information

MDPI

Article

The Impact of Organizational Practices on the Information Security Management Performance

Latifa Alzahrani [1,*] and Kavita Panwar Seth [2]

[1] Department of Management Information Systems, College of Business Administration, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia
[2] Brunel Business School, College of Business, Arts and Social Sciences, Brunel University London, London WC2N 5DU, UK; panwar.kavita@googlemail.com
* Correspondence: lszahrani@tu.edu.sa

Abstract: Information explosion and pressures are leading organizations to invest heavily in information security to ensure that information technology decisions align with business goals and manage risks. Limited studies have been done using small- and-medium-sized enterprises (SMEs) in the manufacturing sector. Furthermore, a small number of parameters have been used in the previous studies. This research aims to examine and analyze the effect of security organizational practices on information security management performance with many parameters. A model has been developed together with hypotheses to evaluate the impact of organizational practices on information security management performance. The data is collected from 171 UK employees at manufacturing SMEs that had already implemented security policies. The structure equation model is employed via the SPSS Amos 22 tool for the evaluation of results. Our results state that security training, knowledge sharing, security education, and security visibility significantly impact information security performance. In addition, this study highlights a significant impact of both security training and knowledge sharing on trust in the organization. Business leaders and decision-makers can reference the proposed model and the corresponding study results to develop favourable tactics to achieve their goals regarding information security management.

Keywords: information security; security performance; knowledge sharing; education trust; training

check for updates

Citation: Alzahrani, L.; Seth, K.P. The Impact of Organizational Practices on the Information Security Management Performance. *Information* **2021**, *12*, 398. https://doi.org/10.3390/info12100398

Academic Editor: Shingo Yamaguchi

Received: 24 August 2021
Accepted: 17 September 2021
Published: 28 September 2021

1. Introduction

The exponential growth of information security management practises has been driven by the requirement for the information technology industry to more readily deal with the quality and dependability of big businesses [1]. The rapid development of information technologies leads to creating a highly efficient, albeit complex, way to organize business tasks and activities. This approach to information management, however, requires constant maintenance and updates. Therefore, it must be explored [2–4]. Pérez-González et al. [5] argue that "experts face similar problems in this domain and they should provide proper solutions for them, preventing the development of the same solutions for similar problems using sharing knowledge" (p. 1264). However, it has also been observed that the problems and solutions may depend on the industry's domain, because manufacturing SMEs issues are entirely different from other SMEs. The information security is a complex subject due to its multidisciplinary character [4,6–9]. According to Fonseca-Herrera et al. [6], a more holistic approach is needed for information security management. Siponen et al. [7] suggested that information security issues should be considered from a management perspective.

The literature on information security in companies has mainly focused on technological issues, with limited consideration to management strategies, security standards, and policies. Recent research [6,8–11] indicates the need of a more holistic approach to understand information security management. Previous studies mainly focused on organizational and human factors. By reviewing the literature, it appears that information security is a relatively recent concept in the focus of business management [6,10,12] and has acquired a greater impact from the generalized use of technology in business and the possibilities that the technologies based on the web allow in all enterprise processes. According to Pérez-González et al. [5], a few studies only considered organizational and human factors but mostly measured employees' perceptions on the predictors of their perceived security in organizations [3–5]. Several studies have been carried out with an emphasis on the organization [6,9,10,13,14] rather than thinking about authoritative factors, examining issues identified with consistency with the principles of information security, creating models and frameworks of data security the executives, and examining its confirmation. The number of articles shows that the examination pattern in investigating the management role in information security is a challenging task. This task is challenging, and inside this methodology, the hierarchical job in data security is getting progressively significant and is acquiring the consideration of scientists. This examination is an endeavour to fill the writing hole by zeroing in on the authoritative practices. In particular, the writing audit stands apart as the most referred to as cross-cutting for any association. It comprises rehearses at the functional level, executed by all workers, which are as follows: data security, information sharing, data security instruction, and data security perceivability. Information security is crucial, particularly with the increased sophistication of cybercrime and heightened regulations in the UK with the introduction of GDPR [11]. UK companies are obliged to meet certain requirements regarding data management and, therefore, the role of management processes in meeting those requirements is particularly important. This study fills a gap in existing research. Previous studies have focused on the technical aspects of information security, whereas this study highlights the importance of organizational procedures and the role of employees. There are the following contributions in this study:

- A model has been developed to evaluate the impact of organizational practices on information security management performance.
- Previous studies only focused on a few aspects of information security, but this study also highlights the importance of organizational procedures and the role of employees.
- To the best of our knowledge, this type of study has not been done yet in the UK. The proposed method was also validated through hypothesis testing.
- This study highlights that employees are often the source of unintentional data breaches, and their training in information security needs to be a priority.

The paper has organized as follows: Section 1 provides information about what is known and where the knowledge gap exists to gain new insight from this study. Section 2 includes a review of the literature and presents scientific information about information security management performance. Section 3 explains in detail the research framework, hypotheses, and data collection. Section 4 provides the results of the investigation. Section 5 presents the practical implications of the results.

2. Literature Review

Various combinations such as "Information security" and "performance measurement" and "Information security performance measurement" have been employed to search the literature. Four repositories: IEEE Xplore, Wiley, World Scientific, and ScienceDirect have directed. In total, 40 studies were finally selected for data utilization purposes. The paper selection process is explained in the Figure 1.

