}}_{\text{reject}} D^{cyb}_{\text{accept}}$ is dominated by the strategy $D^{aut}_{\text{reject}} D^{cyb}_{\text{reject}}$. In addition, $x_{14} = 0, y_{14} = 0$ and $y_{24} = 0$. Thus, we have the following matrix:

$$\begin{array}{c} R^M_{\text{aut}} R^L_{\text{aut}} \\ R^M_{\text{cyb}} R^L_{\text{aut}} \\ \\ \end{array} \begin{bmatrix} D^{\text{aut}}_{\text{accept}} D^{\text{cyb}}_{\text{reject}} & D^{\text{aut}}_{\text{reject}}\ D^{cyb}_{\text{reject}} \\ (x_{12}, y_{12}) & (0, 0) \\ (x_{22}, y_{22}) & (x_{24},\ 0) \end{bmatrix}$$

It can be shown that $y_{22} > 0$. Additionally, if $\delta < x^*$, then $y_{12} > 0$; therefore, we have the reduced matrix as follows:

$$\begin{array}{c} R^M_{\text{aut}}\ R^L_{\text{aut}} \\ R^M_{\text{cyb}}\ R^L_{\text{aut}} \\ \\ \end{array} \begin{bmatrix} D^{\text{aut}}_{\text{accept}}\ D^{\text{cyb}}_{\text{reject}} \\ (x_{12}, y_{12}) \\ (x_{22}, y_{22}) \end{bmatrix}$$

Now, $x_{12} > x_{22}$ if $C_{cyb} > \beta(2p_1 - 1)$. This implies that $\left(R^M_{\text{aut}}\ R^L_{\text{aut}}, D^{\text{aut}}_{\text{accept}}\ D^{\text{cyb}}_{\text{reject}}\right)$ is a pure-strategy BNE, whereas, if $x_{12} < x_{22}$, i.e., $C_{cyb} < \beta(2p_1 - 1)$, then $\left(R^M_{\text{aut}}\ R^L_{\text{aut}}, D^{\text{aut}}_{\text{accept}}\ D^{\text{cyb}}_{\text{reject}}\right)$ is a pure-strategy BNE of the game Γ_2. Subsequently, the above results lead to Equation (5).

(ii) Consider $\delta > x^*$, i.e., $\delta \in \Delta_1$ and $p_2 < \frac{1}{2}$. In this case, $y_{12} < 0$. Let us consider again the payoff matrix below:

$$\begin{array}{c} R^M_{\text{aut}}\ R^L_{\text{aut}} \\ R^M_{\text{cyb}}\ R^L_{\text{aut}} \\ \\ \end{array} \begin{bmatrix} D^{\text{aut}}_{\text{accept}}\ D^{\text{cyb}}_{\text{reject}} & D^{\text{aut}}_{\text{reject}}\ D^{cyb}_{\text{reject}} \\ (x_{12}, y_{12}) & (0, 0) \\ (x_{22}, y_{22}) & (x_{24},\ 0) \end{bmatrix}$$

Clearly, $\delta > x^* = \frac{1}{1+\omega(1-2p_1)}$ holds only when $p_1 < \frac{1}{2}$ as $\delta \in (0, 1)$. But, when $p_1 < \frac{1}{2}$, we must have $C_{cyb} > \beta(2p_1 - 1)$ since $C_{cyb} \in (0, 1)$. But, $x_{22} > x_{12}$ when $C_{cyb} < \beta(2p_1 - 1)$. Thus, corresponding to this inequality, there is no equilibrium. Furthermore, it can be observed that $y_{22} > 0$ always holds and when $C_{cyb} > \beta(2p_1 - 1)$, we have $x_{24} < 0$. Hence, the strategy $\left(R^M_{\text{aut}}\ R^L_{\text{aut}}, D^{\text{aut}}_{\text{reject}}\ D^{\text{cyb}}_{\text{reject}}\right)$ is the only BNE. Thus, from this discussion, we arrive at Equation (6). □

