Journal of Engineering and Applied Research (JEAR)

National University of Skill

Winter & Spring 2026, Vol. 3, No. 1, p. 192- 207

Journal Homepage: https://jear.tvu.ac.ir

:10.48301/jear.2025.385426.1002

Predicting Malicious Behavior of Insiders using Game Theory

Hamed Sepehrzadeh [1*], Sana Haghighi [2]

[1] Department of Computer engineering, Technical and Vocational University (TVU), Tehran, Iran.

[2] Faculty of Computer Science and Engineering, Shahid Beheshti University, Tehran, Iran.

ARTICLE INFO

Article Type:
Original Research

Received: 2023.12.02
Revised: 2025.03.29
Accepted: 2025.04.19

Keyword:
Information Security
Organization
Employee
Insider
Game Theory
Modelling, Evaluation

***Corresponding Author:**
Hamed Sepehrzadeh
Email: *hsepehrzadeh@tvu.ac.ir*

ABSTRACT

Information security is a crucial issue nowadays in organizations. Security flaws are serious threats to an organization. Every organization has sensitive information that may be threatened by malicious adversaries and even employees (insiders). In order to limit security incidents, each organization must concentrate on employee's behavior. Indeed, employees of an organization act as a natural safeguard for information. Therefore, predicting the behavior of internal employees against the information assets of the organization is very important. To this end, this paper proposes a game-theoretic modelling approach to capture the interaction between employees and organization to predict malicious employees (insiders) and organizations behavior with incomplete information. The game parameters are some important elements of security culture including influencing and organizational behavior factors, and security related factors. By solving the game model, Nash equilibriums are computed and best-response strategies for the players are recognized. Quantitative evaluation of the information security of organization can be done according to the probability of performing unacceptable behavior by employees and the probability of organization investment in order to increase the organizational security culture.

E-ISSN: 3060-6357

Introduction

Nowadays concentrating on employee's behavior is very important to limit security incidents. Increasing number of security incidents caused by insiders shows that it is very crucial to have methods to predict the behavior of internal personals. To this end and in order to understand the reasons behind malicious behavior of employees and strengthening information security, human factors should be recognized [1]. Information leakage can be a prelude to further catastrophic attacks [2].

This issue is much more critical in the industry. Leakage of information or any unacceptable behavior of employees may lead to a dangerous event such as an explosion or endanger human safety [3, 4]. Therefore, the role of employees in ensuring the security of the organization is very important and should be given serious attention [5, 6].

Game theory [7] tries to model the mathematical behavior governing a strategic situation (conflict of interest). This situation arises when the success of a person depends on the strategies that others choose. The ultimate goal is to find the optimal strategy for the players. Therefore, game theory will be a suitable choice for modelling the interaction between organizations and their employees [8].

First, this paper tries to identify the important behavioral and organizational factors influencing the employee's decision to engage in adversarial behavior. Then, it provides an approach to model the interaction between employees and organization by employing the recognized factors to predict the employee's behavior.

The proposed modelling approach is based on game theory to find out how the organization and the employees choose their interdependence strategies.

The main contributions of the paper are as follows:

- Identifying the important factors influencing the employee's decision to engage in adversarial behavior which can lead to information leakage.
- Proposing a modelling approach capture interaction between an employee and organization in order to study and predict the employee's behavior with in complete information.
- Evaluating the organization information security by using the proposed model by concentrating on insider's behavior.
- Providing an illustrative example in order to demonstrate the applicability of the presented method.

Note that it is assumed that the organization do not have complete information about the employee for some factors. Therefore, the best option to model the conflict between them is to use the Bayesian game-based modeling method with incomplete information [9]. So, the proposed game-based model is a Bayesian game.

The rest of the paper is structured as follows. Section 2 provides some related researches in the context of information security estimation. Section 3 presents the detailed description of the presented game-based model. Section 4 provides an illustrative example for employing the presented model. Finally, Section 5 concludes the paper.

Related work

In this section, we focus on providing an overview of some related researches in the context of information security and insider threats.

