applied sciences

MDPI

Article

Exploring the Relationship between Internal Information Security, Response Cost, and Security Intention in Container Shipping

Hsin-Wei Wang [1], Szu-Yu Kuo [2] and Liang-Bi Chen [3,*]

[1] Department of Business Computing, National Kaohsiung University of Science and Technology, Kaohsiung 811213, Taiwan; shinwe@nkust.edu.tw
[2] Department of Shipping and Transportation Management, National Penghu University of Science and Technology, Penghu 880011, Taiwan; tykuo@pie.com.tw
[3] Department of Computer Science and Information Engineering, National Penghu University of Science and Technology, Penghu 880011, Taiwan
* Correspondence: liangbi.chen@gmail.com; Tel.: +886-6-926-4115 (ext. 3505)

Abstract: This study empirically investigates the influence of information security marketing and response cost on employees' information security intention in the container shipping industry. Survey data were collected from 285 respondents in Taiwan. Exploratory factor analysis was employed to identify all the measures to be summarized in a relative set. Confirmatory factor analysis was utilized to ensure every measure's construct's convergent and discriminant validity. Structural equation modeling was carried out to the proposed model in this article. The results indicate that organizational information security marketing has a positive impact on information security intention. Furthermore, this study conducted hierarchical regression to examine the moderating effects of information security awareness and information security climate. In particular, information security awareness significantly influenced the relationships between organizational information security marketing, response cost, and information security intention. Moreover, information security climate moderated the relationship between response cost and information security intention. This article concludes by discussing these theoretical and practical findings and implications.

Keywords: information security; response cost; information security intention; information security awareness; information security climate

Citation: Wang, H.-W.; Kuo, S.-Y.; Chen, L.-B. Exploring the Relationship between Internal Information Security, Response Cost, and Security Intention in Container Shipping. *Appl. Sci.* **2021**, *11*, 2609. https://doi.org/10.3390/app11062609

Academic Editor: Ugo Vaccaro

Received: 2 February 2021
Accepted: 11 March 2021
Published: 15 March 2021

1. Introduction

With the increasing circulation of complex information bringing more significant benefits to organizations, information security is of utmost concern in business operations. Information systems with premium designs are beneficial for efficient business operations in swiftly changing business environments. Still, they are relatively more vulnerable to information security threats, such as unauthorized use, improper disclosure and use of information, information destruction, and password theft or destruction. Security threats have followed the development pace in information and technology systems, threatening serious irreparable business losses. Worldwide reports have indicated that almost every industry has addressed information security issues in response to a wide range of threats and requirements. Their expected cost will reach a compounded annual growth rate of 9.6% between 2016 and 2021. In 2017, the world's total expenditures for security products and services reached USD83.5 billion, increasing by 10.3% over 2016 [1]. The Global State of Information Security Survey investigated 9500 executives in 122 countries in 2017, the findings of which reported a total loss of approximately USD578 billion in security incidents, a 13% increase from 2016 [2]. While total losses continue to increase, a key solution has still not been found.

The container shipping industry is critical to international trade and the global economy [3]. More than 80% of global trade relies on transiting merchandise by sea and land transportation [4]. Once information systems have been attacked, it causes uncalculated losses for the shipping industry and impacts many related industries. In 2017, the information system of the largest container shipping company, the A.P. Moller-Maersk Group, was attacked by ransomware, triggering a significant loss of about USD 200 to 300 million [5]. Moreover, another logistics leader, FedEx, also faced exorbitant losses of USD 300 million in September 2017, after the company was attacked by a ransomware blitz [5]. Maintaining an impregnable information system that protects databases is considered a serious challenge. However, most loopholes in information security result from human error caused by poor user behavior and security cognition [6]. According to an investigation by the International Data Group (IDG) [2], 48% of those surveyed did not have a staff security awareness training scheme, and 54% of the companies did not have an incident information security response mechanism. Information security awareness training for employees via marketing management helps fight various security threats, and proper information security intentions and behaviors are a focus of the shipping industry.

The main challenge in dealing with information security is developing and using effective procedures and responsiveness. Marketing is popularly used in organizational management, which is defined as the social and managerial processes used to meet individuals' and organizations' needs by way of creating and exchanging value with others [7]. Marketing can be categorized into external marketing and internal marketing [8]. External marketing is the process by which firms produce value for customers and establish a good relationship with customers by capturing value to keep customers returning [6]. Internal marketing, or treating employees like customers [9], satisfies employees' needs and attitudes, positively affecting managerial outcomes [10,11]. According to this internal marketing concept, successful information security marketing in organizations promotes employees' knowledge and skills and helps them sustain high-quality information security procedures in the workplace.

A workplace climate is a common perception of the work environment, including practices and procedures, that employees identify with [12]. Because other staff members can easily influence employees' behaviors and work attitudes, a positive workplace climate is critical in an organization. An organization's information security climate refers to its information security work practices and procedures that impact employees [13]. Luria and Yagil [14] found that the organizational workplace climate can improve relationships between employees' attitudes in achieving the organization's targets. An organization should therefore be concerned about creating an information security climate that enhances information security intention.

Information security awareness plays a crucial role in improving employees' information security intentions and behaviors [15]. Organizations' internal marketing transfers this awareness to employees. The huge potential impact of information security vulnerabilities on information security includes device control (e.g., personal computers, USBs, and other devices), Internetwork (e.g., webmail, communication messaging, and network hardware), network monitoring (e.g., HTTP, FTP, and SMTP), document security (e.g., encrypted document and file access), and security management (e.g., password management) [6]. Information security awareness is considered a necessary application in information security to ensure that information security is increasingly valued [13].

In conducting information security marketing for employees, response cost is inevitable. Response cost is defined as the policies that an organization uses to address certain information security types to improve individuals' information security intentions and behaviors [16]. If an organization decides to host a training program, purchase assets or software, or add any security equipment related to information security, it needs to budget for those activities in terms of time cost.

One research gap in the literature is marketing management's impact on employees' information security intention. Typically, marketing management is often applied in

advertising, sales strategies, market searches, customer trends and relationships, social networks, a service or product's position, etc. These efforts are related to outside or external marketing activities, in which firms approach their target customers and gain sales revenue [17,18]. However, research on inside marketing management is very rare, but it is also constructive in the management field. Marketing management is a value to be employed within an organization, and the current study employed it to examine employees' security intentions, thus filling the research gap.

It is important to understand how organizations promote and train staff on information security processes and how they affect other information security variables. Hence, this study's major goal was to determine the interrelationships between various variables in the container shipping context and how these different variables are established in different hierarchically structured levels. This study empirically traced the links between information security marketing, information security climate, information security awareness, and response cost for insights into how these variables affect employees' information security intentions and behaviors in the container shipping industry. The contribution is not only to theoretical work but is also dedicated to the practical implications. It aims to understand how to decrease response cost and increase employees' security intention.

Prior studies have demonstrated different approaches such as stochastic, biologically inspired, game theory, genetic algorithms, community detection, and online social networks [19]. Chakraborty et al. [20] employed the FORGE system to analyze the problem of cyber deception and found that FORGE generates highly believable fakes. Unlike other works, this study employed the possible factors by hierarchical regression, SEM (structural equation modeling), and Process [21] to examine their relationship in a further investigation of information security.

Finally, while prior studies have found a direct relationship between awareness and climate and intention and behavior [22–24], further moderating effects are yet to be tested. The contribution of the findings on these interactions in the current study will help fill this research gap. Such moderating effects can eventually lead to finding the key to employees' security intention. The current study includes the variables of awareness and climate as the moderators in the mediation model, the theoretical outcomes of which will contribute to prior research in this area.