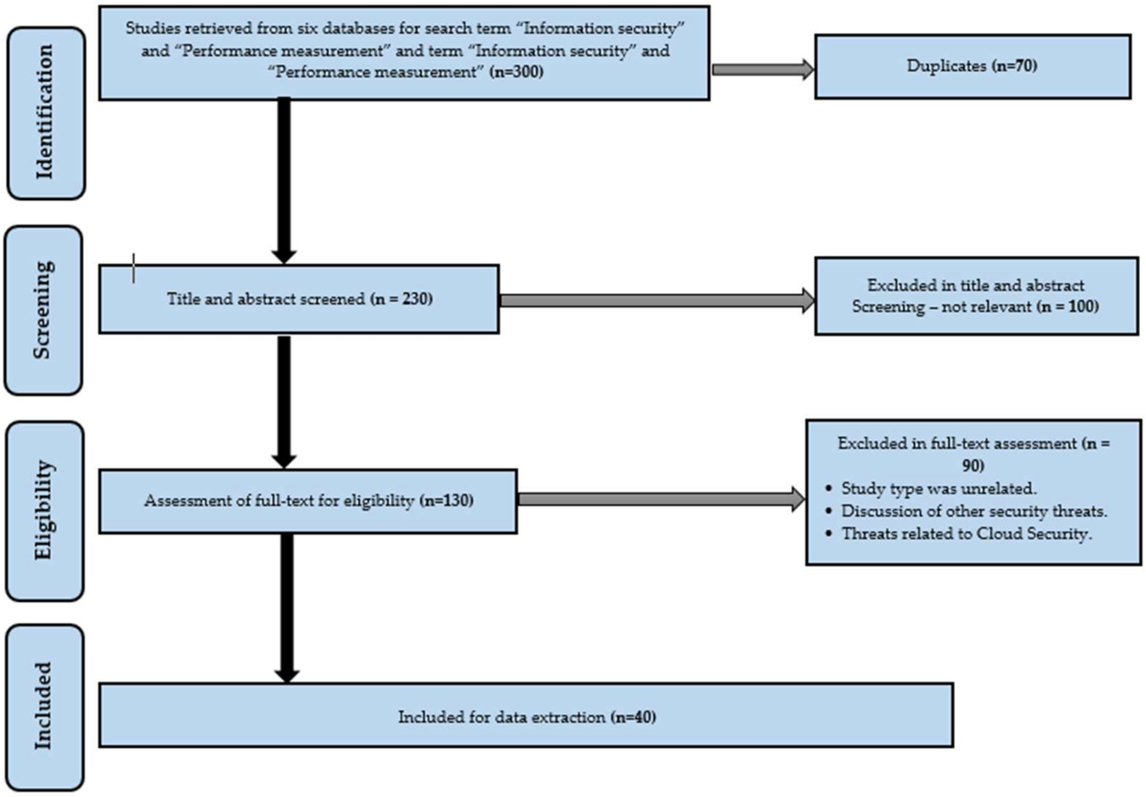
Identification
Studies retrieved from six databases for search term "Information security" and "Performance measurement" and term "Information security" and "Performance measurement" (n=300)
Duplicates (n=70)
Screening
Title and abstract screened (n = 230)
Excluded in title and abstract Screening – not relevant (n = 100)
Eligibility
Assessment of full-text for eligibility (n=130)
Excluded in full-text assessment (n = 90)
• Study type was unrelated.
• Discussion of other security threats.
• Threats related to Cloud Security.
Included
Included for data extraction (n=40)

Figure 1. Article selection process.

Ma et al. [13] developed an ISM-based framework for conceptualized decision-making. Their framework was based on four business-related principles that include the organisation's environment, objectives of information security, requirements of information security, and evaluation of information security protocols. Their results stated that several corporates are either less prepared or completely unprepared to diminish the proposed framework. Flores et al. [14] investigated the impact of establishing information security governance factors incorporated based on culture. The qualitative data of their study were collected from the USA and Sweden of 578 information security authorities. They observed that organization structure, organization policies, and working environment directly impact business-based information security management. Their study also revealed that business needs to impact the structure and management of the information security function. Parsons et al. [15] developed a questionnaire based on human aspects to measure the vulnerabilities for human-based information security. The data of 500 Australian executives were collected to test the proposed hypothesis, including reliability and validity testing. The results revealed that the education and training campaigns positively impacted employees' knowledge of policy and procedures. Singh and Gupta [16] developed a hybrid method to determine the factors related to information security management. They used keywords analysis for qualitative data and survey for quantitative data for exploratory factor analysis. Their results concluded that operational, strategic, and tactical factors impact information security management issues. Safa and Solms [17] integrated several human behaviour methods to determine the information security knowledge sharing development in various organizations. Their conceptual framework covers various factors such as behaviour, attitude, and intention. The major finding of their study is that motivational factors have positively correlated with information security knowledge sharing. Soomro et al. [18] conducted a systemic literature review to investigate the management's roles in information security management to improve productivity. They concluded that human resource management, information security-related policies, corporate infrastructure, and corporate architecture greatly impact information security management. They suggested that managers can play an effective role in information security management using a more holistic approach. Hwang et al. [19] investigated the relationship between organizational security factors and non-compliance causes of individuals. The data of 415 Spanish information security executives were collected to prove their hypothesis. The results stated that anxiety of security management and behaviour of peers are causes of non-compliance of employees. It was also observed that the security systems, security education, and security visibility may improve compliance among employees. Choi et al. [20] investigated the relationship between information security and organizational insiders. The qualitative data was collected from multinational company employees of the research and development department. Their results revealed that information security practices must be developed for information security threats. Moody et al. [21] compared eleven theories related to the behavioural perspective of information system security. They proposed a unified model of information security policy compliance (UMISPC) that employed important features of various models. The importance of the proposed model has also been improved theoretically. Gonzalez el al. [5] investigated the impact of organizational security practices on information security management performance. They proposed a model and validated it through hypothesis testing. Their results concluded that information security (knowledge sharing, education, visibility, and practices) positively correlates with information security management performance. Kobis [12] classified the major organizational threats in the way of information management processes. The particular was the intervention of human resources during the execution of information security management. Their results stated that a limited amount of intervention is mandatory for better working of information security management. Herrera et al. [6] proposed a framework for information security management to protect the data from outsiders, hackers, and unauthorized individuals. The proposed framework was based on NTC-ISO/IEC 27001:2013 standard. The results of the implemented model stated that information assets and technical vulnerabilities are important for information security management. The comparison among related studies and limitations are presented in Table 1.

Table 1. Relevant studies in the field of information security management.

