electronics

Article

Research on the Effectiveness of Cyber Security Awareness in ICS Risk Assessment Frameworks

Keyong Wang [1], Xiaoyue Guo [1] and Dequan Yang [2,*]

[1] School of Continuing Education, Beijing Institute of Technology, Beijing 100081, China; wangkeyong@bit.edu.cn (K.W.); guoxiaoyue@bit.edu.cn (X.G.)
[2] Network Information Technology Center, Beijing Institute of Technology, Beijing 100081, China
* Correspondence: yangdequan@bit.edu.cn

Abstract: Assessing security awareness among users is essential for protecting industrial control systems (ICSs) from social engineering attacks. This research aimed to determine the effect of cyber security awareness on the emergency response to cyber security incidents in the ICS. Additionally, this study has adopted a variety of cyber security emergency response process measures and frameworks and comprehensively proposes a new organizational model of cyber security incident response. The corresponding measures are evaluated based on the MP^2DR^2 risk control matrix model to assess their practical value in the evaluation stage. This study found that after adding security awareness measures to response control measures, the influential value ranking of other control measures changed. The practical value of security awareness control measures was given a higher priority than that of other control measures. The research results highlight the importance of cyber security awareness and aim to inspire ICSs to place a higher priority on staff cyber security awareness in relation to cyber security incidents, which can effectively prevent the occurrence of cyber security incidents and make the field of industrial control application agency respond to incidents faster to restore the regular progress of all works.

Keywords: cyber security awareness; industrial control system; incident response; MP^2DR^2 risk control matrix

Citation: Wang, K.; Guo, X.; Yang, D. Research on the Effectiveness of Cyber Security Awareness in ICS Risk Assessment Frameworks. *Electronics* **2022**, *11*, 1659. https://doi.org/10.3390/electronics11101659

Academic Editors: David G. Rosado, Luis Enrique Sánchez Crespo and Manuel A. Serrano

Received: 2 April 2022
Accepted: 20 May 2022
Published: 23 May 2022

1. Introduction

Cyber security incidents have become more expensive, disruptive, and, in many cases, more political in the past decade [1]. Cyber security profoundly impacts all countries' economic and social development worldwide. Cyber security is employed in many industries today, especially in their industrial control systems (ICSs). Cyber security makes data stored in the controls of these industries secure, complete and accessible [2]. Recent attacks and threats indicate that industrial control systems are often attacked. Communication networks and Internet of Things (IoT) increase the vulnerability of industrial control systems (ICSs) to cyberattacks [3]. The IoT ecosystem poses new security challenges that extend beyond traditional data security, and there are no solutions that address all requirements [4]. The industrial world is shifting to the industrial Internet of Things (IIoT), and increasing number of companies have developed a world of 4.0, taking approach to the industry 4.0 paradigm, adopting advanced technologies such as smart sensors, big data analytics and cloud computing. Cyber security issues represent a complex challenge for all companies committing the to industry 4.0 paradigm [5]. In this industrial scenario, staff must be aware of a number of cyber security issues so as to prevent and minimize the occurrence of cyber security incidents [6].

According to the study, 52% of companies report that personals constitute the most significant weakness in cyber security [7]. A malfunctioning of the systems can be caused by various factors: natural disasters, technical weakness and malicious activities by humans [8]. As the number and frequency of cyber attacks designed to take advantage of unsuspecting

personnel are increasing, the significance of the human factor in information security management cannot be understated. Every related party carries the risk of a security vulnerability. Even if a business follows the greatest cyber security practices, its data, customers, or reputation might be compromised [9]. The purpose of one research is to stop all cyber attacks targeted at the aim of exploiting human factors in the information security chain, in order to reduce the risk of information security that happens due to human-related vulnerabilities, there is a critical importance of Cybersecurity awareness with a objective to reduce the risk of human vulnerability [10]. Cyber security awareness is defined as: "The degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organization's data and networks" [11]. Recognizing and mastering the importance of information security in terms of people should be one of the major and lasting goals of an organization's information security policies [12]. However, in the industrial environment, more attention is paid to the critical elements of the industry. Little attention is paid to all aspects of industrial cyber security awareness. Therefore, security awareness is essential to perfect cyber security incident response systems.

To target these challenges, our paper presents the following contributions:

- We adopt a variety of network security emergency response process measures and frameworks, and comprehensively propose a resilient organization that integrates security awareness into the cyber security emergency response process, so as to present a more effective emergency response to cyber security incidents.
- We use a risk control matrix based on MP^2DR^2 to verify the effectiveness of security awareness in cyber security incident response, and confirm that security awareness has a higher priority in corresponding control measures.

The rest of this paper is organized as follows. In Section 2, relevant works of literature are studied and described. In Section 3, we propose a resilient organizational framework. In Section 4, incident response and evaluation methods are presented. Section 5 evaluates the effectiveness of security awareness in several control measures. Additionally, the results are discussed, showing that security awareness is critical to cyber security incident management. Section 6 discusses the limitations of this study and future research. Lastly, in Section 7, the conclusions of this study will be discussed.

2. Related Research

Industrial controls are the primary component of national infrastructure. They control and automate industrial process operations across a wide range of industries, including nuclear, water, oil and gas, and electricity [13]. The importance of cyber security for critical infrastructures is widely recognized in industrial control systems (ICSs) [14]. Cyberattacks are most likely to affect these systems. Unlike IT systems that are replaced regularly, ICSs can operate continuously for up to 20 years. During a long time with their release, the discovery and patch implementation for vulnerabilities give attackers time to discover and exploit vulnerabilities [15]. Network attacks may be launched in different ways despite the use of traditional methods to protect data (such as password protection). For example, a malicious attacker or insider can enter the factory network and change the data log to prevent determining what the attacker did during the attack [16]. Cyberattacks on ICSs can have damaging consequences, including significant social and economic losses [17]. Therefore, cyber security is currently a serious problem for industrial control systems (ICSs).