Studies on the relationship between marketing management, awareness, cost, and climate with information security issues still lacking to the best of our knowledge. The contribution of the findings on these interactions in the current study will help fill this research gap. The purpose of this paper is to report on an investigation of an information security issue by examining the relationship and moderating effects.

This paper is organized as follows. The research motivation and introduction are presented in Section 1. Next, the theoretical background of information security marketing and the research hypotheses are presented in Section 2. Section 3 discussing the study's methodology, including the samples, the conceptual model, and data analyses. The results of the research hypotheses will be presented in Section 4. Finally, this paper will conclude with a discussion of the implications and limitations of the study and future research opportunities in Section 5.

2. Theoretical Model and Hypotheses

2.1. Conceptual Basis of Information Security Marketing

Marketing management is commonly divided into two types: external marketing and internal marketing. External marketing is the act or business of promoting and selling services or products to potential customers (i.e., the major target group) via market research and advertising. Internal marketing is an ongoing process of motivating, training, and promoting all management staff to consistently achieve satisfactory organizational goals [25,26] by attracting, developing, motivating, and retaining qualified employees (i.e., the main target group) and providing jobs that satisfy their requests [27]. Internal marketing

is a management philosophy that enables employees to obtain a broader understanding of an organization's needs and achieves the organization's targets.

Marketing is an approach or plan to conquer organizational resistance to change and coordinate, motivate, and integrate employees in effectively implementing business and functional strategies [11]. A growing number of studies have evaluated the importance of internal marketing [28–30]. Chen and Lin [28] investigated how internal marketing quality affected employee loyalty in the medical industry and found six key dimensions: work support, organizational atmosphere, organizational communication, educational training, motivation, and empowerment. Chen and Wu [29] examined the impact of internal marketing on relationship management in the lodging industry. They found five dimensions: education and training, managers' support, internal communication, personnel management, and external activities. In the current study, we chose to implement marketing management to extend corporate information security marketing (ISM) beyond the models used in previous studies to clearly understand how ISM influences employees' information security intention (ISI).

2.2. Information Security Marketing and Information Security Intention

Intention is the concept of having a scheme to accomplish a particular purpose [15]. Information security intention can be described as a specific employee's specific willing behavior related to the organization's information security. Internal marketing involves facets of security that can effectively influence behavioral intention through training, rewards, socialization, participatory decision-making, participation, and communication formalization [31]. The implementation of internal marketing is often seen as a set of activities designed to optimize internal processes within the organization [32], and ISM enhances employees' ISI. ISM is envisioned as a behavioral instrumental approach, similar to an internal-directed marketing strategy that focuses on meeting employees' needs and improving their security-related intentions [10]. This study was mainly in line with this view because ISM influences employees' ISI to protect their organization's information assets, which is the basis for the following hypothesis:

Hypothesis 1. *ISM is positively related to ISI in the container shipping industry.*

2.3. Information Security Marketing, and Response Cost and Information Security Intention

Response cost (RSC) refers to the perceived personal efforts and/or the external or inherent individual's cost of performing the proposed expected behavioral intention [33]. This paper will argue that RSC is a critical factor in assessing an organization's potential expenses when organizations use cost to obtain employees' information security intention. RSC is the extent of the cost that can be incurred in terms of time, effort, and convenience in complying with ISI [34]. In the resource-based view (RBV) theory, when organizations exhibit strong marketing management, employees acquire more significant support, training, and rewards and expend less RSC in obtaining ISI [28,29]. It is reasonable to infer that more effective marketing management helps reduce individuals' RSC in realizing an information security plan.

RSC is related to the cost of implementing the proposed protective information security [16]. In the information security intention context, several studies [16,23,35,36] have reported RSC and ISI's effects. Hanus and Wu [16] surveyed 229 students in a business college at a U.S. university, and the results indicated that RSC harmed ISI as student effort related to information security intention incurred a high response cost (e.g., the time required to implement information security measures) to realize their ISI. Reference [35] examined 274 employees working in various industries in Finland to understand the relationship between RSC and ISI and found that complying with information security intention was time-consuming, took up more work time, and made the work more difficult and inconvenient. From these results, the current study hypothesized the following:

Hypothesis 2. *ISM is negatively related to RSC in the container shipping industry.*

Hypothesis 3. *RSC is negatively related to ISI in the container shipping industry.*

2.4. The Moderating Effect of Information Security Awareness

Information security awareness (ISA) is defined as employees' overall understanding of potential information security-related issues and possible consequences and understanding what steps should be taken to address these issues [37]. ISA is the degree of users' protection of information systems, establishing security and protection mechanisms to ensure unpublished data sets or information [38]. When individuals or organizations encounter serious threats and loss of effectiveness in their protection systems, increased awareness of information security can alleviate system abuse or inadequate information security cognition. Marketing management can spread security notions to employees by training, communication, rewards, and participation, which can enrich employees' ISA [31]. In other words, once employees have more incentives, understanding, and direction to learn and follow their company's security instructions, they will have a higher sense of the importance of information security.

ISA is a necessary component that effectively impacts users' ISI. Connolly et al. [37] presented new insights into individuals' security behaviors in a study involving 20 organizations from the U.S. and Ireland, which found that when employees had higher information security awareness, it led to higher security behaviors. ISA was essential in managing illicit security behaviors and intentions in these organizations. Chen et al. [23] investigated how ISA affected individuals' ISI in a study in the Northwest U.S. that included 231 samples working at a university and found that security-aware employees were familiar with their security practices and guides, and through ISA, their ISI improved. Cultivating information security awareness can enhance employees' organizational security intentions and behaviors [24]. To test the moderating effects of ISA, the current study hypothesized the following:

Hypothesis 4. *ISA positively moderates the relationship between ISM and ISI in the container shipping industry; the positive relationship is stronger when ISA is perceived to be higher than lower.*

Hypothesis 5. *ISA positively moderates the relationship between ISM and RSC in the container shipping industry; the negative relationship is weaker when ISA is perceived to be higher than lower.*

2.5. The Moderating Effect of Information Security Climate

The workplace climate can provide researchers the potential level of information security within an organization, and this possible level directly affects employees' behaviors and intentions. The workplace environment is characterized by the working methods and procedures that organize employees' consensus and perceptions that they can identify and follow [12]. Goo et al. [39] stated that the organizational climate is a perception of social construction. Employees can share all aspects of the organizational environment; that is to say, the perceptions of certain aspects of role behavior are supported in the organization. An information security climate (ISC) is the security conceptions of an organization's employees that enhance their workplace security practices to avoid information security problems [22]. ISC can influence an individual's perceptions within an organization and help employees build an information security environment through a common consensus among groups. The organizational climate can also affect employees through cultivating internal marketing. ISM can reduce an unsafe organizational climate, enhance work attitudes, and increase information security intention. A firm can achieve more effective marketing management with a robust information security climate that catches employees' attention and affects their thoughts and behaviors.

In the security climate model [39], ISC is an antecedent of individuals' motivations for and notions of security and their ISI regarding security compliance. Accordingly, a fundamental assumption of ISC research is the relationship between ISA and ISI. Chen et al. [22]

evaluated 140 employees from two intensive information technology organizations in Singapore and found that the information security climate helped improve employees' information security behaviors and strengthened ISI and participation. Goo et al. [39] surveyed 200 information technology users in Korea and found that a strong ISC was an adequate alternative to improve employees' ISI and that ISC helped establish employees' affective and normative commitments, which positively affected their compliance with ISI. These findings led to the following hypotheses:

Hypothesis 6. *ISC positively moderates the relationship between RSC and ISI in the container shipping industry; the negative relationship is weaker when ISC is perceived to be higher than lower.*

Hypothesis 7. *ISC positively moderates the relationship between ISM and ISI in the container shipping industry; the positive relationship is stronger when ISC is perceived to be higher than lower.*

Taken together, these advanced relationships suggest that ISA and ISC moderate the mediating effects of RSC on the relationship between ISM and ISI. Another critical issue in this study was determining how ISI was affected by the moderators ISA and ISC. A moderated mediation model, therefore, was suitable for determining the effects of ISI efforts in the container shipping industry to acquire a high ISI, which led to the following hypothesis:

Hypothesis 8. *There is a moderated mediation model for ISI in the container shipping industry wherein ISA and ISC moderate the mediating effect of RSC between IMC and ISI.*

In sum, by promoting the notions of information security marketing and information security intention from the vantage point of response cost, this study proposed an integrative and moderated mediation model for seven hypotheses (see Figure 1). The model's transaction value for container shipping firms is expected to extend their information security management in considering response cost as a mediator, with enhanced security awareness and information security climate as the two moderators.