Siponen et al. [10] have provided a comparison between guidelines including: BS ISO/IEC17799: 2000, BS7799, the SSE-CMM, and GASPP/GAISP to determine and study how widely they can be exploited.

Their study shows that these guidelines are very generic and consequently they do not pay attention to the different security requirements in different organizations.

Shamala et al. [11] have concentrated on studying the effect of information quality (IQ) dimensions on the quality of the information throughout the information gathering and ISRM process. They have finally emphasized that information quality (IQ) dimensions have a significant effect on ensuring the information quality of an organization.

Kim et al. [12] have proposed an approach to categorize large sets of threat incidents for using as a security information event management (SIEM) operation. To this end, they have exploited deep learning techniques. The classification is done according to accuracy, learning and efficiency.

Wiley et al. [13] have studied the relationship between organizational culture, security culture and information security awareness. Their investigations showed that security culture has a higher priority and importance than others.

Tolah et al. [14] have provided a framework for developing security culture. They have considered two types of factors in their framework including influence security culture factors and reflect security culture factors. Finally, the presented framework was validated through an empirical study.

Figueira et al. [15] have proposed an approach to estimate the state of an organization to evaluate the probability of occurring a threat. Their goal was identifying the current state of vulnerabilities existing in the system, to improve risk calculation, and finally determining the most critical risks. They have provided a validation by applying the proposed method in a business environment.

McCormac et al. [16] have concentrated on exploring the relationship between individual difference variables such as personality, risk-taking propensity, age and gender, and information security awareness. They have used the Human Aspects of Information Security Questionnaire (HAIS-Q) for measurement process. Their examination shows that emotional stability, agreeableness, conscientiousness and risk-taking propensity have a significant effect on individuals information security awareness.

Thangavelu et al. [17] have presented a modelling approach to examine the existing relationship between system, security, situational awareness, and security experts' capability to diagnostic, evaluate, and mitigate potential threats. They have also empirically validated the model and studied the consequences of self-efficacy and metacognitive awareness on the relationship between threat management and security awareness issues.

In order to provide a comparison between alternative security management techniques, Nazareth et al. [18] have proposed a system dynamic modelling

approach. Their study has shown that focusing on security detection tools has a higher outcome than does deterrence investment.

Compared with the described approaches, this paper proposes a modelling approach to predict the employee's unacceptable behavior against information security of the organization. the presented approach models the organization and the employee's interaction as a Bayesian game with incomplete information. The considered parameters for the game are some important elements of security culture including influencing and organizational behavior and security related factors.

The Proposed Model

Description of the game model

A common assumption in games is usually that the players know each other's benefit, and this is only for simplification and can sometimes be acceptable for some applications [9]. In most cases, the players do not have complete information about each other. Therefore, the best option to model the conflict between them is to use the Bayesian game-based modeling method with incomplete information [19, 20]. A game in which at least one of the players does not have complete information about some features of the game that affect his decisions is called a Bayesian game [20]. For this reason, Bayesian game is used in this article to model the conflict between the organization and the employee.

Formally, the proposed game model is defined as a multiple G = <P, Si, Uij>, where P is the set of players, Si is the set of actions or strategies of player i, and Uij is the probability of player i choosing strategy j. The set of players P is defined as P = {E, O}, where E is the set of employee types and O is the set of organization types. Assuming that Tei is the type of employee i, the types of employees Ei will have the probability distribution E = {e1, e2, …, en}. Similarly, there will be probability distributions O = {o1, o2, ..., on} for all types of Oi organizations.