References	Objective	Limitations
Ma et al. [13]	An ISM-based framework was developed for conceptualized decision-making.	It is observed that their framework consists of four principles but didn't explain how information security policy will be implemented. What are the parameters to establish the objectives of information security?
Flores et al. [14]	This study investigated the impact of the establishment of information security governance factors incorporates based on culture.	Only behavioural and cultural factors are included for the establishment of information security knowledge sharing in organizations.
Parsons et al. [15]	Developed a questionnaire based on human aspects to measure the vulnerabilities for human-based information security.	The impact of interventional, individual, and organizational factors on information security management also need to be determined.
Singh et al. [16]	Developed a hybrid method to determine the factors related to information security management.	A small number of factors were considered related to information security management.
Safa and Solms [17]	Integrated several methods using human behaviour to determine the information security knowledge sharing development in various organizations.	The sample size is small and limited techniques were employed for data collection.

Table 1. *Cont.*

References	Objective	Limitations
Soomro et al. [18]	Conducted a systemic literature review to investigate the management's roles in information security management to improve productivity.	A limited number of papers are included for the survey, and management perspective was not mentioned.
Hwang et al. [19]	Investigated the relationship between organizational security factors and non-compliance causes of individuals.	Only two non-compliance factors were determined. Employees actual behaviours in the context of information security need to be incorporated.
Choi et al. [20]	Investigated the relationship between information security and organizational insiders.	The impact of organisational citizenship behaviour needs to be evaluated in detail.
Moody et al. [21]	Compared eleven theories related to the behavioural perspective of information system security.	The proposed model was not proved practically nor empirically.
Pérez-González et al. [5]	Investigated the impact of organizational security practices on information security management performance.	The results cannot be mapped worldwide because the employed data was only collected from Spain since economic and technological development disparity exists worldwide.
Kobis [12]	Classified the major organizational threats in the way of information management processes.	This research lacks human factors (management level) on information security management.
Fonseca-Herrera et al. [6]	Proposed a framework for information security management to protect the data from outsiders, hackers, and unauthorized individuals.	The threats related to management individuals are not incorporated well.

3. Research Methodology

This study aimed to fill the gap in the literature by considering the organisational practices in studying information security management. A framework was developed based on the research framework proposed in the recent study by Pérez-González et al. [5], which studied three organisational factors: information security knowledge sharing, education, and visibility. This study has modified the framework to include two additional organisational factors: trust in an organisation and employee's training. Figure 2 presents the conceptual framework. To achieve the aims of this study, six hypotheses were developed based on the relationships between the constructs of the conceptual framework. When performing a hypothesis test, we tested our assumptions/hypothesis about a random sample, $x = (x_1, \ldots, x_n)$. The assumption could be that the sample observations come from a normal distribution, that the distribution means has a certain value, etc. The assumption that we want to test is known as the hypothesis test or null hypothesis, H_0. There are some well-specified test statistics to use for different kinds of tests. The p-value method has been used to check the significance of the test. The p-value is the area of the null distribution above the observed value of the test statistic, t_{obs}, and is defined as follows: $P = P(T \geq t_{obs})$. If the p-value is smaller than the level of significance, α, the hypothesis is rejected [12,21].

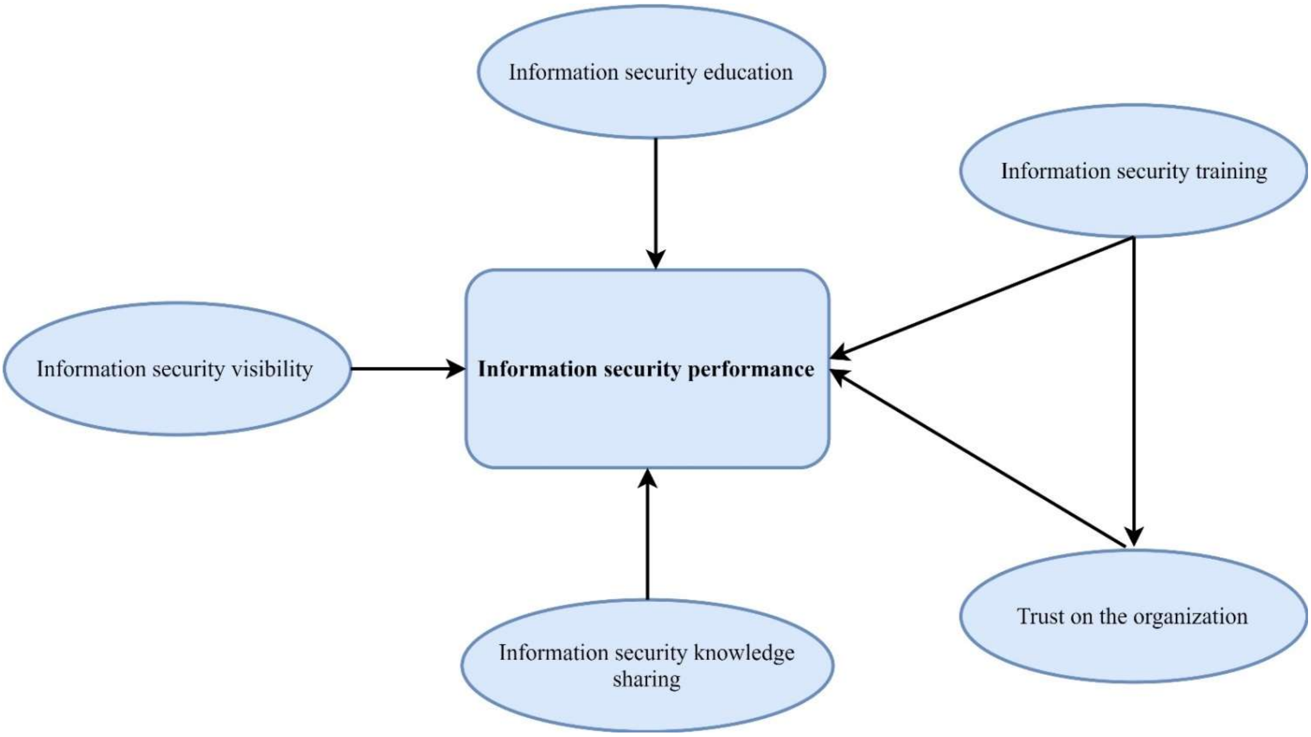
Information security education
Information security training
Information security visibility
Information security performance
Trust on the organization
Information security knowledge sharing

Figure 2. The conceptual framework.