Appendix D

Proof of Proposition 4. (i) If $p_2 > \frac{1}{2}$, we have $y_{21} > y_{22}$ and $y_{23} > y_{24}$. Therefore, the strategy $D^{aut}_{\text{accept}}\, D^{cyb}_{\text{reject}}$ is dominated by $D^{aut}_{\text{accept}}\, D^{cyb}_{\text{accept}}$ and the reduced matrix can be written as

$$\begin{array}{c|ccc} & D^{\text{aut}}_{\text{accept}}\, D^{\text{cyb}}_{\text{accept}} & D^{\text{aut}}_{\text{reject}}\, D^{cyb}_{\text{accept}} & D^{\text{aut}}_{\text{reject}}\, D^{cyb}_{\text{reject}} \\ R^M_{\text{aut}}\ R^L_{\text{aut}} & (x_{11}, y_{11}) & (x_{13}, y_{13}) & (x_{14}, y_{14}) \\ R^M_{\text{cyb}}\ R^L_{\text{aut}} & (x_{21}, y_{21}) & (x_{23}, y_{23}) & (x_{24}, y_{24}) \end{array}$$

Also, it can be shown that $y_{13} = y_{14} = 0$; therefore, the strategy $D^{\text{aut}}_{\text{reject}}\, D^{\text{cyb}}_{\text{reject}}$ is dominated by the strategy $D^{\text{aut}}_{\text{reject}}\, D^{cyb}_{\text{accept}}$. Hence, we have the following payoff matrix:

$$\begin{array}{c|cc} & D^{\text{aut}}_{\text{accept}}\, D^{\text{cyb}}_{\text{accept}} & D^{\text{aut}}_{\text{reject}}\, D^{cyb}_{\text{accept}} \\ R^M_{\text{aut}}\ R^L_{\text{aut}} & (x_{11}, y_{11}) & (x_{13}, y_{13}) \\ R^M_{\text{cyb}}\ R^L_{\text{aut}} & (x_{21}, y_{21}) & (x_{23}, y_{23}) \end{array}$$

In the matrix, the relation $y_{21} > y_{23}$ always holds. Therefore, we consider y_{11} and y_{13}. It can be verified that if $\delta < x^*$, then $y_{11} > y_{13}$. This leads to the following matrix:

$$\begin{array}{c|c} & D^{\text{aut}}_{\text{accept}}\, D^{\text{cyb}}_{\text{accept}} \\ R^M_{\text{aut}}\ R^L_{\text{aut}} & (x_{11}, y_{11}) \\ R^M_{\text{cyb}}\ R^L_{\text{aut}} & (x_{21}, y_{21}) \end{array}$$

If $C_{cyb} > 2\beta(p_1 - p_2)$, then $x_{11} > x_{21}$. Thus, $\left(R^M_{\text{aut}}\, R^L_{\text{aut}}, D^{\text{aut}}_{\text{accept}}\, D^{cyb}_{\text{accept}}\right)$ is a BNE, whereas, if $C_{cyb} < 2\beta(p_1 - p_2)$, then $\left(R^M_{cyb} R^L_{\text{aut}}, D^{\text{aut}}_{\text{accept}}\, D^{cyb}_{\text{accept}}\right)$ is a BNE of the game.

(ii) We now consider $\delta > x^*$ and $p_2 > \frac{1}{2}$. We know that $\delta > x^*$ only when $p_1 < \frac{1}{2}$. Let us recall that $p_1 > p_2$. Thus, this contradicts the condition being considered, i.e., $p_2 > \frac{1}{2}$. Hence, there is no equilibrium in this case. □

Table A1. Notations and their meanings.

Notation	Meaning
R_{aut}	Request through authentication
R_{cyb}	Request through cyberattack
D_{accept}	Accept data access request and release data
D_{reject}	Reject data access request and do not release data
C_{cyb}	Cost of cyberattack
$\mathcal{H}_1$	Action set of an insider
$\mathcal{H}_d$	Action set of the defender
Ω	Type set of an insider
S_1	Pure strategy set of an insider in the simultaneous move gamemodel
S_D	Pure strategy set of the defender in the simultaneous move gamemodel
$S_1^{'}$	Pure strategy set of an insider in the sequential move game model
ω	Payoff due to discovery of malicious insider identity or dataprotection