The ITIL (Information Technology Infrastructure Library) guidance focuses on custom process development, to achieve better approach over time and the results achieved [18]. This approach designed to provide ITIL services is suitable for continuity and availability of services, for example, for higher productivity and for overall productivity [19]. The US National Institute of Standards and Technology (NIST) has offered a 'Computer Security Incident Handling Guide'. The incident response process in this guide is relatively perfect, and its steps include preparation, detection and analysis, containment, eradication, recovery, and post-incident activities [20,21]. ISO/IEC 27035 is an international standard information

security incident management framework that classifies information security incidents from the perspective of threat, which is helpful to manage information security incidents, events, and vulnerabilities [22]. PDCERF is also the international standard process for emergency response: preparation, detection, containment, eradication, recovery, and follow-up [23]. The model can deal with cyber security incidents scientifically, reasonably, and orderly to the maximum extent. However, the standard issue with all these frameworks is that there is no emphasis on the importance and integration of cyber security awareness among personnel.

Although cyber security protection tools are usually well prepared, they cannot completely alleviate network security vulnerabilities. This is closely related to the fact that the weakest link in the cyber security chain is still human error [24,25]. The threat caused by cyber security awareness is considered the second largest cause of incidents, and 51% of respondents said that cyber security affects the security level [26]. Hadlington and Parsons [27] have also shown that numerous employees often neglect to use cyber security technology. Human error in the organization may directly or indirectly lead to the occurrence of major security incidents. As such, it is necessary to protect information security at the individual level against undesirable information security behaviors [28]. Tick et al. [29] pointed out that differences in perceived cyber-related risk and attitudes, as well as differences in behavior can be attributed to the differences in cyber security awareness and cyber security literacy. Kovačević et al. [30] analyzed cyber security awareness in depth, in order to determine how various factors such as cyber security perception, previous cyber security breaches, IT usage, and knowledge may individually or collectively impact cyber security behavior. To prevent or minimize the impact of cyber attacks on business performance, organizations should use regular training as a means to improve the cyber security awareness [31]. When it comes to training, the organizations and educational institutions must begin developing proper training plans [32]. Cyber security training can take two forms—improving understanding of the latest threats and the skill level of security professionals; improving cyber security awareness among non-security professionals and the public [33]. Through the practice and repeated application of better-managed cyber security knowledge, employees can master the cyber security skills necessary to effectively manage and respond to cyber security threats and risks [34]. Some companies have already provided cyber awareness training programs aimed at raising cybercrime awareness among individuals [35]. In addition, LeFebvre [36] examined how student populations are motivated to protect themselves from the threat of cybercrime. Despite efforts to increase information security awareness, research is scant regarding effective information security awareness delivery methods. To this end, Abawajy [10] focused on determining which security awareness delivery method is most successful in providing information security awareness. Their primary research was to propose a cyber security awareness and education framework that would assist in creating a cyber-secure culture among all the users of the internet [37]. In order to accurately reflect the actual behavior of users, Solomon et al. [38] proposed a novel context-based, data-driven, approach for assessing the ISA of users. Brilingaitė et al. [39] provided a proper methodology to optimize the exercises so that every team and each participant, including a non-technical trainee, are adequately evaluated and trained using the allocated resources most effectively. Hart et al. [40] proposed a tabletop game to increase cyber security awareness for people with no technical background working in organizations. Ideally, a program should spend more of its expenses on training employees to deal with the security threats at a lower security level and to reduce more losses at a higher security level [41]. Therefore, it is crucial for industrial control systems to develop a culture of cyber security awareness to positively influence employees' cyber security behavior, which eventually enhances the organization's potential to deal with cyber security threats effectively. Different from the framework mentioned above, we integrate security awareness into an incident response framework to place a higher priority on security awareness in incident response control measures of ICSs, and confirm the effectiveness of security awareness through a risk control matrix.

3. Organizational Framework

This paper builds a flexible cyber security incident response-resilient organization based on the related research. A resilient organization is prepared to deal with the unexpected and able to adapt to current situations. Resilience is an immanent property that must be developed over time [42]. It's a relation between resilience and workplace stress and information security awareness (ISA) and the conclusion that when employees cope with or adapt to job stress, cyber security awareness increases, thus improving resilience of the organization [43]. Generally, small enterprises lack knowledge and resources to address cyber security threats. This is crucial to raise their awareness of cyber security and resilience [44]. Organization must aim to improve employees' security awareness, optimize the cyber emergency response process, and deal with cyber security incidents more wholly and effectively. Table 1 compares the key characteristics of other organization types and resilient organization structures in this study. Functional organization, matrix organization (including weak matrix organization, balanced matrix organization and strong matrix organization) and flexible organization are compared according to the following characteristics, highlighting the advantages of resilient organization in the characteristics of each project: the rights of the project manager, the proportion of staff participating in the project full time, the position of the project manager, technical personnel and management personnel.

Table 1. Impact of organizational structure on projects.

Organization Type / Project Characteristics	Functional Organization	Matrix Organization			Resilience Organization
		Weak Matrix Organization	Balanced Matrix Organization	Strong Matrix Organization	
Rights of project manager	Little	Limited	Little–Moderate	Moderate–Great	Great–Plenipotentiary
The proportion of full-time staff participating in the project	No	0–25%	15–60%	50–95%	85–100%
Position of project manager	Part time	Part time	Full time	Full time	Full time
Technical personnel	Part time	Part time	Part time	Full time	Full time
Management personnel	Part time	Part time	Part time	Full time	Full time

4. Methodology

This section is divided into three parts. In Section 4.1, we propose a new incident response process according to the problems existing in related research and organizational frameworks. Then, in Section 4.2, we briefly describe the work to be performed at each step of the response process and point out that the implementation of the process should be based on the flexibility of situation analysis. Finally, in Section 4.3, we describe in detail the evaluation method of the effectiveness of control measures in the incident response process.