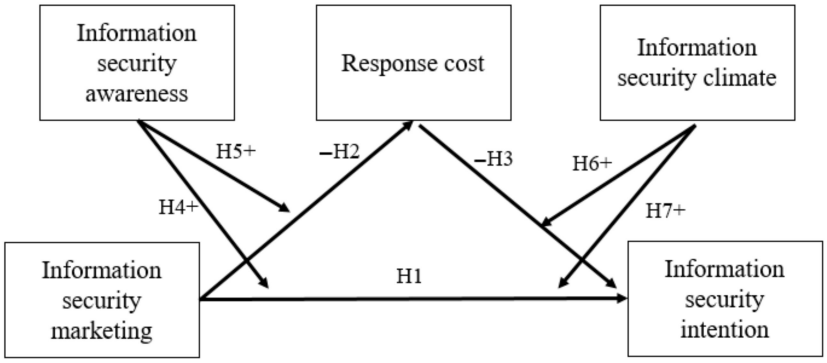

Figure 1. Research conceptual model.

3. Methodology

3.1. Sample Selection and Data Collection

Data collection was drawn from container shipping companies, container shipping agencies, and an ocean freight forwarder in Taiwan. The Directors of the National Association of Shipping Companies and Agencies were selected as the survey population. This survey was conducted by mail. A total of 500 questionnaires were sent to employees who had a position of manager or above. Every company received two survey questionnaires on average. The questionnaires were sent to the potential participants on 8 January 2020; 188 valid responses were returned. Follow-up mail was sent after one month and data were increased by 97. In total, 285 questionnaires were collected, with a response rate of 57%.

The respondents in the study were high-level executives in container shipping firms, such as vice presidents or higher, managers, directors, and IT operators (see Table 1), ensuring that the respondents had strategic-level supervising experience in fields related to IT security management. Further, most respondents had spent more than 63% of their time working in the container shipping industry, indicating that they had sufficient knowledge to answer the questionnaire.

Table 1. Profile of respondents.

	Number of Respondents	Percentage of Respondents
Job title		
Vice president or higher	14	4.9
Manager	77	27.0
Director	22	25.3
General employees	45	15.8
IT operators	77	27.0
Number of employees		
50 or fewer	74	26.0
51–100	37	13.0
101–200	83	29.1
201–300	76	26.7
300 or more	15	5.3
Work experiences (years)		
5 years or fewer	17	6.0
6–10	38	13.3
11–15	47	16.5
16–20	90	31.6
20 or more	93	32.6
Tenure in current company (years)		
5 or fewer	31	10.9
6–10	50	17.5
11–15	84	29.5
20 or more	120	42.1
Length of business operations (years)		
5 or fewer	2	0.7
6–10	10	3.5
11–20	33	11.6
21–30	96	33.7
30 or more	144	50.5
Ownership pattern		
Local firm	197	69.1
Foreign-owned firm	40	14.0
Foreign local firm	48	16.8
Security training participation (number of training courses attended)		
Never	65	22.8
1	95	33.3
2	57	20.0
3	43	15.1
4	11	3.9
5 or above	14	4.9
Security experience		
Phishing	136	22.1
Malware	103	16.7
Ransomware	95	15.4
Spam	203	32.9
Outdated security	49	7.9
None	31	5.0

3.2. Non-Response Bias and Common-Method Variance

To investigate possible bias in the self-reported survey data, non-response bias and common-method variance tests were carried out. Non-response bias was checked by t-test analysis of the data sets of the early and late respondents [40]. The results of the 26 measurement items showed no significant difference ($p < 0.05$) between the two groups, indicating that the data were free of non-response bias.

As the research relied on the single respondent and perceptual scales to evaluate dependent and independent variables, the presence of common-method variance (CMV) was determined. Harman's single factor test with confirmatory factor analysis (CFA) tested whether CMV existed. As CMV is a serious threat to research outcomes, Harman's single factor test can account for most of the variance [41]. When Harman's single factor test results in a poor fit with the data, CMV is not a problem. The CFA results showed that the results of Harman's single factor test and the 26 measurement items did not fit (χ^2 = 2891.44, df = 300; CFI = 0.33; GFI = 0.48; AGFI = 0.39; RMR = 0.21; RMSEA = 0.17), so CMV was not a concern in the current research.

3.3. Measures

This study followed Iacobucci and Churchill's design [42] for data collection and measures. To capture the aim of the questionnaires, besides adapting the survey items from the literature, five experts with over 20 years of management or information security experience in the container shipping industry were interviewed. For every variable in the sections below, the respondents were asked to rate the degree to which the statement items reflecting their experiences in daily work in the organization were favorable. The items used a five-point Likert scale ranging from 1 = strongly disagree to 5 = strongly agree (all the measurement items are listed in Table 2).

Table 2. Exploratory factor analysis.

Items	Mean	S.D.	F1	F2	F3	F4	F5
Information security marketing							
S7 Information security threats are always alerted to all employees through messages or emails in my organization.	4.13	0.72	0.77				
S4 My organization always provides specific training on information security regularly.	4.17	0.78	0.75				
S3 My organization takes information security into account when running the business.	4.31	0.77	0.73				
S6 Any changes related to information security policies are always alerted to all employees through messages or emails in my organization.	4.18	0.68	0.70				
S5 My organization encourages me to attend information security campaigns.	4.14	0.69	0.69				
S8 My company communicates clear information on security policies to employees.	4.04	0.74	0.68				
S1 My organization always seeks improvements related to information security policies.	4.20	0.69	0.66				
S2 My organization is confident that compliance with information security policies is important.	4.29	0.74	0.66				
Information security climate							
C5 My supervisor discusses information security issues with me and my colleagues.	3.97	0.86		**0.88**			
C1 I believe that other employees comply with the information security policies of my organization.	4.09	0.84		**0.85**			
C2 The majority of other employees take the information security of my organization into account to help protect the organization's information systems.	4.12	0.78		**0.85**			

Table 2. *Cont.*

Items	Mean	S.D.	F1	F2	F3	F4	F5
C4 Employees discuss information security threats with each other in my organization.	3.86	0.84		**0.79**			
C3 My supervisor and colleagues support me when I adopt proper information security practices.	3.77	0.90		**0.79**			
Information security intention							
T5 When I access the information system, I consider the organization's information security policies.	4.38	0.70			**0.80**		
T3 I remind others to take care with information security issues.	4.22	0.81			**0.78**		
T4 I assist others in complying with information security policies.	4.35	0.69			**0.77**		
T1 I am likely to follow information security policies.	4.34	0.73			**0.77**		
T2 I consider information security practices when performing my daily work.	4.34	0.68			**0.76**		
Security response cost							
R4 Having to learn how to adopt information security behavior would result in a significant loss of my work time.	2.84	0.93				**0.87**	
R3 Complying with information security policies is costly for me (e.g., learning cost or time cost).	2.95	0.97				**0.87**	
R2 Complying with information security procedures inconveniences my work.	2.99	0.95				**0.82**	
R1 Complying with information security procedures is time-consuming.	3.01	0.95				**0.78**	
Information security awareness							
A3 I believe that violations of the organization's information security policies would cause serious damage to the organization.	4.12	0.87					**0.87**
A4 I am aware that if I do not adopt information security behavior adequately, it will cause security incidents.	4.02	0.85					**0.85**
A2 An information security breach in my organization would be a serious problem for my organization.	3.93	0.88					**0.84**
A1 I understand the potential security threats, risks, and negative consequences.	3.89	0.85					**0.83**
Eigenvalues			4.40	3.60	3.36	3.05	2.96
Cumulative percentage variance (%)			16.93	30.76	43.77	55.39	66.77