Table A1. *Cont.*

Notation	Meaning
β	Payoff corresponding to compromising data
P_1	Probability that malicious insider who uses authentication isdiscovered
P_2	Probability that malicious insider who launches a cyberattack isdiscovered
$V_i(a, b \mid \theta)$	Player i's payoff corresponding to profile (a, b) and insider type θ
$\mathcal{N}$	Set of players in the game
$\mathcal{H}$	Strategy space
$\mathbb{R}$	Set of real numbers
$\mathbb{R}_{++}$	Set of positive real numbers
N	Nature that can be considered as a non-strategic player
M	Malicious type
L	Legitimate type
δ	Probability that an insider is malicious
$1 - \delta$	Probability that an insider is legitimate
$U_i\left(R^M_{cyb} R^L_{\mathrm{aut}}, D_{\mathrm{accept}}\right)$	Player i' s expected payoff corresponding to strategy profile $\left(R^M_{cyb} R^L_{\mathrm{aut}}, D_{\mathrm{accept}}\right)$ in the simultaneous move game
$U_i'\left(R^M_{\mathrm{cyb}}\ R^L_{\mathrm{aut}}, D^{\mathrm{aut}}_{\mathrm{accept}}\ D^{\mathrm{cyb}}_{\mathrm{reject}}\right)$	Player i' s expected payoff corresponding to strategy profile $\left(R^M_{cyb} R^L_{\mathrm{aut}}, D^{\mathrm{aut}}_{\mathrm{accept}}\ D^{\mathrm{cyb}}_{\mathrm{reject}}\right)$ in the sequential move game
S_i'	Strategy space of player i in the sequential move game model
$\mathit{\Gamma}$	Proposed simultaneous move game model
$\mathit{\Gamma}_1$	Extended simultaneous move game model
$\mathit{\Gamma}_2$	Proposed sequential move game model
BNE	Bayesian Nash Equilibrium
PBE	Perfect Bayesian Nash Equilibrium

References

1. Mantha, B.; García De Soto, B.; Karri, R. Cyber security threat modeling in the AEC industry: An example for the commissioning of the built environment. *Sustain. Cities Soc.* **2021**, *66*, 102682. [CrossRef]
2. Watson, S. Cyber-Security: What Will It Take for Construction to Act? Construction News. Available online: https://www.constructionnews.co.uk/tech/cyber-security-what-will-it-take-for-construction-to-act-22-01-2018/ (accessed on 24 November 2023).
3. FinalCode. *Managing CAD File Data Leakage Risks in Design-Centric Businesses*; FinalCode: San Jose, CA, USA, 2016. Available online: https://www.finalcode.com/en/wp-content/uploads/2017/08/FC-WP-CAD-ManagingFileDataLeakage-072516d.pdf (accessed on 5 April 2024).
4. Sawyer, T.; Rubenstone, J. Construction Cybercrime Is on the Rise. Engineering News-Record (ENR). Available online: https://www.enr.com/articles/46832-construction-cybercrime-is-on-the-rise (accessed on 4 February 2024).
5. Tao, X.; Das, M.; Liu, Y.; Cheng, J.C.P. Distributed common data environment using blockchain and Interplanetary File System for secure BIM-based collaborative design. *Autom. Constr.* **2021**, *130*, 103851. [CrossRef]
6. Sonkor, M.S.; García de Soto, B. Towards Secure Construction Networks: A Data-Sharing Architecture Utilizing Blockchain Technology and Decentralized Storage. In Proceedings of the Construction Blockchain Consortium Conference 2021 (CBC2021), London, UK, 20–22 October 2021.
7. Turk, Ž.; Sonkor, M.S.; Klinc, R. Cybersecurity Assessment of BIM/CDE Design Environment Using Cyber Assessment Framework. *J. Civ. Eng. Manag.* **2022**, *28*, 349–364. [CrossRef]
8. Turk, Ž.; García De Soto, B.; Mantha, B.R.K.; Maciel, A.; Georgescu, A. A systemic framework for addressing cybersecurity in construction. *Autom. Constr.* **2022**, *133*, 103988. [CrossRef]