4.1. Propose a Model

In the cyber security response process, cyber security teams aim to detect, analyze, eradicate, and recover from potential cyber security incidents in a timely and cost-effective manner [45]. On the basis of resilient organization as part of an organizational framework, this paper proposes a model with a combination of security awareness and incident response. As a comprehensive work, cyber security incident response not only involves key technologies such as intrusion detection, timely diagnosis, attack isolation, and rapid recovery but also puts forward higher requirements for security awareness management. Hence, in this paper, emergency response is divided into six stages: awareness, preparation, detection, containment, eradication, and recovery.

4.2. Implementation of the Process

The aim of this model was to gain a deeper understanding of the impact of security awareness on the cyber security incident response process. According to information security studies, positive results were demonstrated between intention and behavior [46].

Therefore, this study will highlight the whole model through awareness and use the matrix to give results. The process is as follows:

1. Awareness. The objectives for the first step were to obtain a capability which is referred to as Cyber Situation Awareness (CSA), through training. CSAcan usually be described as a three-phase process: situation recognition, situation comprehension, and situation projection [47]. CSA considers the ability to understand the current situation, potential changes, and consequences.
2. Preparation. There are two tasks in this stage: one is to initialize the snapshot of the cyber information system, and the other is to prepare the emergency response kit.
3. Detection. This part needs to use detection technology combined with the system initialization snapshot generated in the preparation stage to determine whether the system is abnormal; the cause, nature, and impact scope of the incident; and the emergency response scheme.
4. Containment. Control the scope and degree of the attack; control, block, and transfer the security attack through various methods; take targeted security remedial work to contain further deepening and expansion of the attack.
5. Eradication. Based on the containment stage, the technical causes of such security problems are eliminated technically, and the consequences caused by such security problems remedied and eliminated.
6. Recovery. By taking a series of measures to restore the system to the average business state, the system is installed and reinforced in strict accordance with the initialization security policy of the system

Technology is not omnipoten, therefore the best countermeasures are determined on a basis of the analysis of the attack types. In particular, depending on the nature of the attack, on the current state of the system, and the available protection actions, a decision problem needs to be solved in the feedback loop [48]. This model draws upon the literature in information security, incident response, theory of planned behavior, and security awareness to expand and improve overall industrial organization cyber security performance.

4.3. Evaluation

The evaluation of the research adopts the ranking model of security measures based on the MP^2DR^2 risk control matrix proposed by LV J [49]. The following notations in Table 2 are considered here to illustrate the model:

Table 2. Notation.

Notation	Definition
t	threat
ω	weight of threat
a	asset
λ	weight of asset
s	type of asset
c	control measure
x	effective control degree of control measure
X	effectiveness matrix of each control measure counters the threat
R	response control matrix
B	scheme ranking matrix
E	asset effect matrix
H	evaluation matrix of control measures

There are three sets: threat set $T = (t_1, t_2, \cdots, t_n)$, asset set $A = (a_1, a_2, \cdots, a_l)$ and control measure set $C = (c_1, c_2, \cdots, c_l)$. The weights of various threats are $\omega_1, \omega_2, \cdots, \omega_n$, $0 \leq \omega_j \leq 1, j = 1, 2, \cdots, n$,

$$\sum_{j=1}^{n} \omega_j = 1 \tag{1}$$

ω results from risk assessment.

$$\omega_j = cc_j \,/\, \sum_{j=1}^{n} cc_j \tag{2}$$

where cc_j represents the proximity between the risk caused by threat j and the negative ideal solution. The weights of various assets are $\lambda_1, \lambda_2, \cdots, \lambda_l$, $0 \leq \lambda_i \leq 1$, $i = 1, 2, \cdots, l$,

$$\sum_{i=1}^{l} \lambda_i = 1 \tag{3}$$

λ is determined according to the importance of assets. For the s-th asset, the effectiveness matrix of each control measure against the threat is $X = \left[x_{ij}(s)\right]_{l \times n}$; $x_{ij}(s)$ indicates the effective control degree of the s-th asset and the i-th control measure against the j-th threat. The matrix X is composed of six control matrices, including the response control matrix $R(s) = \left[r_{ij}(s)\right]_{m \times n}$. This paper describes the evaluation method of the response control matrix:

$$R(s) = \left[r_{ij}(s)\right]_{m \times n} \begin{array}{c} \\ c_1 \\ c_2 \\ \vdots \\ c_m \end{array} \begin{array}{c} \begin{array}{cccc} t_1 & t_2 & \cdots & t_n \end{array} \\ \begin{bmatrix} r_{11}(s) & r_{12}(s) & \cdots & r_{1n}(s) \\ r_{21}(s) & r_{22}(s) & \cdots & r_{2n}(s) \\ \vdots & \vdots & \vdots & \vdots \\ r_{m1}(s) & r_{m2}(s) & \cdots & r_{mn}(s) \end{bmatrix} \end{array}, s = 1, 2, \cdots, l \tag{4}$$

The decision problem is to rank the effectiveness of response measures according to various assets and threats.

Firstly, the scheme ranking matrix under each threat is determined according to the asset type s:

$$B(s) = \begin{array}{c} Importance \\ 1 \\ 2 \\ \vdots \\ m \end{array} \begin{array}{c} \begin{array}{cccc} t_1 & t_2 & \cdots & t_m \end{array} \\ \begin{bmatrix} b_1^1(s) & b_1^2(s) & \cdots & b_1^n(s) \\ b_2^1(s) & b_2^2(s) & \cdots & b_2^n(s) \\ \vdots & \vdots & \vdots & \vdots \\ b_m^1(s) & b_m^2(s) & \cdots & b_m^n(s) \end{bmatrix} \end{array} \tag{5}$$