Information security marketing measures: This study measured an organization's ISM from the employees' perspectives using a version of the eight items adapted from [29,30,39,43–46]. In asking the respondents how they felt about their organization's ISM, the scale used empirical practices for security marketing. Higher ratings on the scales represented greater ISM in the organization. **Response cost measures:** Self-reported RSC was measured using four items developed by [34,44,47]. The respondents were asked to answer whether they had trouble conducting security procedures or policies. Higher mean scales indicated that the respondents needed to spend the more implicit cost to follow security procedures. **Information security intention measures:** To evaluate ISI, the respondents were asked to rate their ISI with five items to understand whether they were willing to collaborate with their organization. The measurement items examined this construct based on [6,34,39,43,44,48]. These items were used to check the respondents' intentions (either their own or in helping others) to enhance information security at their workplace. **Information security awareness:** Four items, developed by [13,38,44,47,48], on the respondents' willingness to take ISA into account were used to test their initial awareness regarding information security processing. **Information security climate:** In line with previous studies [22,34,39], this study used five items to examine the typical environment of information security by asking the respondents to rate these items using indices showing the overall level of ISC.

3.4. Analytic Method

Before testing the research hypotheses, this study employed exploratory factor analysis (EFA) and CFA to perform the convergent and discriminant validity of every measure's constructs to ensure that they were reliable. The antecedents of relationships between ISM, RSC, and ISI were examined by structural equation modeling (SEM). A hierarchical regression approach was carried out to assess the moderating effects [49]. Processing software [50] was employed to determine the paths of moderated mediation between model constructs to evaluate their significance and the model's predictive relevance. According to the guidelines of [49,50], these stages were analyzed using statistical packages SPSS 25.0 and AMOS 25.0 for Windows.

4. Results and Empirical Approach

4.1. Exploratory Factor Analysis

This study assessed a series of analyses to test the properties of the measurement scales. EFA with eigenvalues greater than 1.0 and with VARIMAX rotation approach was performed on the scale items, analyzing one scale at a time to ensure unidimensionality [49]. Bartlett's Test of Sphericity was 4059.192 ($p < 0.001$), and the KMO value was 0.86, indicating that they could be further analyzed (see Table 2).

The Corrected Item-Total Correlation (CITC) reliability results are shown in Table 3 below. All CITC values were more than 0.6, the R^2 values were over 0.4, and the Cronbach's alpha values achieved levels greater than 0.8, indicating that the scales were reliable [49].

Table 3. Parameter estimate and convergent and discriminant validity.

Latent Variable Items	Standardized Loading	Standard Error [a]	Critical Ratio [b]	R^2	Mean	S.D.	Item-Total Correlation	Cronbach's Alpha
ISM					4.18	0.53	0.62–0.67	0.88
SM1	0.68	0.10	9.63	0.46				
SM2	0.70	0.10	10.22	0.49				
SM3	0.72	0.11	10.52	0.52				
SM4	0.69	0.11	10.16	0.48				
SM5	0.68	0.10	9.98	0.46				
SM6	0.66	0.09	9.77	0.44				
SM7	0.72	0.10	10.44	0.51				
SM8	0.80	- [c]	- [c]	0.44				
RSC					2.95	0.99	0.68–0.80	0.88
RS1	0.71	0.05	13.57	0.51				
RS2	0.80	0.05	16.18	0.64				
RS3	0.83	0.05	17.04	0.69				
RS4	0.88	- [c]	- [c]	0.77				
ISI					4.33	0.53	0.68–0.73	0.88
IT1	0.74	0.08	12.99	0.55				
IT2	0.77	0.70	13.47	0.59				
IT3	0.77	0.08	13.55	0.60				
IT4	0.77	0.07	13.57	0.59				
IT5	0.79	-[c]	-[c]	0.63				
ISA					3.99	0.74	0.70–0.76	0.87
IA1	0.76	0.07	13.43	0.58				
IA2	0.77	0.07	13.56	0.59				
IA3	0.84	0.07	14.90	0.71				
IA4	0.81	- [c]	- [c]	0.65				
ISC					3.96	0.71	0.71–0.82	0.90
IC1	0.82	0.08	12.99	0.68				
IC2	0.78	0.07	13.47	0.61				
IC3	0.78	0.08	13.55	0.61				
IC4	0.75	0.07	13.57	0.56				
IC5	0.88	- [c]	- [c]	0.77				

Note: [a] Standard Error is an estimate of the standard error of the covariance; [b] Critical Ratio is the critical ratio obtained by dividing the estimate of the covariance by its standard error, and a value exceeding 1.96 represents a level of significance of 0.05; [c] Indicates a parameter fixed at 1.0 in the original solution.

4.2. Confirmatory Factor Analysis

Consistent with the method supported by [49], a measurement model was evaluated by conducting CFA. The CFA model was developed with five latent variables, and the results were expected to be correlated with each other. Given the sensitivity of the chi-squared test (X^2 = 512.469; df = 289) and its unreliability in the case of examining model fit in SEM, this study relied on the unlikeness of good-fit indices, including the following: comparative-fit index (CFI), which was 0.94 (>0.9); adjusted-goodness-of-fit index (AGFI), which was 0.85 (>0.8); Tucker-Lewis index (TLI), which was 0.94 (>0.9); the

root-mean-square residual (RMR), which was 0.03 (<0.08); and the root-mean-square error of approximation (RMSEA), which was 0.05 (<0.05). All the fit indices were considered to have a good fit with the data.

Next, the convergent and discriminant validities of five constructs were investigated. Construct reliability (CR) assesses the internal consistency of a measure, and convergent validity exists if the CR value (between 0.87 and 0.90) exceeds the request level of 0.7 [51]. Table 4 shows that the CR values were between 0.87 and 0.90, reflecting a high reasonable standard, giving strong support for the convergent validity of all measurements in the five constructs. The average variance extracted (AVE) was conducted next to assess discriminant validity. The AVE value is the amount of variance obtained by each construct in association with variance due to random measurement error [51]. Discriminant validity exists if the minimum AVE value is 0.5, and the level of the square root of the AVE should be greater than the correlations between any two constructs. The AVE values were between 0.5 (ISM) and 0.65 (RSC, ISC). These results confirmed that the measurement model had relevant psychometric properties.

Table 4. Average variance extracted, composite reliability, and collections.

Measure	AVE [a]	Construct Reliability [b]	SMC	RSC	ISI	ISA	ISC
ISM	0.50	0.89	1 [c]				
RSC	0.65	0.88	−0.22 **	1			
ISI	0.59	0.88	0.50 **	−0.30 **	1		
ISA	0.63	0.87	0.07 **	−0.13 **	0.00 **	1	
ISC	0.65	0.90	0.27 **	0.11	0.12 **	0.21 **	1

Note: ** Correlation is significant at the 0.05 level; [a] Average variance extracted (AVE) = (sum of squared standardized loading)/[(sum of squared standardized loadings) + (sum of indicator measurement error)], and indicator measurement error is calculated as 1 − (standardized loading)^2; [b] Construct reliability = (sum of standardized loadings)^2/[(sum of standardized loadings)^2 + (sum of indicator measurement error)], and indicator measurement error is calculated as 1 − (standardized loading)^2; [c] The square root of the shared variance between the constructs and their measures are provided in the diagonal.