9. García De Soto, B.; Turk, Ž.; Maciel, A.; Mantha, B.; Georgescu, A.; Sonkor, M.S. Understanding the Significance of Cybersecurity in the Construction Industry: Survey Findings. *J. Constr. Eng. Manag.* **2022**, *148*, 04022095. [CrossRef]
10. Maglaras, L.; Janicke, H.; Ferrag, M.A. Cybersecurity of Critical Infrastructures: Challenges and Solutions. *Sensors* **2022**, *22*, 5105. [CrossRef]
11. Gheyas, I.A.; Abdallah, A.E. Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis. *Big Data Anal.* **2016**, *1*, 6. [CrossRef]
12. Hu, P.; Li, H.; Fu, H.; Cansever, D.; Mohapatra, P. Dynamic defense strategy against advanced persistent threat with insiders. In Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM), Hong Kong, China, 26 April–1 May 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 747–755.
13. Ni, S.; Zou, S.; Chen, J. Evolutionary Game Model of Internal Threats to Nuclear Security in Spent Fuel Reprocessing Plants Based on RDEU Theory. *Sustainability* **2022**, *14*, 2163. [CrossRef]
14. Kim, K.-N.; Suh, Y.-A.; Schneider, E.; Yim, M.-S. Physical Protection System Design Analysis against Insider Threat based on Game Theoretic Modeling. In Proceedings of the Transactions of the Korean Nuclear Society Spring Meeting, Jeju, Korea, 7–8 May 2015.
15. Kim, K.-N.; Yim, M.-S.; Schneider, E. A study of insider threat in nuclear security analysis using game theoretic modeling. *Ann. Nucl. Energy* **2017**, *108*, 301–309. [CrossRef]
16. Liu, D.; Wang, X.; Camp, J. Game-theoretic modeling and analysis of insider threats. *Int. J. Crit. Infrastruct. Prot.* **2008**, *1*, 75–80. [CrossRef]
17. Kantzavelou, I.; Katsikas, S. A game-based intrusion detection mechanism to confront internal attackers. *Comput. Secur.* **2010**, *29*, 859–874. [CrossRef]
18. Elmrabit, N.; Yang, S.-H.; Yang, L.; Zhou, H. Insider Threat Risk Prediction based on Bayesian Network. *Comput. Secur.* **2020**, *96*, 101908. [CrossRef]
19. Laszka, A.; Johnson, B.; Schöttle, P.; Grossklags, J.; Böhme, R. Managing the Weakest Link. In Proceedings of the Computer Security—ESORICS 2013, Egham, UK, 9–13 September 2013; Crampton, J., Jajodia, S., Mayes, K., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; pp. 273–290. [CrossRef]
20. Feng, X.; Zheng, Z.; Cansever, D.; Swami, A.; Mohapatra, P. Stealthy attacks with insider information: A game theoretic model with asymmetric feedback. In Proceedings of the MILCOM 2016—2016 IEEE Military Communications Conference, Baltimore, MD, USA, 1–3 November 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 277–282. [CrossRef]
21. Cansever, D. Security Games with Insider Threats. In *Decision and Game Theory for Security*; Zhu, Q., Baras, J.S., Poovendran, R., Chen, J., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2020; Volume 12513, pp. 502–505.
22. Liu, D.; Wang, X.; Camp, L.J. Mitigating Inadvertent Insider Threats with Incentives. In *Financial Cryptography and Data Security*; Dingledine, R., Golle, P., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2009; Volume 5628, pp. 1–16.
23. Gataullin, T.M.; Gataullin, S.T.; Ivanova, K.V. Synergetic Effects in Game Theory. In Proceedings of the 2020 13th International Conference "Management of Large-Scale System Development" (MLSD), Moscow, Russia, 28–30 September 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–5. [CrossRef]
24. Joshi, C.; Aliaga, J.R.; Insua, D.R. Insider Threat Modeling: An Adversarial Risk Analysis Approach. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 1131–1142. [CrossRef]
25. Hu, T.; Xin, B.; Liu, X.; Chen, T.; Ding, K.; Zhang, X. Tracking the Insider Attacker: A Blockchain Traceability System for Insider Threats. *Sensors* **2020**, *20*, 5297. [CrossRef]
26. Kim, J.; Park, M.; Kim, H.; Cho, S.; Kang, P. Insider Threat Detection Based on User Behavior Modeling and Anomaly Detection Algorithms. *Appl. Sci.* **2019**, *9*, 4018. [CrossRef]
27. Hall, A.J.; Pitropakis, N.; Buchanan, W.J.; Moradpoor, N. Predicting Malicious Insider Threat Scenarios Using Organizational Data and a Heterogeneous Stack-Classifier. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 5034–5039. [CrossRef]
28. Al-Shehari, T.; Alsowail, R.A. An Insider Data Leakage Detection Using One-Hot Encoding, Synthetic Minority Oversampling and Machine Learning Techniques. *Entropy* **2021**, *23*, 1258. [CrossRef] [PubMed]
29. Azaria, A.; Richardson, A.; Kraus, S.; Subrahmanian, V.S. Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data. *IEEE Trans. Comput. Soc. Syst.* **2014**, *1*, 135–155. [CrossRef]
30. Chattopadhyay, P.; Wang, L.; Tan, Y.-P. Scenario-Based Insider Threat Detection From Cyber Activities. *IEEE Trans. Comput. Soc. Syst.* **2018**, *5*, 660–675. [CrossRef]
31. Brdiczka, O.; Liu, J.; Price, B.; Shen, J.; Patil, A.; Chow, R.; Bart, E.; Ducheneaut, N. Proactive Insider Threat Detection through Graph Learning and Psychological Context. In Proceedings of the 2012 IEEE Symposium on Security and Privacy Workshops, San Francisco, CA, USA, 24–25 May 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 142–149. [CrossRef]
32. Fudenberg, D.; Tirole, J. *Game Theory*; MIT Press: Cambridge, MA, USA, 1991.