In (5), $s = 1, 2, \cdots, l$; $b_1^j(s), b_2^j(s), \cdots, b_m^j(s)$ is the order of the number $1, 2, \cdots, m$. Additionally, it represents the effectiveness ranking of various control measures for each threat. If $b_i^j(s) = k$, this means that the control effectiveness of control measure k on the j-th threat ranks i. For l assets, the ranking value of the effect of control measures on each asset is

$$e_{ij}(s) = \sum_{b_j^k = i} \omega_k \tag{6}$$

The asset effect matrix is as follows:

$$E(s) = \left[e_{ij}(s)\right]_{m \times m} \begin{array}{c} \\ c_1 \\ c_2 \\ c_3 \\ c_4 \end{array} \begin{array}{c} \begin{array}{cccc} Importance\ ranking & 1 & 2 & 3 \quad 4 \end{array} \\ \begin{bmatrix} \sum\limits_{b_1^k(s)=1} \omega_k & \sum\limits_{b_2^k(s)=1} \omega_k & \cdots & \sum\limits_{b_m^k(s)=1} \omega_k \\ \sum\limits_{b_1^k(s)=2} \omega_k & \sum\limits_{b_2^k(s)=2} \omega_k & \cdots & \sum\limits_{b_m^k(s)=2} \omega_k \\ \vdots & \vdots & \vdots & \vdots \\ \sum\limits_{b_1^k(s)=m} \omega_k & \sum\limits_{b_2^k(s)=m} \omega_k & \cdots & \sum\limits_{b_m^k(s)=m} \omega_k \end{bmatrix} \end{array} \tag{7}$$

Considering the importance weight of various assets, the comprehensive effect ranking value is

$$h(ij) = \sum_{s=1}^{l} \lambda_s e_{ij}(s) \tag{8}$$

Then, the evaluation matrix of control measures is:

$$H(s) = \left(h_{ij}\right)_{m\times n} \begin{matrix} \\ c_1 \\ c_2 \\ c_3 \\ c_4 \end{matrix} \begin{matrix} \textit{Importance ranking} \quad 1 \quad\quad 2 \quad\quad 3 \quad\quad 4 \\ \begin{bmatrix} \sum\limits_{s=1}^{l} \lambda_s e_{11}(s) & \sum\limits_{s=1}^{l} \lambda_s e_{12}(s) & \cdots & \sum\limits_{s=1}^{l} \lambda_s e_{1m}(s) \\ \sum\limits_{s=1}^{l} \lambda_s e_{21}(s) & \sum\limits_{s=1}^{l} \lambda_s e_{22}(s) & \cdots & \sum\limits_{s=1}^{l} \lambda_s e_{2m}(s) \\ \vdots & \vdots & \vdots & \vdots \\ \sum\limits_{s=1}^{l} \lambda_s e_{m1}(s) & \sum\limits_{s=1}^{l} \lambda_s e_{m2}(s) & \cdots & \sum\limits_{s=1}^{l} \lambda_s e_{mm}(s) \end{bmatrix} \end{matrix} \tag{9}$$

5. Results and Discussion

This study aims to verify the effectiveness of security awareness in cyber security incident response and its priority in various control measures. Aligning with the MP^{2}DR^2 risk control matrix model, we established the final version of the calculation and made the following assumptions based on the data:

- There are four corresponding control measures—vulnerability assessment (c_1), big data analysis (c_2), emergency response (c_3), and security event processing (c_4)—and they must be sorted to determine priority.
- To simplify the problem, the asset type is set as tangibles (a_1), and data and documents (a_2). The weights of the three assets are $\lambda_1 = \frac{1}{3}, \lambda_2 = 2/3$.
- There are six threats: hardware failure (t_1), physical environment threat (t_2), hacker attack (t_3), malicious code and viruses (t_4), ultra viruses and abuse (t_5), and hacker attacks (t_6); the weights of each threat are $\omega_1 = 3/12$, $\omega_2 = 3/12, \omega_3 = 3/12$, $\omega_4 = 1/12, \omega_5 = 2/12, \omega_6 = 1/12$.

The effectiveness ranking results of control measures are shown in Table 3. The effect matrix of control measures can be calculated according to Equation (7), as shown in Table 4. According to Equation (9), the sequence of the comprehensive effect matrix of control measures can be calculated, as shown in Table 5.

Table 3. Effectiveness ranking of control measures.

Sort	**a_1**				**a_2**			
	1	**2**	**3**	**4**	**1**	**2**	**3**	**4**
t_1	3	4	1	2	4	1	3	2
t_2	3	4	1	2	4	1	3	2
t_3	2	4	3	1	4	3	2	1
t_4	1	2	3	4	1	2	3	4
t_5	2	4	3	1	4	3	2	1
t_6	1	4	2	3	1	2	3	4

Table 4. Effect matrix of control measures.

Sort	**a_1**				**a_2**			
	1	**2**	**3**	**4**	**1**	**2**	**3**	**4**
c_1	1/6	0	1/2	1/3	1/6	1/2	0	1/3
c_2	1/3	1/12	1/12	1/2	0	1/6	1/3	1/2
c_3	1/2	0	5/12	1/12	0	1/3	2/3	0
c_4	0	11/12	0	1/12	5/6	0	0	1/6

Table 5. Comprehensive effect matrix of control measures.

Measure	Sort 1	Sort 2	Sort 3	Sort 4
c_1	0.1667	0.3333	0.1667	0.3333
c_2	0.1111	0.1389	0.2500	0.5000
c_3	0.1667	0.2222	0.5833	0.0278
c_4	0.5556	0.3056	0.0000	0.1389

Threats and assets remain unchanged, and security awareness (c_5) is added to the set of control measures. The effectiveness ranking results of control measures are shown in Table 6. The effect matrix of control measures can be calculated according to Equation (7), as shown in Table 7. According to Equation (9), the sequence of the comprehensive effect matrix of control measures can be calculated, as shown in Table 8.

Table 6. Effectiveness ranking of control measures.