4.3. Structural Equation Modeling

SEM analysis is evaluated by overall and relative model fit and structural parameter estimates, depicted with one-headed arrows on a path diagram [49]. The theoretical model shown in Figure 2 is examined based on how well it reproduces the observed covariance matrix and on the significance and direction of the hypothesized paths between ISM, RSC, and ISI. The model fit indices suggested a good fit between the hypothesized framework and the data (chi-squared = 211.805, $p < 0.001$; X^2/df = 1.83; CFI = 0.96; AGFI = 0.89; TLI = 0.95; RMR = 0.029; RMSEA = 0.05) [45]. The results indicated that ISM had a positive impact on ISI (standardized coefficient = 0.512, $p < 0.001$). Thus, Hypothesis 1 was supported. The effect of ISM on RSC was examined and it had a negative relationship (standardized coefficient = −0.246, $p < 0.001$), supporting Hypothesis 2. Hypothesis 3 pertained to the relationship between RSC and ISI (standardized coefficient = −0.205, $p < 0.001$), which was also supported.

4.4. Hierarchical Regression Testing

Hierarchical regression testing is usually accessed by moderating effects test [52]. The next step aimed to test the moderating effects of ISA and ISC using a hierarchical regression model. As shown in Table 5, sex and age were the control variables for this study as these might have presented alternative demonstrations for the hypothesized relationships. The control variables were included only in Model 1 and Model 4. The main effects of ISM, RSC, ISI, ISA, and ISC were set into proper constructs, respectively (see Model 2 and Model 5).

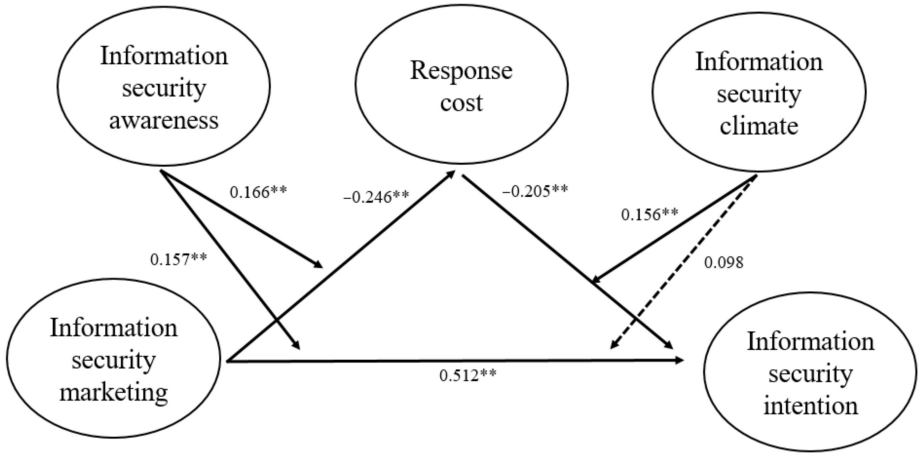

Figure 2. Depiction of results. (Note: ** $p < 0.05$).

Table 5. Summary of moderating test results.

	RSC Model 1	RSC Model 2	RSC Model 3	ISI Model 4	ISI Model 5	ISI Model 6	ISI Model 7	ISI Model 8
Control variables								
Sex	−0.096	−0.098	−0.081	−0.060	−0.072	−0.053	−0.066	−0.063
Age	0.045	0.049	0.043	0.052	0.123 **	0.069	0.080	0.068
Main effects								
ISM		−0.217 ***	−0.175 **		0.438 ***	0.482 ***	0.474 ***	0.413 ***
RSC					−0.238 ***	−0.246 ***	−0.234 ***	−0.220 ***
ISA		−0.116 **	−0.101		−0.064	−0.049	−0.068	−0.061
ISC					0.021	0.013	0.019	0.027
Moderating effects								
ISM x ISA			0.166 **			0.157 **		
ISM x ISC							0.098	
RSC x ISC								0.156 **
F-value	1.592	5.707 ***	6.238 ***	0.884	17.640 ***	18.652 ***	17.543 ***	18.779 ***
Adjust R^2	0.004	0.062	0.084	−0.001	0.289	0.303	0.290	0.305
Durbin-Watson	0.840	0.877	0.882	1.696	1.576	1.602	1.551	1.642

Note: *** Coefficient is significant at the 0.01 level; ** coefficient is significant at the 0.05 level.

The Durbin–Watson value was assessed to examine the multicollinearity of the regression equation. The results showed that it ranged from 0.840 to 1.696 (>0.60), proving that there were no problems concerning correlated residuals. In Model 1 and Model 4, sex and age had no significant impact on the dependent variables. ISM had a negative effect on RSC in Model 2 and a positive influence on ISI in Model 5, at a significance level of 0.01. This outcome met the SEM test. The moderating effects were investigated in Model 3, Model 6, Model 7, and Model 8. In Model 3 and Model 6, ISA had a robust positive significant impact on the relationship between ISM and RSC ($\beta = 0.166$, $p < 0.05$) and ISM and ISI ($\beta = 0.157$, $p < 0.01$). ISC was verified as an important moderating variable for ISI ($\beta = 0.156$, $p < 0.05$) in Model 8. Conversely, ISA was not found to have a significant

moderating effect on ISI ($\beta = 0.098$, $p > 0.05$) in Model 7. Figures 3–5 present a positive relationship between ISM and RSC with ISI when ISA and ISC were higher rather than lower. Therefore, Hypotheses 4–6 were supported, while Hypothesis 7 was not supported based on the results of this study.

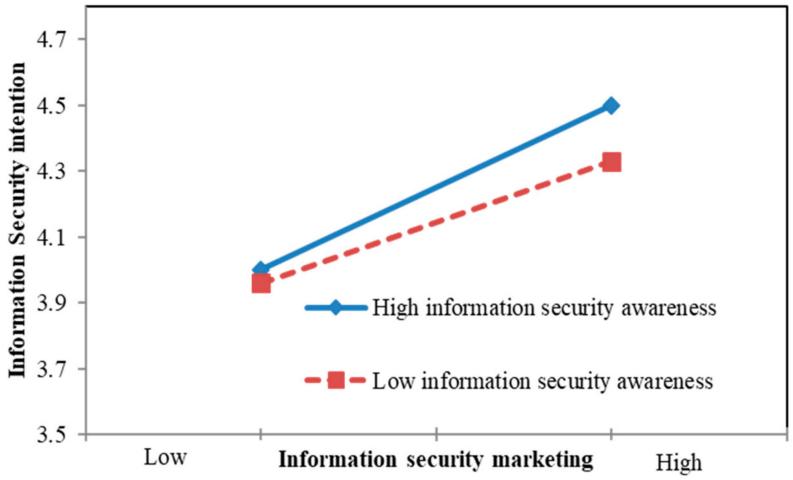

Figure 3. The moderating effect of information security awareness on information security marketing and information security intention.