As data and quantitative information become ubiquitous and ever more important in contemporary societies, so does statistics as a means to extract knowledge from this information. Furthermore, people not involved in analyzing data are expected to understand and, even better, critically assess statistical information on topics like political elections, economic characteristics, etc. [22,23]. The organisations selected for this study are SMEs from the United Kingdom (UK). The UK's economic freedom score is 78.4, making its economy the seventh freest in the 2021 Index (heritage.org/Index2021/). The UK is ranked third among 45 countries in the European region, and its overall score is above the regional and world averages.

The SMEs were selected in this study according to the relevance they have in the economy. Due to COVID-19, most of these organisations rely on IT for education, service, and manufacturing. There has been little research into how organisational practices affect the information security of similar companies. International organisations' reports suggest that the industrial sector is behind in implementing IT in their information security processes, and therefore, there is room for improvement.

A total of 20 SMEs were identified, and an online questionnaire was sent to participants, along with follow-up emails. The questionnaire consisted of six sections: security knowledge, security visibility, security education, training, trust in an organisation, and information security management performance. The purpose of the questionnaire was to identify the relevance and impact of company training programmes. Overall, we sent 300 questionnaires but received only 193. Of those, 171 were complete and were used for data analysis.

3.1. Information Security Knowledge Sharing

Information security knowledge sharing decreases the costs of developing new means of protection and increases the efficiency of current ones by adding to the knowledge of the potential threats [5,17,24,25]. Shared studies have covered an extensive range of security breaches, which benefits all companies. Therefore, this discussion leads to the following hypotheses:

Hypothesis 1 (H1). *Information security knowledge sharing positively correlated with the performance of information security.*

3.2. Information Security Education

The second factor—information security education—stems from these studies. Personnel with an adequate level of information security knowledge adds to a company's security. At the same time, employees who lack this training have a high chance of becoming the source of a data breach [5,12,26]. Based on this discussion, the following hypothesis is proposed:

Hypothesis 2 (H2). *Information security education positively correlated with the performance of information security.*

3.3. Information Security Visibility

Information security visibility can be a significant issue in a company with weak organisational culture and where the pressure from non-compliant peers is high [19,20]. Therefore, employees need to receive information security training [5,19]. When developing their information security systems and protocols, companies must refer to the three interconnected factors (information security knowledge sharing, education, and visibility). Thus, the following hypothesis is suggested:

Hypothesis 3 (H3). *Information security visibility positively correlated with the performance of information security.*

3.4. Information Security Training

Recent studies show that employees' training must be specific and easily accessible and followed up to check for knowledge retention [5,13,15,20,27]. Studies by Peikari et al. [28] show that "training can increase staff knowledge and awareness about the threats and consequences of a security breach, leading to the prevention of such incidents" (p. 3). However, Peikari et al. [28] state that "organisations do not usually employ security trained staff, which leads to vulnerabilities in their information security" (p. 3). Therefore, the following hypotheses are proposed:

Hypothesis 4 (H4). *Employee's training positively correlated with the trust in an organisation.*

Hypothesis 5 (H5). *Employee's training positively influences performance in information security.*

3.5. Trust in an Organisation

Trust is considered a critical requirement to increase employees intention to use any given service [27]. In the context of information security, many studies agree that trust in an organisation has a significant effect on the employees performance in information security [5,28]. According to Peikari et al. [28], there is a strong correlation between employees trust and performance in information security. Similarly, Pérez-González et al. [5] undertook an empirical study to analyse the role of trust in information security. Therefore, the following hypothesis is proposed:

Hypothesis 6 (H6). *Trust in an organisation positively correlated with employee's performance in information security.*

4. Results

The data analysis was composed of a coding process used to derive commonalities and reoccurring themes from the researcher's continual data comparison that caused new concepts to emerge after the inductive stage. The data analysis was conducted in a five-stage process. SPSS 25 Software was used to do the factor analysis followed by reliability tests for internal consistency for the items in the components. Upon satisfactory results, SPSS Amos 22.0 software was used to perform confirmatory factor analysis (CFA) to confirm the findings. Once the model was validated, the construct validity and convergent validity of the model were tested. Finally, the structural equation model (SEM) was performed to estimate the relationships between the independent and dependent variables to either accept or reject the hypothesis.

4.1. Exploratory Factor Analysis

This study adopted the Kaiser–Meyer–Oklin (KMO) and Bartlett's tests to test the suitability of data for factor analysis. The KMO value in this study was 0.912, exceeding the recommended value of 0.70, which can be considered adequate. Bartlett's test of sphericity reached statistical significance (approximately chi-square 2373.939, df 153 and Sig. 000), which signified the data were good for conducting factor analysis.

The 18 items were subjected to Principal Component Analysis (PCA) with Varimax Rotation Method Kaiser Normalisation used for factor analysis. The items with a factor loading of less than 0.50 should be eliminated [14]. However, in this study, the factor loading of all items was above 0.50, and hence, none were excluded. Therefore, all 18 items were accepted, and PCA revealed that they were grouped into six components. The total percentage of variance was 83.812. The individual dimensions of the proposed instrument explained total variance exceeding 60%, suggesting the appropriateness of the process. The results of the PCA can be viewed in Table 2 below.

Table 2. Factors extraction results of the items in the questionnaire.