In a Bayesian game, the strategy of the players is determined before that the player's type is recognized. In fact, before choosing the type, each player decides what action to perform for each existing type. A Bayesian Nash equilibrium is defined as a strategy profile that maximizes the expected profit for each player given the type of each player and the strategies that other players take. That is, strategy profile x is a Nash-Bayesian equilibrium if and only if for each player i, and assuming the strategy of every other player is constant, strategy xi maximizes player i's expected profit. Regarding the equilibrium points of the Bayesian game, if the first player does not know the type of the second one, his choice of a1 is optimal if the following relationship holds:

$$p \times u_1(a_1, a_2(t_1)) + (1-p) \times u_1(a_1, a_2(t_2)) \geq p \times u_1(a_1', a_2(t_1)) + (1-p) \times u_1(a_1', a_2(t_2)); \forall a_1' \quad (1)$$

where p is the probability of choosing player type 1, u1 is the utility function of player 1, a2(t1) is the choice of player 2 if player 1 is type 1, and a2(t2) is the choice of player 2 if the second player's type is 2.

If the second player knows the type of the first player, then we will have the game for equilibrium:

$$u_2(a_1, a_2(t_1), t_1) \geq u_2(a_1, a_2'(t_1), t_1); \forall a_2' \quad (2)$$

in which, t1 and t2 are the type of the second player, u2 is the utility function of the second player and a2(t1) is the choice of player two if the second player is of type one. This relationship is also valid for the case where the type of the second player is 2 (t2). In this case, because the player knows his type, the probability p is not important for him.

Employees' strategy is considered to perform malicious behavior (P) or not to perform (NP): SE = {P, NP}. Also, the strategy of the system is considered in the form of investigation in information security improvement (I) and not investigation (NI): SS = {I, NI}. The cost of improving security can include training employees, establishing a new security policy, performing security risk assessment, and so on.

In this model, it is assumed that the organization does not have full understanding about the employee's job satisfaction, and for this reason, it estimates that the employee's job satisfaction will be lower than S' with probability of PS and higher than S' with probability of 1-PS. we refer to the Ps parameter as the uncertainty parameter. According to this assumption, the employee's profit from doing unacceptable behavior will be different. As a result, we can assume that we are dealing with two types of employees: type 1, employees with a low level of job satisfaction, and type 2, employees with a high level of job satisfaction. According to the mentioned description, the organization do not have complete information about employees, so the game is a Bayesian game with incomplete information.

Now, it is the time to discuss about the game parameters. As stated before, the game parameters are some important elements of security culture including influencing and organizational behavior factors. First, we concentrate on influencing and organizational behavior factors.

- **Information security enhancement cost**: This factor is an influencing factor. Top managers or senior leadership are one of the important elements that leads to the information security improvement in an organization. To what extent the top managers are aware of the importance of the information security function will play a significant role in improving the information security of the organization. In order to achieve information security success, top managers should invest on security risk assessment, establishing and improving security policies, and training employees [14, 21].
- **Access level**: Access levels restrict employees access to the important organizational information and assets. Indeed, they are a way to control which person has access to organization resources or information. By using access levels, organizations can determine whether an employee should be able to perform a certain issue or observe a certain document.

- **Security knowledge**: The employee's knowledge about information security has a great impact on the organization's information security [22]. An employee may unintentionally cooperate with attackers due to the lack of knowledge and information about the importance of information security, penetration paths, and suspicious behavior of attackers.
- **The value of the organization's assets**: Every organization has valuable resources of information and infrastructure that may be misused by internal employees or become available to attackers. One of the goals of the organization is to protect these assets from being misused by internal employees and attackers. How much the unacceptable behavior of an employee affects the valuable assets of the organization should be estimated.
- **Job satisfaction**: Job satisfaction [14] is defined as employee satisfaction with the organization in which he/she works, his/her salary and income, his/her managers, and his/her position in the organization. Job satisfaction plays a significant role in attitudes [21] and even behaviors of employees towards information security. An employee who is not satisfied with his/her job is more likely to engage in unacceptable behavior towards information security.
- **Personality trait**: Personality traits describe the potential factors of employees and help to understand the psychological mechanisms that influence the employee's behavior regarding the organization's information security [23]. There are some important factors, such as agreeableness, openness, conscientiousness, extroversion and neuroticism which can affect the employee's personality traits [14].
- **Detection probability**: The organization may discover unacceptable behavior of its employees with a probability.
- **Penalty**: The organization may consider penalties for unacceptable behavior of its employees as a way to prevent this from happening.