Sort	a_1					a_2				
	1	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**
t_1	3	4	1	5	2	4	1	5	3	2
t_2	3	4	1	5	2	4	1	5	3	2
t_3	2	4	5	3	1	5	4	3	2	1
t_4	1	5	2	3	4	1	5	2	3	4
t_5	2	4	5	3	1	5	4	3	2	1
t_6	5	1	4	2	3	5	1	2	3	4

Table 7. Effect matrix of control measures.

Sort	a_1					a_2				
	1	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**
c_1	1/12	1/12	1/2	0	1/3	1/12	7/12	0	0	1/3
c_2	1/3	0	1/12	1/12	1/2	0	0	1/6	1/3	1/2
c_3	1/2	0	0	5/12	1/12	0	0	1/3	2/3	0
c_4	0	5/6	1/12	0	1/12	1/2	1/3	0	0	1/6
c_5	1/12	1/12	1/3	1/2	0	5/12	1/12	1/2	0	0

Table 8. Comprehensive effect matrix of control measures.

Measure	Sort 1	Sort 2	Sort 3	Sort 4	Sort 5
c_1	0.0833	0.4167	0.1667	0.0000	0.3333
c_2	0.1111	0.0000	0.1389	0.2500	0.5000
c_3	0.1667	0.0000	0.2222	0.5833	0.0278
c_4	0.3333	0.5000	0.0278	0.0000	0.1389
c_5	0.3056	0.0833	0.4444	0.1667	0.0000

After adding the control measure of security awareness, threats of operational errors and process violations (t_2) can be effectively solved, resulting in a new threat set. The weight of each threat changes to $\omega_1 = 3/10$, $\omega_2 = 3/10, \omega_4 = 1/12, \omega_5 = 2/10, \omega_6 = 1/10$. The results obtained according to the above calculation process are shown in Tables 9–11.

To facilitate analysis of the change in effective value after adding security awareness, data in Tables 5, 8 and 11 are presented in broken line charts, as shown in Figures 1–3.

The abscissa indicates the priority of each control measure, and the ordinate represents the effective value of each control measure. Figure 1 shows the change in the effective value of the priority of the original four control measures in the incident response. Figure 2 shows the effective value of each control measure ranked in terms of priority after adding the control measure of security awareness. Figure 3 shows the change in threat set after adding security awareness to the control measures. After recalculating the data of the new threat

set, the effective value of each control measure in priority ranking changes. Comparing the three figures shows that security awareness impacts the incident response of cyber security incidents. As shown in Figure 2, among all the control measures ranked first, the effective value of security awareness is similar to that of security event processing. Further, the addition of security awareness to the original control measures has a significant regulatory effect on the effectiveness ranking for the sequence of control measures. Therefore, security awareness is necessary for the cyber security incident response process.

Table 9. Effectiveness ranking of control measures.

Sort	a_1					a_2				
	1	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**
t_1	3	4	1	5	2	4	1	5	3	2
t_2	3	4	1	5	2	4	1	5	3	2
t_4	1	5	2	3	4	1	5	2	3	4
t_5	2	4	5	3	1	5	4	3	2	1
t_6	5	1	4	2	3	5	1	2	3	4

Table 10. Effect matrix of control measures.

Sort	a_1					a_2				
	1	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**
c_1	1/10	1/10	3/5	0	1/5	1/10	7/10	0	0	1/5
c_2	1/5	0	1/10	1/10	3/5	0	0	1/5	1/5	3/5
c_3	3/5	0	0	3/10	1/10	0	0	1/5	4/5	0
c_4	0	4/5	1/10	0	1/10	3/5	1/5	0	0	1/5
c_5	1/10	1/10	1/5	3/5	0	3/10	1/10	3/5	0	0

Table 11. Comprehensive effect matrix of control measures.

Measure	Sort 1	Sort 2	Sort 3	Sort 4	Sort 5
c_1	0.1000	0.5000	0.2000	0.0000	0.2000
c_2	0.0667	0.0000	0.1667	0.1667	0.6000
c_3	0.2000	0.0000	0.1333	0.6333	0.0333
c_4	0.4000	0.4000	0.0333	0.0000	0.1667
c_5	0.2333	0.1000	0.4667	0.2000	0.0000

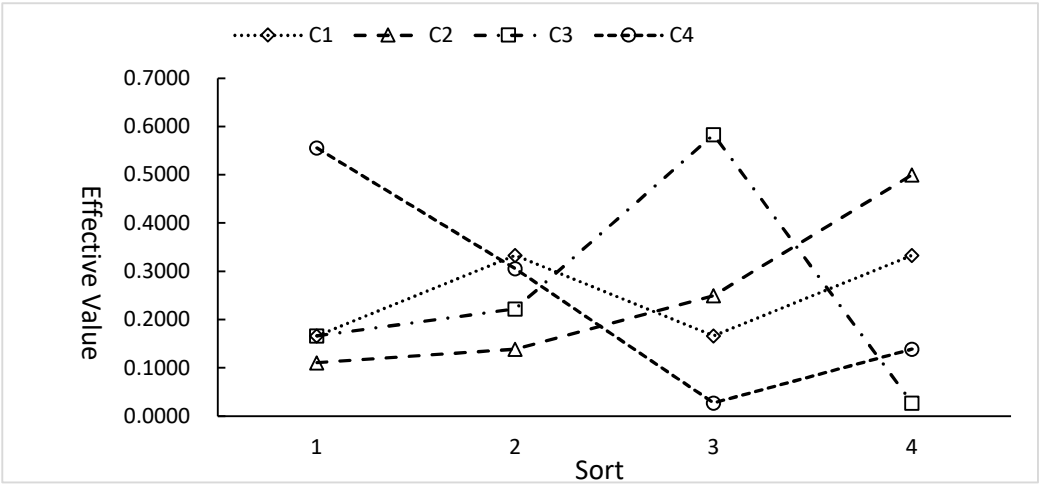

Figure 1. Effect change in control measures.