Component 1	**Factor Loadings**	**Eigenvalue**	**% Variance**
SV1	0.837	9.596	53.311
SV2	0.788		
SV3	0.869		
Component 2	Factor Loadings	Eigenvalue	% Variance
ST1	0.798	1.399	7.771
ST2	0.807		
ST3	0.846		
Component 3	Factor Loadings	Eigenvalue	% Variance
SE1	0.756	1.305	7.251
SE2	0.795		
SE3	0.843		
Component 4	Factor Loadings	Eigenvalue	% Variance
KS1	0.819	1.043	5.793
KS2	0.731		
KS3	0.804		
Component 5	Factor Loadings	Eigenvalue	% Variance
TR1	0.773	0.908	5.046
TR2	0.751		
TR3	0.777		
Component 6	Factor Loadings	Eigenvalue	% Variance
SP1	0.769	0.835	4.638
SP2	0.731		
SP3	0.762		
Total percentage of variance: 83.812			

4.2. Reliability Tests

This study used Cronbach's alpha to assess the reliability, or internal consistency, of the items in the six components. The resulting α coefficient of reliability ranges from 0 to 1 in providing an overall assessment of a measure's reliability. If all scale items are independent of one another, then $\alpha = 0$; if all items have high covariance, then α will approach 1. The higher the score, the more reliable the generated scale. Hair et al. [14] has indicated that 0.7 is an acceptable reliability coefficient. As shown in Table 3, the questionnaire data were reliable and could be used for further analysis.

Table 3. The Cronbach's alpha coefficient values.

Component	Items	Cronbach's Alpha	No of Items
1	SV1, SV2, SV3	0.890	3
2	ST1, ST2, ST3	0.900	3
3	SE1, SE2, SE3	0.915	3
4	KS1, KS2, KS3	0.919	3
5	TR1, TR2, TR3	0.857	3
6	SP1, SP2, SP3	0.902	3

4.3. Confirmatory Factor Analysis

The CFA aims to explain the extent that observed variables are linked to the latent factors in the research. CFA postulates the relationships between the variables based on theory, empirical research, or both and then tests the hypothesised structure statistically. The model was developed based on a priori subject in this study, and CFA was used to confirm it. SPSS Amos 22 software was used to perform CFA. A total of 171 distinct sample moments and 51 distinct parameters were estimated. The degree of freedom (171–51) was 120 and is, therefore, positive. Thus, the model was over-identified and presented a preferable situation for analysis.

The measurement model represents the pattern in which each measure loads on a particular factor as shown in Figure 3. It shows how the measured variables come together to represent construct and is used for validation and reliability checks. As shown in Table 4, the covariance between all the latent variables was significant as the p-value was less than 0.05.

Table 4. Covariance between the latent variables.

			Estimate	SE	CR	P
ST	<–>	KS	0.683	0.115	5.913	***
ST	<–>	SE	0.659	0.117	5.632	***
ST	<–>	SV	0.590	0.113	5.228	***
ST	<–>	TR	0.759	0.128	5.912	***
ST	<–>	SP	0.658	0.106	6.211	***
KS	<–>	SE	0.792	0.125	6.359	***
KS	<–>	SV	0.612	0.115	5.338	***
KS	<–>	TR	0.793	0.131	6.044	***
KS	<–>	SP	0.728	0.111	6.560	***
SE	<–>	SV	0.686	0.121	5.644	***
SE	<–>	TR	0.917	0.140	6.559	***
SE	<–>	SP	0.749	0.113	6.611	***
SV	<–>	TR	0.642	0.126	5.076	***
SV	<–>	SP	0.628	0.107	5.867	***
TR	<–>	SP	0.777	0.121	6.424	***

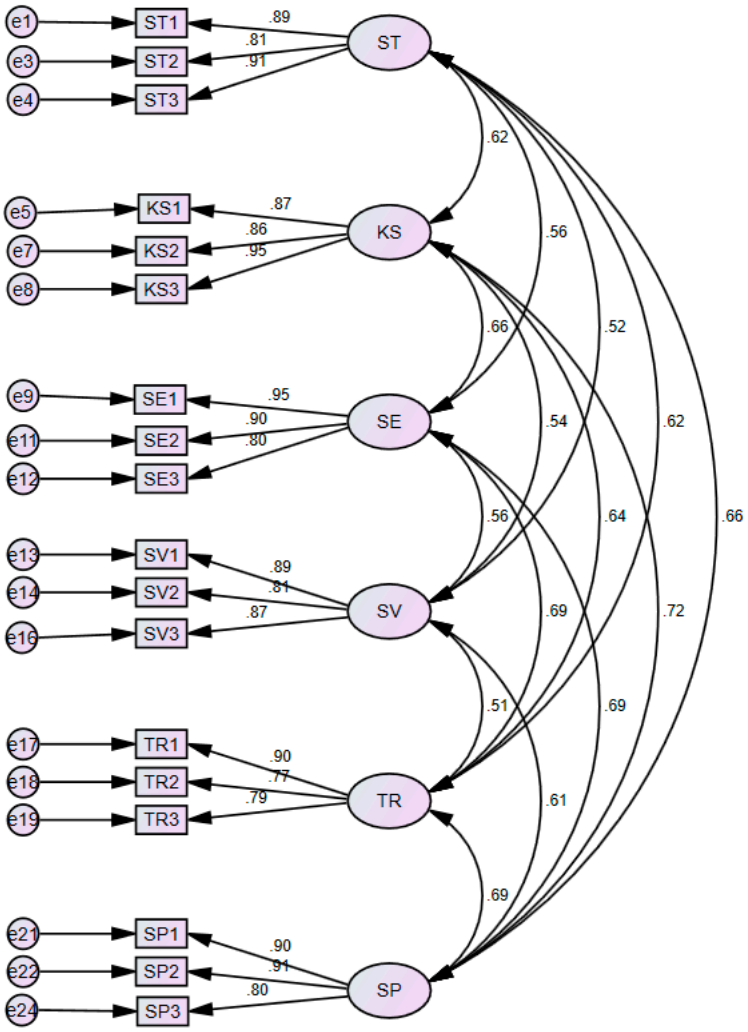

Figure 3. The measurement model.

Based on the SEM using SPSS Amos 22, we found that chi-square (CMIN) = 129.317, degree of freedom (DF) = 120, and the probability level was about 0.000, which proved that the hypothesis is significant. CMIN/DF (the minimum discrepancy) was 1.078. The following values in Table 5 were used in our study for each parameter to test model fit.