In order to model the game that can be solved using the conventional game solving method, the standard representation of the game model is given in Table 1. The first line in each cell shows the profit of the employee and the second line shows the profit of the organization.

In summary, the game parameters are as follows:

- C: the cost of security enhancement activities,
- d: the detection probability of malicious behavior of employees,
- PY: the penalty of employees due to his/her malicious behavior,
- V: the value of the organization's assets available to the employee,
- S: job satisfaction of the employee,
- PT: the employee's personality trait,
- K: the employee's knowledge level in information security domain,

AL: the employee's access level to the organization confidential information and infrastructure.

A strategy profile (P, Q) is defined as the action taken by players of the game, in which, P ∈ A1 and Q ∈ A2. It is assumed that an employee based on his/her knowledge, access level, job satisfaction, and personal traits can target the information security of the organization. The higher job satisfaction, personal traits, and information security knowledge of an employee, the lower the possibility of unacceptable behavior. Also, a higher access level may lead to a greater effect. So, the effect parameter E, which denotes the effect of the employee's unacceptable behavior on the assets of the organization, can be defined as follows:

$$E = \frac{AL}{PT \times S \times K} \quad (3)$$

It is assumed that the employee's earning and penalty as a result of an unacceptable behavior is related to his/her effect parameter.

First, we explain the strategy profile (P, I), where the employee decides to perform a malicious behavior and the organization decides to invest in information security. In this case, the employee gets a reward of E×V for his effect on the assets of the organization, gets a reward C because of imposing cost for investing in the information security protection, and incurs a penalty d×E×PY as a result of the detection of his/her unacceptable behavior. The organization incurs a cost C as a result of investing in information security improvement and incurs a cost E×V for the effect of employee behavior on the organization's information security.

The second strategy profile is (NP, I), where the employee decides not to perform a malicious behavior and the organization decides to invest in information security. Here, the employee's profit is zero due to the lack of action against the organization's information security. The organization incurs a cost C for investing in the information security and gets a reward V as a result of protecting against unacceptable employee's behavior.

The third strategy profile is (P, NI), where the employee decides to perform an unacceptable behavior and the organization decides not to invest in information security. In this case, the employee gets a reward of E×V for his effect on the assets of the organization, and incurs a penalty d×E×PY as a result of the detection of his/her unacceptable behavior. Besides, the organization incurs a cost V for the effect of employee behavior on the organization's information security due to not investing in information security.

The final strategy profile is (NP, NI), where the employee decides to perform an unacceptable behavior and the organization decides not to invest in information security. In this case, the employee's payoff is equal to zero and the organization's payoff is equal to V, as a result of protecting against unacceptable employee's behavior.

Solving the game

This section describes the game solution process. First, we concentrate on Nash equilibrium analysis. Then, we focus on the mixed strategy equilibrium analysis.

According to the definition of the Nash equilibrium, the strategy profile (P, I) is a Nash equilibrium, if we have:

$$C + E \times (V - d \times PY) > 0\,, -C - E \times V > -V \quad (4)$$

Similarly, the strategy profile (*P*, *NI*) is a Nash equilibrium, if we have:

(5)

$$E \times (V - d \times PY) > 0\,, -V > -C - E \times V \rightarrow V > d \times PY, C > V \times (1 - E)$$

Table 1. The presented game model

		Organization	
		I	***NI***
Employee	*P*	$C + E \times (V - d \times PY)$	$E \times (V - d \times PY)$
		$-C - E \times V$	$-V$
	NP	0	0
		$-C + V$	V

For the strategy profile (NP, I), we don't have any Nash equilibrium and finally, the strategy profile (NP, NI) is a Nash equilibrium, if we have:

$$E \times (V - d \times PY) < 0\,, V > -C + \mathrm{V} \rightarrow V < d \times PY, C > 0 \quad (6)$$