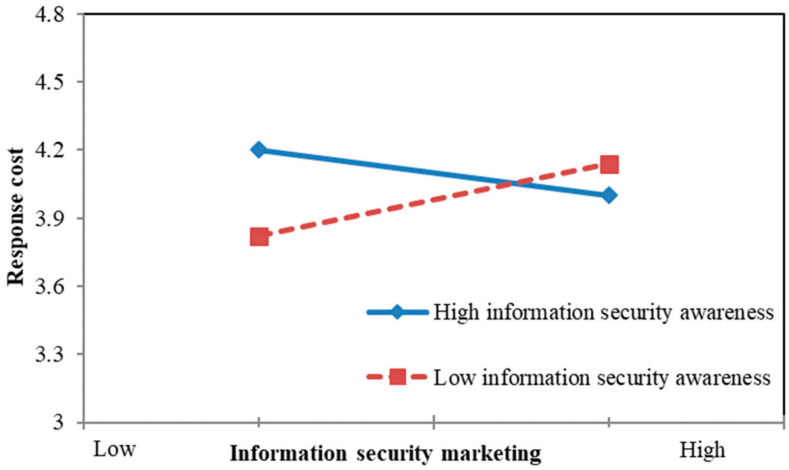

Figure 4. The moderating effect of information security awareness on information security marketing and response cost.

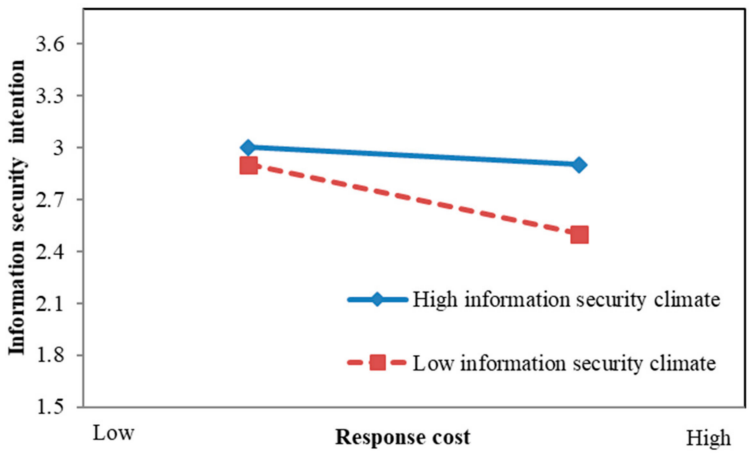

Figure 5. The moderating effect of information security climate on response cost and information.

4.5. Moderated Mediating Effect Testing

Hypothesis 8 posited a moderated mediating effect, whereby the mediating effect would vary by RSC, ISA, and ISC. This study used the software Process version 3.0 for SPSS [50] to test ISM's indirect effect on ISI. ISA and ISC were evaluated as having moderating effects in impacting the main effects on the dependent variables. The analyses showed an indirect effect of the role model on ISI (indirect effect = 0.08; confidence [0.02, 0.16]). The results showed a confidence interval that did not include zero, but a definitive claim could not be made that the moderator's indirect effect was related. This explained why ISM's indirect effect on ISI through RSC was moderated by ISA and ISC, signifying that the mediation of the effect of ISM on ISI was moderated, so Hypothesis 8 was supported.

5. Discussion and Implications

This study empirically investigated the effects of ISM and RSC on ISI in the container shipping context. This study also explored the moderating effects of ISA and ISC on these relationships and found that some of them moderated these relationships. This study sought to address several important issues associated with organizational information security marketing and information security intention in container shipping firms. The main findings are discussed as follows.

5.1. Discussion

Based on their ISM concerns, the respondents considered that security policies were the most important in running their business operation processes. One research question asked whether establishing a complete information security policy was necessary. However, the respondents replied that their company did not communicate clear information on their employees' security policies. This usually caused employees to follow incorrect procedures and indicated that most of the shipping did not implement their right processes. This study's findings can advance container shipping firms' information ex-changes and publishing platforms, which may facilitate employees in clearly receiving the latest news as soon as it is available.

The respondents also believed that learning how to adopt security behaviors would result in a significant loss of their work time. How can organizations progress from passive to active learning? A proper reward or a rewarding scheme [53] has encouraged employees to continue learning while working. Research findings have also shown that this is the largest RSC, and total RSC could be improved if employees are willing to improve their workplace security behaviors. This implied the container shipping companies are suggested to establish a rewarding policy or system that encourages employees' security intention.

Regarding ISI, most of the respondents' agreement was that they considered their security policies when using their information systems. This implied that the respondents had a basic security concept when assessing their work systems. The shipping companies may consider holding more security training activities to improve greater information security. On the other hand, employees almost focused on their attention; however, they did not always remind their partners to consider security issues, which should be promoted. Having more warning messages in the workplace, enhancing supervisors' security leadership [12] in information security, and having clear security work procedures [52,54] would effectively help solve this circumstance.

ISA was noted in the respondents' cognition of information security. Responding to calls to conceptualize and investigate ISA, the results indicated that violations of the organization's security policies would cause severe damage. On the other hand, the respondents did not fully know the potential security threats and their risk consequences. This implied that organizations were only aiming for employees to follow the security instruction but did not show the severe outcomes of the damage. For example, system breakdown cannot handle the ports, ships, cargo, and other partners. All world shipping operations may be interrupted, bringing a great deal of business loss. Organizations should

share more knowledge about the threats caused by the lack of information security to emphasize its importance.

From an ISC perspective, most employees were focused on information security and the need to protect it well. However, a perfect security climate is one in which most employees reach a security consensus. How can an organization encourage security consensus of most employees? To cultivate abundant ISC, the current study results notably suggested that supervisors and colleagues should support their coworkers in adopting security practices. When employees feel they are supported, they are more willing to act themselves and influence others.

5.2. Theoretical Implications

This study has several theoretical implications. First, the work extends the marketing literature. Previous research mainly focused on the detrimental effects of sales strategies, market searches, customer trends, and so on [55], while overlooking the internal marketing that potentially drives employees' intentions to enhance their work. This study demonstrates how marketing management helps with information protection by examining the impacts of response cost and information security intention. Based on Hypotheses 1 and 2 being supported, organizational ISM is vital for both RSC and ISI. These findings enrich the literature on the RBV theory in the container shipping industry with information security management, security policy improvements, security compliance, regular security training, and an alerting system. Supervisors' practices can establish clear security policies by demonstrating work procedures so that employees can comply with them effectively. This is congruent with RBV theory. Stewardship practices are likely to be part of information security marketing's organizational management, thus contributing to employees' information security intentions and behaviors.

Second, this study primarily focused on the overall yet rarely studied response cost to consider when an organization needs to proceed with security marketing. ISM harmed RSC. Although ISM is critical to an organization and improves employees' efficient security intentions, RSC is often restrained [53,55]. In this context, the cost is not likely to be in terms of cash but instead lost time, working inconvenience, and learning price. It is not easy to achieve high efficiency when complying with security procedures for sufficient work in a busy environment.

Third, there was a negative influence of ISI on RSC [55]. This can be interpreted as employees needing to pay a high cost to obeying security policies, reducing their information security intentions. This implies that stewardship must show or participate in security activities, encouraging employees to follow security procedures to strengthen their ISI.

Fourth, there was also a positive moderating effect between ISM and ISI/RSC in ISA. For organizations with better ISA, ISM can positively impact ISI and RSC, while such a positive association is not easy to find when ISA is low [24]. Regarding this advanced ISA on the positive association between ISM and ISI/RSC, if employees know that violations of the organization's security policies will cause serious damage, they may adequately adopt security action and recognize potential security threats and risks to avoid information breaches. The application of ISA can help ISM reduce RSM for performance improvement.

Fifth, the theoretical predictions were supported in that ISC had a moderating effect on the relationship between RSC and ISI. Even with RSC's negative influence on ISI, ISC moderated RSC's effects, such as employees considering information security and protecting information systems, encouraging other employees to comply with security policies, supporting other colleagues in adopting proper security practices, and discussing security threats in the organization. Cultivating an information security climate requires everyone's involvement. Such ISA is reflected in employees' ISI, so better ISA will lead to better ISI.