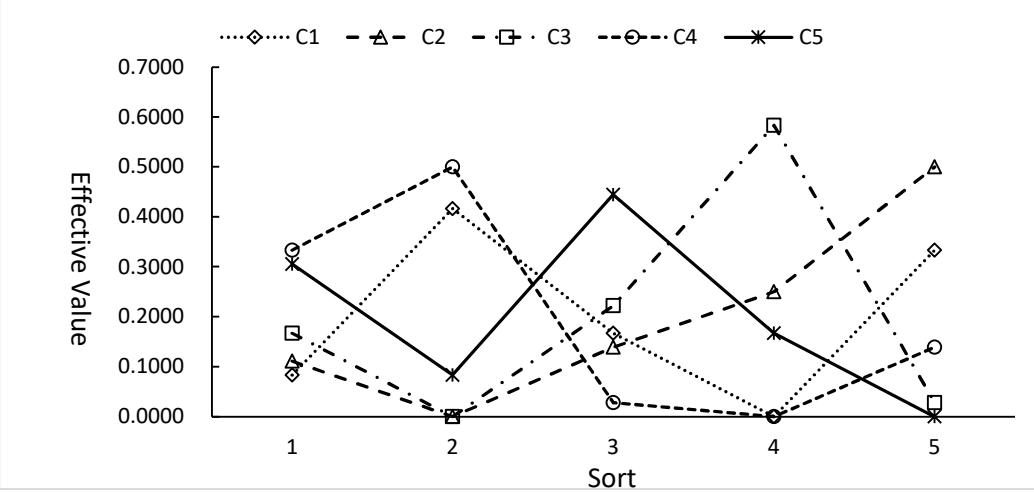

Figure 2. Effect change in control measures.

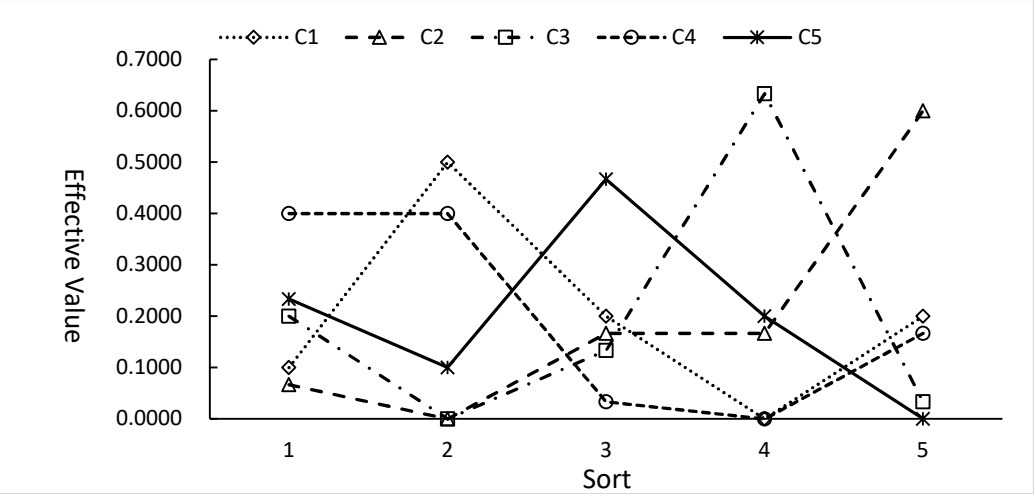

Figure 3. Effect change in control measures.

6. Limitations and Future Research

This study has several limitations, opening avenues for future research to explore interesting areas. First, this model was developed using thematic interpretations that were part of a scoping review. The model is a result of the authors' ideological frame of reference and understanding of information security awareness. To reduce this bias, future research may want to pursue a more structured approach to the literature review, or go further and perform a meta-analysis of information security awareness.

Second, our method is aimed at security awareness among employees during incident handling and response and does not include security awareness among personnel outside of the organization being evaluated. Therefore, our findings are limited because we cannot point out the impact of external security awareness on industrial control systems. It is for this reason that we advocate future research expanding security awareness in terms of the severity of industrial control system cyber security incidents to a wider range and evaluating security awareness beyond that of the organization to determine its effects, so as to better protect the industrial control system in cyber security incidents.

7. Conclusions

Cyber security incident response is essential to ensure business continuity. There are various approaches to incident management, and different approaches have multiple limitations. Cyber security risks are inevitable, and it is far from sufficient to build cyberspace

only from the perspective of security technology. The existence of network vulnerability is sometimes due to the lack of cyber security awareness among some computer users, technology developers, and system managers. Vulnerabilities caused by a lack of security awareness in industrial control systems, in particular, pose severe risks to critical infrastructure. Increasing employees' level of knowledge on possible security threats, system vulnerabilities, and security risks in industrial control systems, and allowing them to be responsible in terms of information security and aware of potential cyber attacks, will ensure that the information, systems, and networks they interact with are well protected. We should recognize the substantial effectiveness of cyber security and even citizens' national cyber security awareness.

The current research can be extended by considering personal, social, and cultural characteristics that are indicative of the level of susceptibility that one may exhibit towards certain attack types [50]. In terms of cyber security awareness education and training, a recent study proposed a cyber security competency model that integrates learning theories (cognitive, affective, and psychomotor), learning continuum hierarchy (awareness and training), and cyber security domain knowledge [51], which are some rewarding future research directions of the current study. By considering highly interactive digital and face-to-face cyber security training, one can extend the current study [52]. Moreover, Izosimov et al. [53] state that security awareness among users and developers is the foundation to deployment of an interconnected system of systems, and provide recommendations for steps forward, highlighting the roles of people, organizations and authorities. Thus, this research can be extended by considering different forms of cyber security awareness projects for different groups, encouraging and mobilizing the participation of the whole of society, establishing and improving the "top-down" three-dimensional network security education strategy, and supporting the formation and promotion of national cyber security awareness through the systematization of implementation subjects.