We now explain the mixed strategy equilibrium analysis of the game model. Let Q is the probability of performing unacceptable behavior of the employee and R is the probability of investing in investing security by the organization, for the probability mixed strategy Nash Equilibrium [24, 25] of the employee (UE) we will have:

$$U_E = Q \times P + (1 - Q) \times NP \quad (7)$$

The probability mixed strategy Nash Equilibrium of the organization (UO) is given as:

$$U_O = R \times I + (1 - R) \times NI \quad (8)$$

From the game theory basic principles, the players should be indifferent between their possible strategies. So, they should have same expected payoffs regarding their strategies. Therefore, for the organization and the employee we have:

$$U_O(I) = U_O(NI) \tag{9}$$

and

$$U_E(P) = U_E(NP) \tag{10}$$

For the organization, we have:

$$\begin{aligned} U_O(P) = U_O(NP) \\ &\rightarrow P \times (C + E \times (V - d \times PY)) + (1 - P) \\ &\times (E \times (V - d \times PY)) = 0 \end{aligned}$$

$$\rightarrow P = \frac{E \times (d \times PT - V)}{C} \tag{11}$$

Considering the employee, we will have:

$$\begin{aligned} U_O(P) = U_O(NP) &\rightarrow I \times (-C - E \times V) + (1 - I) \times (-C + V) \\ &= I(-V) + (1 - I) \times V \end{aligned}$$

$$\rightarrow I = \frac{C}{V \times (1 - E)} \tag{12}$$

Consequently, the player's optimal strategy in the presented game can be calculated from Eqs. (11) and (12).

An illustrative example

In this section, by providing an illustrative example, we intend to show how the presented modelling method can be used to assess the security of CPSs. Table 2 provides the game parameters related to the considered hypothetical organization and its employees.

Considering the default values of the game parameters, the game solution is as follows:

- The probability of performing malicious behavior by the employee is equal to 0.4,
- The probability of investing in information security is equal to 0.3.

Now, we investigate the effect of some parameters on the game player's behaviors. First, we examine the effect of the investment cost on the probabilities of performing unacceptable behavior by the employee and investing in information security. As Figure 1 displays, the probability of investing in security decreases as investment cost increases. This is because the

organization has to spend more, and with the increase in the investment cost, the probability of investing in information security will decrease. On the other hand, as demonstrated in Figure 2, the probability of performing unacceptable behavior by the employee increases as investment cost increases.

Table 2. The game parameters and values

Parameter	Value	Rang
V	5	[5, 5]
AL	0.5	[0, 0.99]
R	1	[1, 2]
S	1	[1, 2]
K	1	[1, 2]
d	0.6	0.6
PT	7	7
C	1	[0, 2]

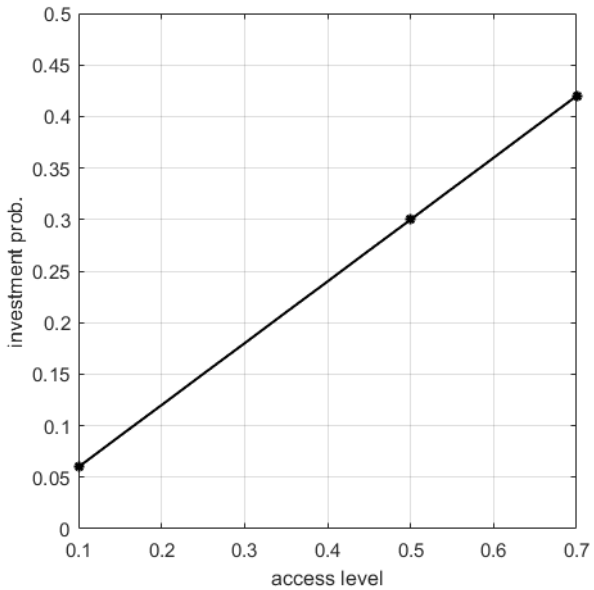

Figure 1. The effect of access level on the information security investment probability of the organization