Table 5. Parameter value for model fit measures with SPSS Amos.

Name of Parameter	Value
The goodness of fit index	0.925
Comparative fit index	0.996
Root mean square error of approximation (RMSEA)	0.022

4.4. Reliability and Validity Tests

Table 6 presents the composite reliability for each variable. It shows that all variables had good composite reliability of greater than 0.7. Regarding the validity, as shown in Table 6, all the variables had average variance extracted values greater than 0.5, which indicate good convergent validity in the variables.

Table 6. Composite reliability test.

	CR Value	AVE
ST	0.903	0.757
KS	0.923	0.801
SE	0.916	0.786
SV	0.892	0.735
TR	0.862	0.676
SP	0.904	0.759

Table 7 presents the discriminant validity for each variable. This study demonstrates that the discriminant value was greater than the corresponding correlation between the variables, as there was strong discrimination between the factors in the analysis.

Table 7. Discriminant validity.

	ST	KS	SE	SV	TR	SP
ST	0.870					
KS	0.616	0.895				
SE	0.555	0.66	0.886			
SV	0.523	0.536	0.561	0.857		
TR	0.62	0.64	0.692	0.509	0.822	
SP	0.657	0.719	0.691	0.609	0.694	0.871

4.5. Structural Equation Model Path Analysis

In this study, SPSS Amos 22 software was adopted to perform path analysis using the SEM. The total distinct sample moments were 171, and the number of distinct parameters was estimated to be 49. The degrees of freedom (171–49) was 122 and, therefore, positive. Thus, the model was over-identified and presented a preferable situation for SEM. Figure 4 presents the path diagram of the model using SPSS Amos to specify the relationship between the variables. The model's portion that specifies how the variables are related to each other is called the structural model. The estimates with the largest value represent the most important dimension in their influence on dependent variables.

Table 8 highlights the results of the unstandardised regression weights estimations. The *p*-value shows the significance of the estimation. If the *p*-value is less than 0.05, then the independent variable significantly affects the dependent variable.

As presented in Table 8, all *p*-values are **** (i.e., 0.000) which are less than 0.05. Therefore, this study concluded that all factors—security training, knowledge sharing, education, and visibility—significantly impact security performance. In addition, this study highlighted the significant impact that security training and knowledge sharing have on trust in an organisation.

Based on the SEM using SPSS Amos 22, this study found that the chi-square (CMIN) = 148.862 and degree of freedom (DF) = 122. The probability level was about 0.0; CMIN/DF was 1.220. According to Bollen 22, if the minimum discrepancy is less than five, the model is a reasonable fit. Table 9 presents the values for each parameter to test model fit. The index values were greater than 0.9, and the RMSEA value was less than 0.05, indicating that the model fits and is accepted [26–29].

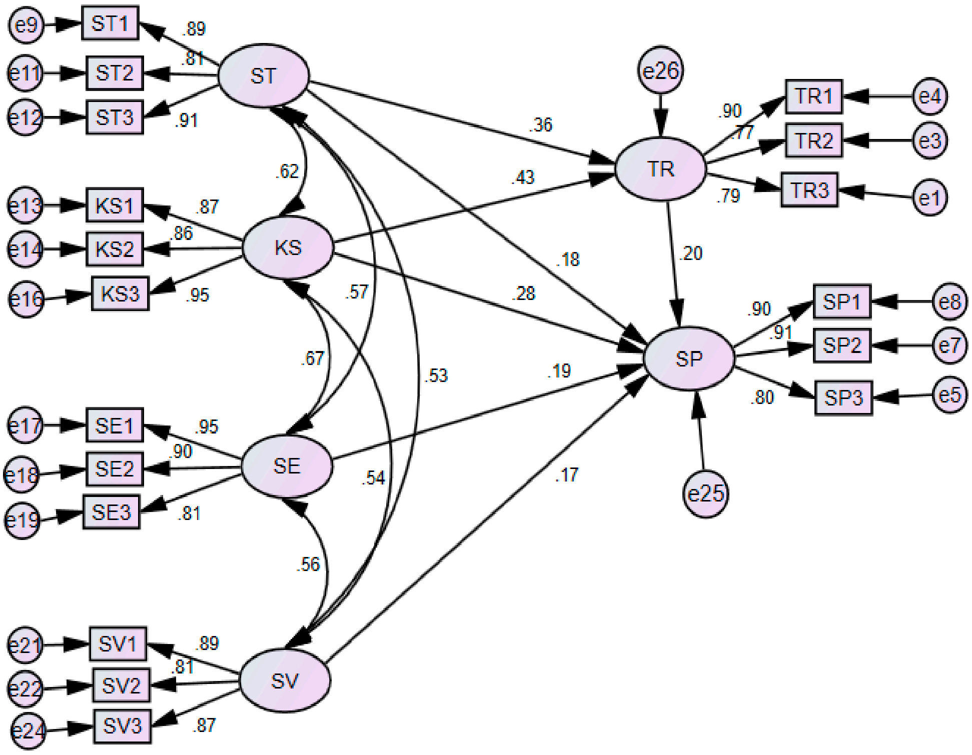

Figure 4. Structure equation model—the path diagram.

Table 8. Unstandardised regression weights estimations.

			Estimate	SE	CR	P
TR	<—	ST	0.366	0.093	3.930	***
TR	<—	KS	0.432	0.093	4.638	***
SP	<—	SV	0.131	0.059	2.227	0.026
SP	<—	SE	0.141	0.063	2.257	0.024
SP	<—	KS	0.220	0.077	2.865	0.004
SP	<—	ST	0.144	0.069	2.082	0.037
SP	<—	TR	0.156	0.070	2.228	0.026

Table 9. Parameter value for model fit measures with SPSS Amos.