Author Contributions: K.W., conceptualization, methodology, data curation, writing—original draft, and writing—review and editing. X.G., conceptualization, methodology, and writing—review and editing. D.Y., methodology, validation, investigation, writing—review and editing, supervision, and funding acquisition. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Hainan Provincial National Science Foundation of China (621MS0789).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Cavelty, M.D.; Wenger, A. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemp. Secur. Policy* **2019**, *41*, 5–32. [CrossRef]
2. Babbar, G.; Bhushan, B. Framework and Methodological Solutions for Cyber Security in Industry 4.0. 2020. In Proceedings of the International Conference on Innovative Computing & Communications (ICICC), New Delhi, India, 15 May 2020. [CrossRef]
3. Abdulrahman Al-Abassi, H.; Karimipour, A.; Dehghantanha, A.; Parizi, R. An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System. *IEEE Access* **2020**, *8*, 83965–83973. [CrossRef]
4. Chmiel, M.; Korona, M.; Kozioł, F.; Szczypiorski, K.; Rawski, M. Discussion on IoT Security Recommendations against the State-of-the-Art Solutions. *Electronics* **2021**, *10*, 1814. [CrossRef]
5. Lezzi, M.; Lazoi, M.; Corallo, A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Comput. Ind.* **2018**, *103*, 97–110. [CrossRef]
6. Corallo, A.; Lazoi, M.; Lezzi, M.; Luperto, A. Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Comput. Ind.* **2022**, *137*, 103614. [CrossRef]
7. Kaspersky Lab. The Human Factor in IT Security: How Employees Are Making Businesses Vulnerable from Within. 2018. Available online: https://www.kaspersky.com/blog/the-human-factor-in-it-security/ (accessed on 1 December 2021).
8. Bruzgiene, R.; Jurgilas, K. Securing Remote Access to Information Systems of Critical Infrastructure Using Two-Factor Authentication. *Electronics* **2021**, *10*, 1819. [CrossRef]
9. Taherdoost, H. A Review on Risk Management in Information Systems: Risk Policy, Control and Fraud Detection. *Electronics* **2021**, *10*, 3065. [CrossRef]
10. Abawajy, J. User preference of cyber security awareness delivery methods. *Behav. Inf. Technol.* **2014**, *33*, 236–247. [CrossRef]

11. Shaw, R.S.; Chen, C.C.; Harris, A.L.; Huang, H.J. The impact of information richness on information security awareness training effectiveness. *Comput. Educ.* **2009**, *52*, 92–100. [CrossRef]
12. Hassanzadeh, M.; Jahangiri, N.; Brewster, B. A Conceptual Framework for Information Security Awareness, Assessment, and Training. In *Emerging Trends in ICT Security*; Elsevier: Amsterdam, The Netherlands, 2014; Chapter 6; pp. 99–110. [CrossRef]
13. Green, B.; Krotofil, M.; Abbasi, A. On the significance of process comprehension for conducting targeted ICS attacks. In Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy, Co-Located with CCS 2017, Dallas, TX, USA, 3 November 2017; pp. 57–68.
14. Kobara, K. Cyber Physical Security for Industrial Control Systems and IoT. *IEICE Trans. Inf. Syst.* **2016**, *99*, 787–795. [CrossRef]
15. Marnerides, A.K.; Giotsas, V.; Mursch, T. Identifying infected energy systems in the wild. In Proceedings of the 10th ACM International Conference on Future Energy Systems, Phoenix, AZ, USA, 25–28 June 2019; pp. 263–267.
16. Van Vliet, P.; Kechadi, M.-T.; Le-Khac, N.-A. Forensics in industrial control system: A case study. In *Security of Industrial Control Systems and Cyber Physical Systems*; Springer: Cham, Switzerland, 2015; pp. 147–156.
17. Zhou, C.; Hu, B.; Shi, Y.; Tian, Y.U.; Li, X.; Zhao, Y. A Unified Architectural Approach for Cyberattack-Resilient Industrial Control Systems. *Proc. IEEE* **2021**, *109*, 517–541. [CrossRef]
18. Cusick, J.J.; Ma, G. Creating an ITIL Inspired Incident Management Approach: Roots, Responses, and Results. In *IFIP/IEEE BDIM International Workshop on Business Driven IT Management*; IEEE: Piscataway, NJ, USA, 2010.
19. Shinde, N.; Kulkarni, P. Cyber incident response and planning: A flexible approach. *Comput. Fraud. Secur. Issues* **2021**, *1*, 14–19. [CrossRef]
20. Cichonski, P.; Millar, T.; Grance, T.; Scarfone, K. *Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology*; US Department of Commerce, Technology Administration, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2012.
21. Mukundhan, H. A Business-integrated Approach to Incident Response. *ISACA J.* **2015**, *6*, 42–46.
22. Hartanto, R.; Nugroho, L.E. Perancangan sistem manajamen insiden keamanan informasi berdasarkan sni iso/iec 27035 di instansi pemerintah. *J. Teknol. Technosci.* **2020**, *13*, 1–10.
23. De Muynck, J.; Portesi, S. *Strategies for Incident Response and Cyber Crisis Cooperation*; ENISA: Heraklion, Greece, 2016.
24. Parsons, K.; McCormac, A.; Butavicius, M.; Pattinson, M.; Jerram, C. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Comput. Secur.* **2014**, *42*, 165–176. [CrossRef]
25. Anwar, M.; He, W.; Ash, I.; Yuan, X.; Li, L.; Xu, L. Gender difference and employees' cybersecurity behaviors. *Comput. Hum. Behav.* **2017**, *69*, 437–443. [CrossRef]
26. Alghamdi, M.I. Determining the impact of cyber security awareness on employee behavior: A case of Saudi Arabia. *Mater. Today Proc.* **2021**. [CrossRef]
27. Hadlington, L.; Parsons, K. Can cyberloafing and Internet addiction affect organizational information security? *Cyberpsychology Behav. Soc. Netw.* **2017**, *20*, 567–571. [CrossRef]
28. Khando, K.; Gao, S.; Islam, S.M.; Salman, A. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Comput. Secur.* **2021**, *106*, 102267. [CrossRef]
29. Tick, A.; Cranfield, D.J.; Venter, I.M.; Renaud, K.V.; Blignaut, R.J. Comparing Three Countries' Higher Education Students' Cyber Related Perceptions and Behaviours during COVID-19. *Electronics* **2021**, *10*, 2865. [CrossRef]
30. Kovačević, A.; Putnik, N.; Tošković, O. Factors Related to Cyber Security Behavior. *IEEE Access* **2020**, *8*, 125140–125148. [CrossRef]
31. He, W.; Ash, I.; Anwar, M.; Li, L.; Yuan, X.; Xu, L.; Tian, X. Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *J. Intellect. Cap.* **2020**, *21*, 203–213. [CrossRef]
32. Yeoh, W.; Huang, H.; Lee, W.S.; Al Jafari, F.; Mansson, R. Simulated Phishing Attack and Embedded Training Campaign. *J. Comput. Inf. Syst.* **2021**, 1–20. [CrossRef]
33. Yamin, M.M.; Katt, B.; Gkioulos, V. Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. *Comput. Secur.* **2020**, *88*, 101636. [CrossRef]
34. Baets, W.R.; Linden, G. *Virtual Corporate Universities*; Springer: Boston, MA, USA, 2003.
35. Dodge, R.C., Jr.; Carver, C.; Ferguson, A.J. Phishing for user security awareness. *Comput. Secur.* **2007**, *26*, 73–80. [CrossRef]
36. LeFebvre, R. The Human Element in Cyber Security: A Study on Student Motivation to Act. In Proceedings of the 2012 Information Security Curriculum Development Conference, Kennesaw, GA, USA, 12–13 October 2012.
37. Kortjan, N.; von Solms, R. A Conceptual Framework for Cyber-security Awareness and Education in SA. *S. Afr. Comput. J.* **2014**, *52*, 29–41. [CrossRef]
38. Solomon, A.; Michaelshvili, M.; Bitton, R.; Shapira, B.; Rokach, L.; Puzis, R.; Shabtai, A. Contextual security awareness: A context-based approach for assessing the security awareness of users. *Knowl. Based Syst.* **2022**, *246*, 108709. [CrossRef]
39. Brilingaitė, A.; Bukauskas, L.; Juozapavičius, A. A Framework for Competence Development and Assessment in Hybrid Cybersecurity Exercises. *Comput. Secur.* **2020**, *88*, 101607. [CrossRef]
40. Hart, S.; Margheri, A.; Paci, F.; Sassone, V. Riskio: A Serious Game for Cyber Security Awareness and Education. *Comput. Secur.* **2020**, *95*, 101827. [CrossRef]
41. Zhang, Z.J.; He, W.; Li, W.; Abdous, M.H. Cybersecurity Awareness Training Programs: A Cost-benefit Analysis Framework. *Ind. Manag. Data Syst.* **2021**, *121*, 613–636. [CrossRef]