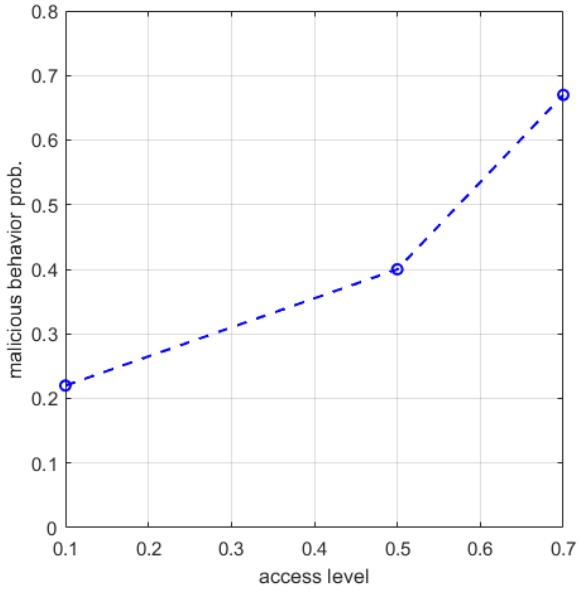

Figure 2. The effect of access level on the malicious behavior probability of the employee

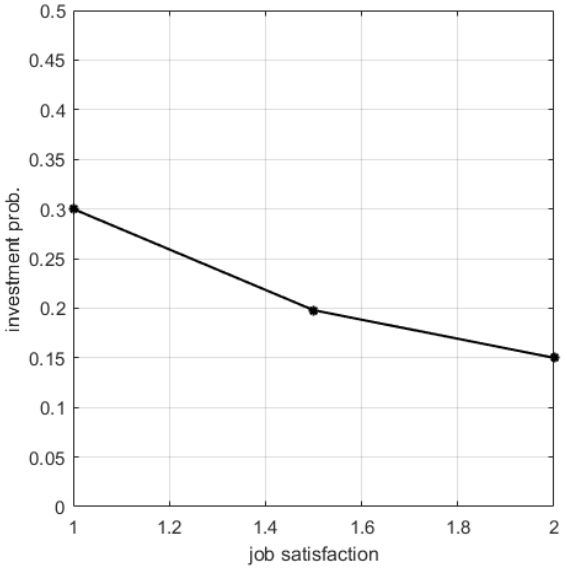

Figure 1. The effect of job satisfaction on the information security investment probability of the organization

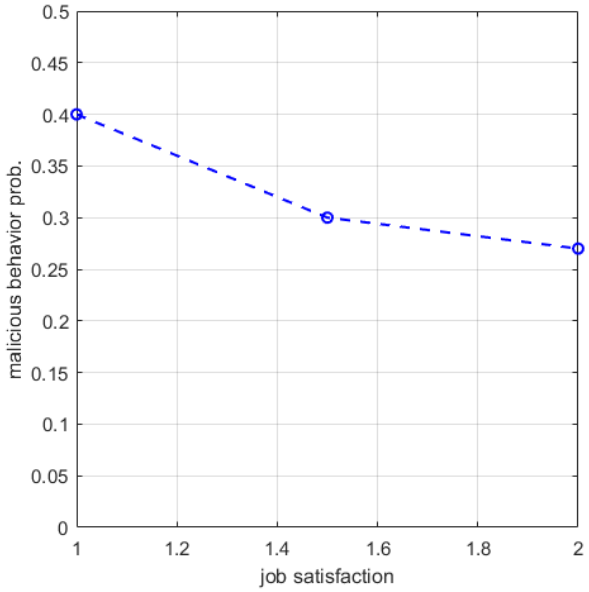

Figure 2. The effect of job satisfaction on the malicious behavior probability of the employee