Name of the Parameter	Value
Goodness of fit index	0.914
Comparative fit index	0.988
Root mean square error of approximation	0.037

5. Discussion

Over the last few years, there has been a significant increase in information security breaches in the corporate sector. Data from the Privacy Rights Clearinghouse reveals that, since 2005, there have been 788 publicly disclosed data breaches in various corporates resulting in 14.8 million records being compromised. Of these breaches, 30% were the result of human error [25,26]. Currently, there is a need to research the effects of the human aspects of information security programs and their causal effect on organizational information security performance measurement. Information security programs that enhance an organisation's overall information security performance are necessary to decrease the human error that leads to this type of information loss. This study investigated and analysed the effects of information security organisational practices (information security knowledge sharing, education, visibility, training, and trust in an organisation) on the performance of information security management in UK industrial SMEs. The findings reveal that information security knowledge sharing, training, education, and visibility significantly impact security performance. In addition, this study highlights the importance of security training and knowledge sharing on trust in an organisation.

Regarding knowledge sharing, security education, and security visibility, the results highlight their positive impact on the information security performance of SMEs. These findings support recent research such as Flores et al. [14], Soomro et al. [18], and Hwang et al. [19]. They found that these factors are effective tools in developing the information security performance of organisations.

Considering trust in an organisation, this study analysed and examined its effect on information security performance. The results show a positive relationship between these two constructs, confirming the findings of previous novel research [19]. In addition, concerning information security training, the findings of this study reveal the positive influence of security training on trust in an organisation and information security performance. This result is supported by province studies such as Parsons et al. [15], Choi et al. [20], and Pérez-González et al. [5]. Thus, information security performance in industrial SMEs is influenced positively by information security knowledge sharing, visibility, education, training, and trust in an organisation. When information security management is viewed as an inconvenience or a barrier to task completion, employees can be deterred from following security rules and policy compliance. Management can mitigate this risk by properly training their employees on the computers and data systems they operate to complete tasks. Research has shown that computer skills and level of experience can affect an employee's potential security behaviour [29,30]. Organizations need to provide employee information systems and security training that is sufficient to eliminate errors. The training should be delivered in various modalities to include classroom training, online training via web-based delivery systems and video, newsletters, posters, and fliers. An organization benefits from this variety because it allows the content to be delivered multiple times and in multiple ways. Security education must be monitored and measured regularly.

This study identifies the need for managers and decision-makers to consider the role of employees in information security and are, therefore, highly relevant. Managers can influence their employees' motivation levels, loyalty, and innovative risk-taking to create a trustworthy relationship in the organization. A strong tool for a manager to be an influencer is to have a trustful relationship with employees. Such initiatives positively affect information security management performance also an organization's profitability. A good manager, through employee's and organizational trust, may achieve organizational goals. Information security training is another aspect to improve the information security measurement performance that emerged from our study.

Furthermore, training workshops are essential to the organization seeking a competitive advantage through a highly skilled and flexible workforce. An effective training strategy enables employees to be confident in using new technologies and provides progressive adjustment to change in information security. Continuous training is required to review and update the knowledge and skills of employees, as it makes them functionally effective in their information security management performance. Policymakers should arrange training sessions for employees to improve information security measurement. Emphasizing the roles and responsibilities of the employees provides a personalization to compliance and promotes ownership. Personalization gives the employee an active role in compliance and mitigates the restrictive connotation. The policies should be easily accessible, reviewed periodically, and apply to all members, partners, and agents of the organization. It is organizational management's responsibility to support the information security management policy construction process. Therefore, management must make sure that employees fully understand the policies and favourably perceive them. Additionally, organizational management must take an active role in motivating their employees towards policy compliance. Employees are often the source of unintentional data breaches, and their training in information security needs to be a priority as highlighted by this study.

The findings from our study could be useful to enhance information security measurement performance if the organization promotes healthy working relationships that assist managers in facilitating organizational changes. Employees are more susceptible to accepting directives by a manager if they trust them. This allows leadership to motivate the employees to commit to organizational goals and changes willingly. The existence of trust by the employee is viewed as a positive moderator to mitigate hesitation by the employee. The findings were limited to the interpretation of this investigator and could have a different meaning to other researchers. The scientific method of data collection and data analysis called for by the chosen research methodology reduces bias by substantiating concepts with the emerged data. Although the findings from this study were composed of narratives from both men and women who were employed in different industries, the participation was limited to organizational professionals referred to as white-collar workers. These workers were specialists in their roles who practised administrative and strategic tasks.

In comparison, wage-earning workers, known as blue-collar workers, practice manual labour. Because only white-collar workers were filled the questionnaire, the data were limited; the perceptions of the blue-collar workers were not collected. Further research that included blue-collar workers might provide another way to view trust or determine whether the same levels of trust can be found between blue- and white-collar workers who work in the same organizations.

6. Conclusions

The human factor has been shown to be the most critical in information security. This is due to the employee role in data breaches and policy compliance. This study aimed to examine and analyse the influence of organisational practices on information security performance. The majority of the existing studies have focused mainly on the technical aspects of information security with limited consideration to organisational processes. Thus, we aimed to address this research gap by examining and analysing the relationship between organisational factors and information security performance. In terms of practical implications, this study's findings present important considerations for managers and policymakers regarding organisational factors that develop and enhance employee information security performance. Therefore, an emphasis must be placed on information security performance based on their effectiveness in strengthening employees' security aptitude and behaviour. A sound information security performance measurement demonstrates an organization's overall attitude towards information security and compliance. Therefore, it should be treated with the same level of importance as the strategic plan and with the same level of investment as any technical security control.

Despite its merits, this research has limitations. This study considered organisational practices and their impact on information security performance. However, other aspects need consideration, such as employees' commitment, culture, and loyalty. Thus, future research could focus on such factors to understand all factors that influence information security performance.

Author Contributions: Data curation, K.P.S.; Formal analysis, L.A.; Investigation, L.A. and K.P.S.; Methodology, L.A. Both authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data of the underlying article will be shared at reasonable request to the corresponding authors.

Acknowledgments: The authors thank Brunel University London and particularly the study participants. They also gratefully acknowledge Taif University, as this study is supported by Taif University Researchers Supporting Project Number TURSP-2020/186, Taif University, Taif, Saudi Arabia.