Sixth, this study did not support the idea that ISA moderates the relationship between ISM and ISI, despite empirical evidence on ISA as a moderator for ISM and ISI in performing

goals. Finally, this study has shed light on the moderated (ISA and ISC) mediating (RSC) effects associated with the links between ISM and ISI by developing a model to understand the underlying mechanisms, through which ISM predicted ISI through the relationships between RSC, ISA, and ISC to find the indirect effects of ISM on ISI. The research findings addressed the issue that ISM is crucial for organizational security intention, as shown by its significant impact on ISI under the moderated mediation model.

5.3. Practical Implications

The current work's findings highlight a set of helpful directions that managers and organizations may use to take the most significant advantage of employees' information security intentions and behaviors. The current findings also highlight the critical outcomes of information security intention, such as policy compliance, and that participation can be accomplished when marketing management is employed within organizations. As a result, organizations and stewardship need to create organizational marketing systems with a promoting–sharing policy to appeal to employees' daily involvement.

This study also sheds light on ISA and how it is beneficial for organizations to reduce costs and achieve employees' security intentions. ISA is likely to take place in various occupations organized in routine work in shipping, such as information technology personnel who keep data safe, email receivers/senders, and other workers who access the Internet in the office. Similarly, this also applies to employees who frequently use the Internet for work and other branches or offices in charge of global regions. High levels of ISA can be established by regular training (e.g., email exercises, workshops, user manuals, or classes about security information), thus benefitting the protection of an organization's information system.

The study further found that spam is the most popular computer virus reported by the respondents, followed by phishing, malware, and ransomware. This implies that many firms' systems cannot accurately identify different kinds of email. Despite information technology needing to be enhanced, organizational employees should notify their information technology personnel when receiving any suspicious email. Although it is not easy to find the most effective approach to avoid spam, its prevalence can be reduced using a firewall.

5.4. Limitations and Suggestions for Future Research

Despite the strength of the results of this study (e.g., strong ISM, mediator examination, dependent variables to validate outcomes, frequent, ongoing visits by experts to discuss the questionnaire, theoretical inferences, and support of the hypotheses), this study has several limitations that should be addressed in future research. First, the study variables were self-reported by the respondents, due to the method used in the current work (i.e., multiple measurements were collected from the same participants). Each respondent served as his/her control group, captured in field contexts so that typical daily work in organizational marketing management, response cost, and information security intention could be obtained. This may lead to the non-response bias problem and cause fake results. Future studies should use non-self-report methods to reveal the study variables, such as obtaining financial performance for the dependent variable of employee security ratings. Moreover, while this study presented proof of the ISM effect of employees' RSC on ISI, it did not consider other possible variables that may have also impacted their ISI. Considering other potential variables, for example, encouragement [56], leadership [12], risk management [57], or institutions [58], future studies should further examine the consequences of these variables to compare different outcomes of employees' ISI. Further, due to the limited time and cost, this study only focused on the container shipping industry. This cannot represent every industry. Other sectors may have different views and result in different outcomes. We suggest that further research studies can investigate various industries and the differences between them. Additionally, a longitudinal approach can solve the problem of data collection at one point in time. This may lose the changes in the other time point.

Using data collected from various points to investigate the research model's short- and long-term effects might bring complete outcomes and contributions. Finally, this study was conducted in Taiwan. Although Taiwan is known as a key shipping region, other areas should also be investigated. Ultimately, future research should employ this research framework to examine different areas.

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

Funding: This research has been sponsored by the Higher Education Sprout Project, Ministry of Education (MoE) in Taiwan under research grant number MOE-108G0038. This work also was supported in part by the Ministry of Science and Technology (MoST), Taiwan, under Grants MOST 109-2222-E-346-001.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. IDC. Worldwide Semiannual Security Spending Guide. 2017. Available online: https://www.idc.com/getdoc.jsp?containerId=IDC_P33461 (accessed on 7 August 2018).
2. IDG. 2018 Global State of Information Security Survey. 2018. Available online: https://zh.scribd.com/document/366302651/2018-Global-State-of-Information-Security-Survey#download&from_embed (accessed on 8 August 2018).
3. Kuo, S.Z.; Lin, P.C.; Lu, C.S. The effects of dynamic capabilities, service capabilities, competitive advantage, and organizational performance in container shipping. *Transp. Res. Part A* **2017**, *95*, 356–371. [CrossRef]
4. UNCTAD. *Review of Maritime Transport 2018*; UNCTAD/RMT/2019; UNCTAD: New York, NY, USA, 2019.
5. IQPC. The Depth of This Year's NotPetya Attack Is Now Coming to Light, and It Is Certainly No Laughing Matter—Especially for Companies' Bottom Lines. 2017. Available online: https://www.cshub.com/attacks/news/notpetya-costs-merck-fedex-maersk-800m (accessed on 8 August 2018).
6. Huang, L.; Cha, O. Examining technostress creators and role stress as potential threats to employees' information security compliance. *Comput. Hum. Behav.* **2018**, *81*, 282–293. [CrossRef]
7. Armstrong, G.; Kolter, P. *Marketing: An Introduction*, 14th ed.; Pearson Education: Upper Saddle River, NJ, USA, 2019.
8. Ferdous, A.S.; Herington, C.; Merrilees, B. Developing an integrative model of internal and external marketing. *J. Strateg. Mark.* **2013**, *21*, 637–649. [CrossRef]
9. Barry, L.L. The employee as customer. *J. Retail Bank.* **1981**, *3*, 25–28.
10. Pantouvakis, A. Internal marketing and moderating role of employees: An exploratory study. *Total Qual. Manag.* **2012**, *23*, 177–195. [CrossRef]
11. Rafiq, M.; Ahmed, P.K. Advances in the internal marketing concept: Definition, synthesis and extension. *J. Serv. Mark.* **2000**, *14*, 449–462. [CrossRef]
12. Lu, C.S.; Kuo, S.Y.; Chiu, Y.T. Ethical leadership and ethical climate in the container shipping industry. *Int. J. Shipp. Transp. Logist.* **2013**, *5*, 591–604. [CrossRef]
13. Yazdanmehr, A.; Wang, J. Employees' information security policy compliance: A norm activation perspective. *Decis. Support Syst.* **2016**, *92*, 36–46. [CrossRef]
14. Luria, G.; Yagil, D. Procedural justice, ethical climate and service outcomes in restaurants. *Int. J. Hosp. Manag.* **2008**, *27*, 276–283. [CrossRef]
15. Safa, N.S.; Solms, R. An information security knowledge sharing model in organizations. *Comput. Hum. Behav.* **2016**, *57*, 442–451. [CrossRef]
16. Hanus, B.; Wu, A.Y. Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Inf. Syst. Manag.* **2016**, *33*, 2–16. [CrossRef]
17. Adams, P.; Freitas, I.M.B.; Fontana, R. Strategic orientation, innovation performance and the moderating influence of marketing management. *J. Bus. Res.* **2019**, *97*, 129–140. [CrossRef]
18. Ellram, L.M.; Murfield, M.L.U. Supply chain management in industrial marketing-relationships Matter. *Ind. Mark. Manag.* **2019**, *79*, 36–45. [CrossRef]