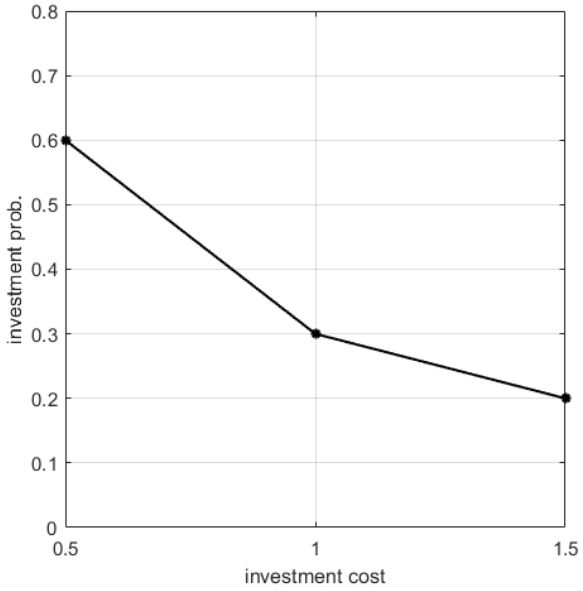

Figure 3. The effect of security investment cost on the information security investment probability of the organization

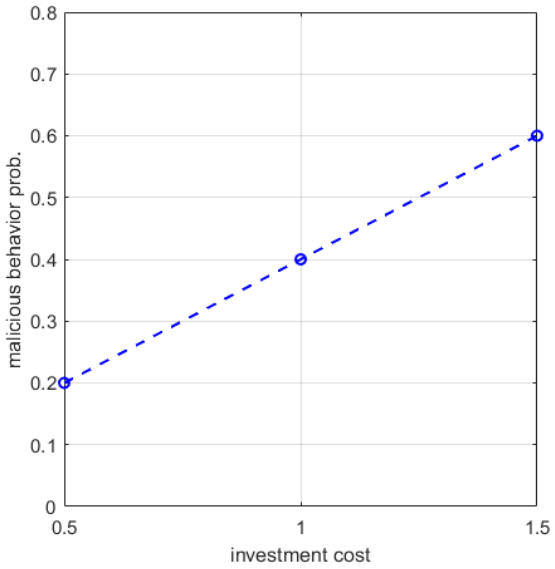

Figure 4. The effect of security investment cost on the malicious behavior probability of the employee

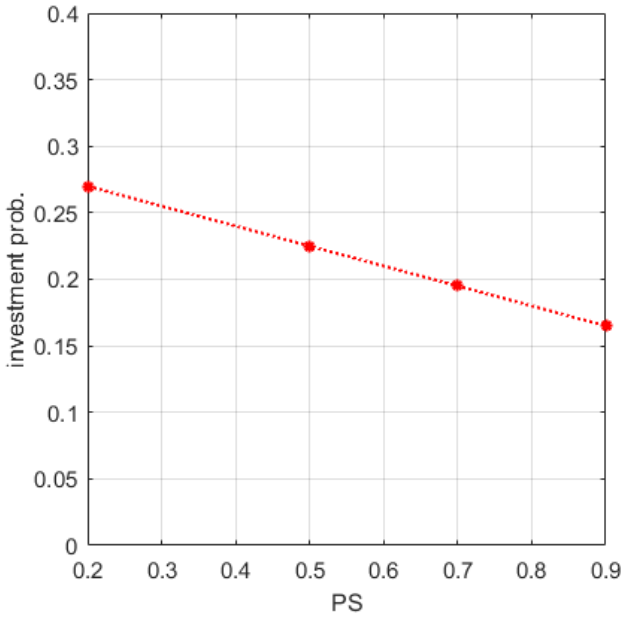

Figure 5. The effect of *PS* on the information security investment probability of the organization

Conclusion

This paper proposes a game-theoretic based modelling approach to model the organization and the employee's interactions. The proposed model is a two person non-zero-sum Bayesian game to predict the employee's malicious behavior. The proposed model employs the important elements of security culture for organizational employees in the model including: job satisfaction, access level, security investment, personality trait, information security knowledge of employees, and sensitive information assets. By solving the game model, we can estimate the probability of performing unacceptable behavior of an employee and the probability of organization investment in order to increase the organizational security culture and protect information security. As a future work, we want to extend the proposed model and its parameters for increasing the accuracy of assessments.