42. Bartnes, M.; Moe, N.B.; Heegaard, P.E. The future of information security incident management training: A case study of electrical power companies. *Comput. Secur.* **2016**, *61*, 32–45. [CrossRef]
43. McCormac, A.; Calic, D.; Parsons, K.; Butavicius, M.; Pattinson, M.; Lillie, M. The effect of resilience and job stress on information security awareness. *Inf. Comput. Secur.* **2018**, *26*, 277–289. [CrossRef]
44. Van Haastrecht, M.; Golpur, G.; Tzismadia, G.; Kab, R.; Priboi, C.; David, D.; Răcătăian, A.; Baumgartner, L.; Fricker, S.; Ruiz, J.F.; et al. A Shared Cyber Threat Intelligence Solution for SMEs. *Electronics* **2021**, *10*, 2913. [CrossRef]
45. Cichonski, P.; Mllar, T.; Grance, T. Computer Security Incident Handling Guide. *Nist Spec. Publ.* **2012**, *800*, 1–147.
46. Teoh, A.A.; Binti, N.; Ahmad, M.; Jhanjhi, N.; Alzain, M.A.; Masud, M. Organizational Data Breach: Building Conscious Care Behavior in Incident Response. *Comput. Syst. Sci. Eng.* **2022**, *40*, 505–515. [CrossRef]
47. Barford, P.; Dacier, M.; Dietterich, T.G.; Fredrikson, M.; Giffin, J.; Jajodia, S.; Jha, S.; Li, J.; Liu, P.; Ning, P.; et al. Cyber SA: Situational Awareness for Cyber Defense. In *Cyber Situational Awareness*; Springer: Boston, MA, USA, 2010; pp. 3–13.
48. Delaval, G.; Hore, A.; Mocanu, S.; Muller, L.; Rutten, E. Discrete Control of Response for Cybersecurity in Industrial Control. *IFAC-PapersOnLine* **2020**, *53*, 1747–1754. [CrossRef]
49. Lv, J. *Information Security Risk Management Method and Application*; Intellectual Property Publishing House: Beijing, China, 2010.
50. Pollini, A.; Callari, T.C.; Tedeschi, A.; Ruscio, D.; Save, L.; Chiarugi, F.; Guerri, D. Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach. *Cogn. Technol. Work* **2021**, *24*, 371–390. [CrossRef]
51. Yaokumah, W. Cyber Security Competency Model Based on Learning Theories and Learning Continuum Hierarchy. In *Research Anthology on Advancements in Cybersecurity Education*; IGI Global: Hershey, PA, USA, 2022; pp. 139–156.
52. Nweke, L.O.; Bokolo, A.J.; Mba, G.; Nwigwe, E. Investigating the Effectiveness of a HyFlex Cyber Security Training in A Developing Country: A Case Study. *Educ. Inf. Technol.* **2022**. [CrossRef]
53. Izosimov, V.; Törngren, M. Security Awareness in the Internet of Everything. In *Research Anthology on Advancements in Cybersecurity Education*; IGI Global: Hershey, PA, USA, 2022.