19. Amato, F.; Moscato, V.; Picariello, A.; Sperlí, G. Diffusion Algorithms in multimedia social networks: A preliminary model. In *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017*; Association for Computing Machinery: New York, NY, USA, 2017; pp. 844–851.
20. Chakraborty, T.; Jajodia, S.; Katz, J.; Picariello, A.; Sperli, G.; Subrahmanian, V.S. Forge: A fake online repository generation engine for cyber deception. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 518–533. [CrossRef]
21. Hayes, A.F. *Introduction to Mediation, Moderation, and Conditional Process Analysis*, 2nd ed.; The Guilford Press: New York, NY, USA, 2017.
22. Chen, M.; Woon, I.; Kankanhalli, A. Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *Int. J. Inf. Secur. Priv.* **2005**, *1*, 18–41. [CrossRef]
23. Chen, X.; Chen, L.; Wu, D. Factors that influence employees' security policy compliance: An awareness-motivation-capability perspective. *J. Comput. Inf. Syst.* **2018**, *58*, 312–324. [CrossRef]
24. Spears, J.L.; Barki, H. User participation in information systems security risk management. *MIS Q.* **2010**, *34*, 503–522. [CrossRef]
25. Bansal, H.S.; Mendelson, M.B.; Sharma, B. The impact of internal marketing activities on external marketing outcomes. *J. Qual. Manag.* **2001**, *6*, 61–76. [CrossRef]
26. Gyepi-Garbrah, T.F.; Asamoah, E.S. Towards a holistic internal market orientation measurement scale. *J. Strateg. Mark.* **2015**, *23*, 273–284. [CrossRef]
27. Kaur, J.; Sharma, S.K. Internal marketing: Scale development and validation. *J. Bus. Perspect.* **2015**, *19*, 236–247. [CrossRef]
28. Chen, Y.C.; Lin, S. Modeling internal marketing and employee loyalty: A quantitative approach. *Asian Soc. Sci.* **2013**, *9*, 99–109. [CrossRef]
29. Chen, J.H.; Wu, S.I. The impact of customer relationship management and internal marketing on business performance: A comparison of lodging industries. *Total Qual. Manag.* **2016**, *27*, 17–33. [CrossRef]
30. Huang, Y.T.; Rundle-Thiele, S. A holistic management tool for measuring internal marketing activities. *J. Serv. Mark.* **2015**, *29*, 571–584. [CrossRef]
31. Ferdous, A.S.; Polonsky, M. The impact of frontline employees' perceptions of internal marketing on employee outcomes. *J. Strateg. Mark.* **2014**, *22*, 300–315. [CrossRef]
32. Cătălin, C.M.; Andreea, P.; Adina, C. A Holistic approach on internal marketing implementation. *Bus. Manag. Dyn.* **2014**, *3*, 9–17. [CrossRef]
33. Menard, P.; Bott, G.J.; Crossler, R.E. User motivations in protecting information security: Protection motivation theory versus self-determination theory. *J. Manag. Inf. Syst.* **2017**, *34*, 1203–1230. [CrossRef]
34. Chen, X.; Wu, D.; Chen, L.; Teng, J.K.L. Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Inf. Manag.* **2018**, *55*, 1049–1060. [CrossRef]
35. Moody, G.D.; Siponen, M.; Pahnila, S. Toward a unified model of information security policy compliance. *MIS Q.* **2018**, *42*, 185–311. [CrossRef]
36. Yoon, C.; Hwang, Y.W.; Kim, R. Exploring factors that influence students' behaviors in information security. *J. Inf. Syst. Educ.* **2012**, *23*, 407–415.
37. Connolly, L.Y.; Lang, M.; Gathegi, J.; Tygar, D.J. Organizational culture, procedural countermeasures, and employee security behavior: A qualitative study. *Inf. Comput. Secur.* **2017**, *25*, 118–136. [CrossRef]
38. Ortiz, J.; Chil, W.H.; Tsai, F.S. Information privacy, consumer alienation, and lurking behavior in social networking sites. *Comput. Hum. Behav.* **2018**, *80*, 143–157. [CrossRef]
39. Goo, J.; Yim, M.S.; Kim, D.J. A path to successful management of employee security compliance: An empirical study of information security climate. *IEEE Trans. Prof. Commun.* **2014**, *57*, 286–308. [CrossRef]
40. Armstrong, J.S.; Overton, T.S. Estimating nonresponse bias in mail surveys. *J. Mark. Res.* **1977**, *14*, 396–402. [CrossRef]
41. Fuller, C.M.; Simmering, M.J.; Atinc, G.; Atinc, Y.; Babin, B.J. Common methods variance detection in business research. *J. Bus. Res.* **2016**, *69*, 3192–3198. [CrossRef]
42. Iacobucci, D.; Churchill, G.A. *Marketing Research: Methodological Foundation*; The Dryden Press: New York, NY, USA, 2010.
43. Chen, S.H.; Liu, P.Y. Effects of internal marketing, organizational commitment, job involvement and job satisfaction on work performance: A study of the elderly care institutions in Taiwan. *Mark. Rev.* **2012**, *9*, 277–302.
44. Humaidi, N.; Balakrishnan, V. The moderating effect of working experience on health information system security policies compliance behaviour. *Malays. J. Comput. Sci.* **2015**, *28*, 70–92.
45. Lin, C.C. Evaluating the effects of safety marketing on logistics operation in Taiwan free trade port zones. *Marit. Q.* **2016**, *25*, 1–30.
46. Narteh, B.; Odoom, R. Does internal marketing influence employee loyalty? Evidence from the ghanaian banking industry. *Serv. Mark. Q.* **2015**, *36*, 112–135. [CrossRef]
47. Vance, A.; Siponen, M.; Pahnila, S. Motivating IS security compliance: Insights from habit and protection motivation theory. *Inf. Manag.* **2012**, *49*, 190–198. [CrossRef]
48. Siponen, M.; Mahmood, M.A.; Pahnila, S. Employees' adherence to information security policies: An exploratory field study. *Inf. Manag.* **2014**, *51*, 217–224. [CrossRef]
49. Hair, J.F., Jr.; Black, W.C.; Babin, B.J.; Anderson, R.E. *Multivariate Data Analysis*, 7th ed.; Pearson: Upper Saddle River, NJ, USA, 2013.

50. Fornell, C.; Larcker, D.F. Evaluating structural equation models with un-observable and measurement Error. *J. Mark. Res.* **1981**, *18*, 39–50. [CrossRef]
51. Lu, C.S.; Kuo, S.Y. The effects of port employees' perceptions of tacit knowledge and transaction cost on knowledge transfer. *Int. J. Shipp. Transp. Logist.* **2014**, *6*, 46–68. [CrossRef]
52. Lu, C.S.; Kuo, S.Y. The effects of job stress on self-reported safety behavior in container terminal operations: The moderating role of emotional intelligence. *Transp. Res. Part F* **2016**, *37*, 10–26. [CrossRef]
53. Jeevan, J.; Othman, M.R.; Hasan, Z.R.A.; Pham, T.Q.M.; Park, G.K. Exploring the development of Malaysian seaports as a hub for tourism activities. *Marit. Bus. Rev.* **2019**, *4*, 310–327. [CrossRef]
54. Martin, S.L.; Javalgi, R.G.; Cavusgil, E. Marketing capabilities, positional advantage, and performance of born global firms: Contingent effect of ambidextrous innovation. *Int. Bus. Rev.* **2017**, *23*, 527–543. [CrossRef]
55. Alaghehband, F.K.; Rivard, S.; Wu, S.; Goyette, S. An assessment of the use of transaction cost theory in information technology outsourcing. *J. Strateg. Inf. Syst.* **2011**, *20*, 125–138. [CrossRef]
56. Chen, Y.; Ramamurthy, K.; Wen, K.W. Organizations' information security policy compliance: Stick or carrot approach? *J. Manag. Inf. Syst.* **2012**, *29*, 157–188. [CrossRef]
57. Lee, J.S.; Keil, M.; Shalev, E. Seeing the trees or the forest? The effect of IT project managers' mental construal on IT project risk management activities. *Inf. Syst. Res.* **2019**, *30*, 1015–1072. [CrossRef]
58. Wang, M.C.; Yip, T.L. Influence of transportation infrastructure on the relationship between institutions and economic performance. *Marit. Bus. Rev.* **2019**, *4*, 395–412. [CrossRef]