References

[1] AlHogail, A., (2015). Design and validation of information security culture framework. *Computers in human behavior*, *49*, 567-575.

[2] Reid, R. and Van Niekerk, J., (2014). Brain-compatible, web-based information security education: a statistical study. *Information Management & Computer Security*.

[3] Orojloo, H. and Azgomi, M.A., (2017). A method for evaluating the consequence propagation of security attacks in cyber–physical systems. *Future Generation Computer Systems*, *67*, 57-71.

[4] Humayed, A., Lin, J., Li, F. and Luo, B., (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal*, *4*(6), 1802-1831.

[5] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C., (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security*, *42*, 165-176.

[6] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T., (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security*, *66*, 40-51.

[7] Osborne, M.J., (2004). *An introduction to game theory* (Vol. 3, No. 3). New York: Oxford university press.

[8] Liang, X. and Xiao, Y., (2012). Game theory for network security. *IEEE Communications Surveys & Tutorials*, *15*(1), 472-486.

[9] Cui, Y., Quddus, N., & Mashuga, C. V. (2020). Bayesian network and game theory risk assessment model for third-party damage to oil and gas pipelines. *Process Safety and Environmental Protection*, 134, 178-188.

[10] Siponen, M. and Willison, R., (2009). Information security management standards: Problems and solutions. *Information & management*, *46*(5), 267-270.

[11] Shamala, P., Ahmad, R., Zolait, A. and Sedek, M., (2017). Integrating information quality dimensions into information security risk management (ISRM). *Journal of Information Security and Applications*, *36*, 1-10.

[12] Kim, J.Y. and Kwon, H.Y., (2022). Threat Classification Model for Security Information Event Management Focusing on Model Efficiency. *Computers & Security*, p.102789.

[13] Wiley, A., McCormac, A. and Calic, D., (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, *88*, p.101640.

[14] Tolah, A., Furnell, S.M. and Papadaki, M., (2021). An empirical analysis of the information security culture key factors framework. *Computers & Security*, *108*, p.102354.
[15] Figueira, P.T., Bravo, C.L. and López, J.L.R., (2020). Improving information security risk analysis by including threat-occurrence predictive models. *Computers & Security*, *88*, p.101609.
[16] McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Pattinson, M., (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151-156.
[17] Thangavelu, M., Krishnaswamy, V. and Sharma, M., (2021). Impact of comprehensive information security awareness and cognitive characteristics on security incident management–an empirical study. *Computers & Security*, *109*, p.102401.
[18] Nazareth, D.L. and Choi, J., 2015. A system dynamics model for information security management. *Information & Management*, *52*(1), 123-134.
[19] Abapour, S., Mohammadi-Ivatloo, B., & Hagh, M. T. (2020). A Bayesian game theoretic based bidding strategy for demand response aggregators in electricity markets. *Sustainable Cities and Society*, 54, 101787.
[20] Dahiya, A., & Gupta, B. B. (2021). A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense. *Future Generation Computer Systems*, 117, 193-204.
[21] Pattinson, M., Parsons, K., Butavicius, M., McCormac, A. and Calic, D., (2016). Assessing information security attitudes: a comparison of two studies. *Information & Computer Security*, *24*(2), 228-240.
[22] Safa, N.S. and Von Solms, R., (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442-451.
[23] Hadlington, L., Binder, J. and Stanulewicz, N., (2021). Exploring role of moral disengagement and counterproductive work behaviours in information security awareness. *Computers in Human Behavior*, *114*, p.106557.
[24] Lye, K.W. and Wing, J.M., (2005). Game strategies in network security. *International Journal of Information Security*, *4*(1), 71-86.
[25] Njilla, L.Y., Pissinou, N. and Makki, K., (2016). Game theoretic modeling of security and trust relationship in cyberspace. *International Journal of Communication Systems*, *29*(9), 1500-1512.