33. Manshaei, M.H.; Zhu, Q.; Alpcan, T.; Bacşar, T.; Hubaux, J.-P. Game theory meets network security and privacy. *ACM Comput. Surv.* **2013**, *45*, 1–39. [CrossRef]
34. Zhu, Y.; Huang, D.; Hu, C.-J.; Wang, X. From RBAC to ABAC: Constructing Flexible Data Access Control for Cloud Storage Services. *IEEE Trans. Serv. Comput.* **2015**, *8*, 601–616. [CrossRef]
35. Adzroe, E.; Ingirige, B. Innovation in e-business: Issues related to adoption for micro and SME organisations. In *Advances in Construction ICT and e-Business*; Perera, S., Ingirige, B., Ruikar, K., Obonyo, E., Eds.; Routledge: London, UK, 2017; pp. 316–339. [CrossRef]
36. Vasilyevna, N.B. An RBAC Design with Discretionary and Mandatory Features. In Proceedings of the 2008 International Symposium on Ubiquitous Multimedia Computing, Hobart, Australia, 13–15 October 2008; IEEE: Piscataway, NJ, USA, 2008; pp. 260–263. [CrossRef]
37. Autodesk. Security Whitepaper. Available online: https://construction.autodesk.com/resources/guides/acc-security-whitepaper/ (accessed on 9 April 2023).
38. Homoliak, I.; Toffalini, F.; Guarnizo, J.; Elovici, Y.; Ochoa, M. Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. *ACM Comput. Surv.* **2020**, *52*, 1–40. [CrossRef]
39. Das, M.; Tao, X.; Cheng, J.C.P. BIM security: A critical review and recommendations using encryption strategy and blockchain. *Autom. Constr.* **2021**, *126*, 103682. [CrossRef]
40. Stamou, A.I. Verification and application of a mathematical model for the assessment of the effect of guiding walls on the hydraulic efficiency of chlorination tanks. *J. Hydroinform.* **2002**, *4*, 245–254. [CrossRef]
41. Yao, D. Game-Models-Simulation-Code. GitHub. Available online: https://github.com/SMART-NYUAD/Game-models-simulation-code (accessed on 2 April 2024).
42. Hughes, W.; Murdoch, J. *Roles in Construction Projects: Analysis and Terminology*; Construction Industry Publications: Birmingham, UK, 2001.
43. FIRST. *Common Vulnerability Scoring System Version 3.1*; FIRST: Cary, NC, USA, 2019. Available online: https://www.first.org/cvss/v3.1/specification-document (accessed on 4 February 2024).
44. Parker, D.B. *Fighting Computer Crime: A New Framework for Protecting Information*; Wiley: New York, NY, USA, 1998.
45. Dreyfus, H.L.; Drey-fus, S.E.; Zadeh, L.A. Mind over Machine: The Power of Human Intuition and Expertise in the Era of the Computer. *IEEE Expert* **1987**, *2*, 110–111. [CrossRef]
46. *ISO/IEC ISO/IEC 27001:2022*; Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. ISO/IEC: Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/27001 (accessed on 4 February 2024).
47. Silvander, J.; Singh, S.P. Validating Trust in Human Decisions to Improve Expert Models Based on Small Data Sets. In *Business Modeling and Software Design*; Shishkov, B., Ed.; Lecture Notes in Business Information Processing; Springer Nature: Cham, Switzerland, 2023; Volume 483, pp. 256–267. [CrossRef]
48. Almomani, M.A.; Basri, S.; Almomani, O.; Capretz, L.F.; Balogun, A.; Husni, M.; Gilal, A.R. Using an Expert Panel to Validate the Malaysian SMEs-Software Process Improvement Model (MSME-SPI). In *Software Engineering Perspectives in Intelligent Systems*; Silhavy, R., Silhavy, P., Prokopova, Z., Eds.; Advances in Intelligent Systems and Computing; Springer International Publishing: Cham, Switzerland, 2020; Volume 1294, pp. 844–859. [CrossRef]
49. Pleshakova, E.; Osipov, A.; Gataullin, S.; Gataullin, T.; Vasilakos, A. Next gen cybersecurity paradigm towards artificial general intelligence: Russian market challenges and future global technological trends. *J. Comput. Virol. Hacking Tech.* **2024**, *20*, 429–440. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.