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

References

1. Diesch, R.; Pfaff, M.; Krcmar, H. A comprehensive model of information security factors for decision-makers. *Comput. Secur.* **2020**, *92*, 101747. [CrossRef]
2. Doherty, N.F.; Tajuddin, S.T. Towards a user-centric theory of value-driven information security compliance. *Inf. Technol. People* **2018**, *31*, 348–367. [CrossRef]
3. Fonseca-Herrera, O.A.; Rojas, A.E.; Florez, H. A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard. *IAENG Int. J. Comput. Sci.* **2021**, *48*, IJCS_48_2_01.
4. Kobis, P. Human factor aspects in information security management in the traditional IT and cloud computing models. *Oper. Res. Decis.* **2021**, *1*, 61–76.
5. Pérez-González, D.; Preciado, S.T.; Solana-Gonzalez, P. Organizational practices as antecedents of the information security management performance: An empirical investigation. *Inf. Technol. People* **2019**, *32*, 1262–1275. [CrossRef]
6. Safa, N.S.; Von Solms, R. An information security knowledge sharing model in organizations. *Comput. Hum. Behav.* **2016**, *57*, 442–451. [CrossRef]
7. Hwang, I.; Kim, D.; Kim, T.; Kim, S. Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Inf. Rev.* **2017**. Available online: https://www.emerald.com/insight/content/doi/10.1108/OIR-11-2015-0358/full/html (accessed on 16 September 2021). [CrossRef]
8. Miladinović, V.T. Development of Awareness and Competences of Employees in the Processes of Information Security Management System: Guidelines for practical application. *JITA-J. Inf. Technol. Appl.* **2020**, *20*, 87–95.
9. Putra, I.M.M.; Mutijarsa, K. Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005. In Proceedings of the 2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT), Surabaya, Indonesia, 9–11 April 2021; pp. 14–19.
10. Siponen, M.; Pahnila, S.; Mahmood, M.A. Compliance with information security policies: An empirical investigation. *Computer* **2010**, *43*, 64–71. [CrossRef]
11. Marelli, L.; Lievevrouw, E.; Van Hoyweghen, I. Fit for purpose? The GDPR and the governance of European digital health. *Policy Stud.* **2020**, *41*, 447–467. [CrossRef]
12. Ma, Q.; Schmidt, M.B.; Pearson, J.M. An Integrated Framework for Information Security Management. *Rev. Bus.* **2009**, *30*, 58–69.
13. Rocha Flores, W.; Antonsen, E.; Ekstedt, M. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Comput. Secur.* **2014**, *43*, 90–110. [CrossRef]
14. 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]
15. Singh, A.N.; Gupta, M.; Ojha, A. Identifying factors of "organizational information security management". *J. Enterp. Inf. Manag.* **2014**, *27*, 644–667. [CrossRef]
16. Soomro, Z.A.; Shah, M.H.; Ahmed, J. Information security management needs more holistic approach: A literature review. *Int. J. Inf. Manag.* **2016**, *36*, 215–225. [CrossRef]
17. Choi, S.; Martins, J.T.; Bernik, I. Information security: Listening to the perspective of organisational insiders. *J. Inf. Sci.* **2018**, *44*, 752–767. [CrossRef]
18. Moody, G.D.; Siponen, M.; Pahnila, S. Toward a unified model of information security policy compliance. *MIS Q.* **2018**, *42*, 285–311. [CrossRef]
19. Hwang, I.; Cha, O. Examining technostress creators and role stress as potential threats to employees' information security compliance. *Comput. Hum. Behav.* **2018**, *81*, 282–293. [CrossRef]
20. Shaukat, K.; Alam, T.M.; Luo, S.; Shabbir, S.; Hameed, I.A.; Li, J.; Abbas, S.K.; Javed, U. A review of time-series anomaly detection techniques: A step to future perspectives. In Proceedings of the Future of Information and Communication Conference, Vancouver, BC, Canada, 29–30 April 2021; pp. 865–877.
21. Shaukat, K.; Luo, S.; Chen, S.; Liu, D. Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective. In Proceedings of the 2020 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, 20–21 October 2020; pp. 1–6.
22. Shaukat, K.; Luo, S.; Varadharajan, V.; Hameed, I.A.; Chen, S.; Liu, D.; Li, J. Performance comparison and current challenges of using machine learning techniques in cybersecurity. *Energies* **2020**, *13*, 2509. [CrossRef]
23. Mamonov, S.; Benbunan-Fich, R. The impact of information security threat awareness on privacy-protective behaviors. *Comput. Hum. Behav.* **2018**, *83*, 32–44. [CrossRef]
24. Willison, R.; Warkentin, M. Beyond deterrence: An expanded view of employee computer abuse. *MIS Q.* **2013**, *37*, 1–20. [CrossRef]
25. Peikari, H.R.; Ramayah, T.; Shah, M.H.; Lo, M.C. Patients' perception of the information security management in health centers: The role of organizational and human factors. *BMC Med Inform. Decis. Mak.* **2018**, *18*, 102. [CrossRef] [PubMed]
26. Bentler, P.M. Comparative fit indexes in structural models. *Psychol. Bull.* **1990**, *107*, 238. [CrossRef] [PubMed]
27. Bentler, P.M.; Bonett, D.G. Significance tests and goodness of fit in the analysis of covariance structures. *Psychol. Bull.* **1980**, *88*, 588. [CrossRef]

28. Bollen, K.A. *Structural Equations with latent Variables*; John Wiley & Sons: New York, NY, USA, 1989; p. 210. Available online: https://www.wiley.com/en-ca/Structural+Equations+with+Latent+Variables-p-9780471011712 (accessed on 16 September 2021).
29. Qu, X. *Multivariate Data Analysis*; Taylor & Francis: London, UK, 2007; Available online: https://www.tandfonline.com/doi/abs/10.1198/tech.2007.s455 (accessed on 16 September 2021).
30. Shaukat, K.; Luo, S.; Varadharajan, V.; Hameed, I.A.; Xu, M. A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. *IEEE Access* **2020**, *8*, 222310–222354. [CrossRef]