Factors Impacting Users' Compliance with Information Security Policies: An Empirical Study

Latifa Alzahrani
Department of Management Information Systems
College of Business Administration, Taif University, Saudi Arabia

***Abstract*—One of the main concerns for organizations in today's connected world is to find out how employees follow the information security policy (ISP), as the internal employee has been identified as the weakest link in all breaches of the security policies. Several studies have examined ISP compliance from a dissuasive perspective; however, the results were mixed. This empirical study analyses the impact of organisational security factors and individual non-compliance on users' intentions toward information security policies. A research model and hypotheses have been developed in this quantitative study. Data from 352 participants was collected through a questionnaire, which then validated the measurement model. The findings revealed that while security system anxiety and non-compliant peer behaviours negatively impact users' compliance intentions, work impediments positively influence these intentions. Security visibility negatively influences users' non-compliance, and security education systems positively impact work impediments. This research will help information security managers address the problem of information security compliance because it provides them with an understanding of one of the many factors underlying employee compliance behaviors.**

Keywords*—Information security; users' compliance; compliance factors; security education systems; information security policies

I. Introduction

The COVID-19 pandemic raised a crucial technical issue within many organisations due to a lack of relevant information security protocols [1]. Information security is the process and controls put in place to guarantee data access is protected for reading by authorized personnel only, writing by authorized personnel only, and its readiness is protected when needed by authorized parties, etc. According to Miller [2], even before the virus outbreak, IT threats against organisations increased by 35% in the fourth quarter of 2019 compared to the fourth quarter of 2018. The necessity to transfer IT, users, to remote workplaces opened up a new set of vulnerabilities quickly identified by hackers and scammers who took advantage of the situation [2]. Although the US's Cybersecurity and Infrastructure Security Agency advised preventing cyber-attacks, the need for effective and advanced information security measures remains .Information security is defined as a set of processes and policies that protect information from unauthorised access [3]. There is a significant requirement to analyse the actions of organisations related to higher information security standards (ISS) and protective measures. Now more than ever, during the COVID-19 pandemic, companies' most valuable assets consist of digital data, which puts them at risk of a set of threats from both inside and outside actors [4]. Any organisation needs to implement strategies to prevent commercial data leaks to their competitors and protect their users' privacy [5]. With an ever-expanding set of information technologies, organisations must explore all possible ways to leak information .The COVID-19 pandemic has caused rapid transformation and increased IT in most organisations in many sectors, including education [6], healthcare [7, 8], business [9], and economics [10]. This recent development has considerably changed critical resources and assets. It is vital to ensure that no information is unintentionally disclosed or altered [11, 12]. To shield resources and safeguard organisations' important data from existing threats, progressive information security plans must be developed to list inappropriate and appropriate ISS activities for IT operators [13]. Information security is a complex issue due to its multidisciplinary nature involving organisational, behavioural, and technical aspects [5, 14, 15] and a holistic method is necessary for information security management (ISM) [16, 17]. Also, Siponen et al. [13] recommended that information security matters be regarded from a management perspective.

Existing studies have indicated that even though scholars in the computer science field have investigated the significant phenomenon of information security [18], most have evaluated the subject from an engineering viewpoint. These researchers have concentrated on expanding technical solutions with limited consideration of security from a behavioural perspective [19]. The existing literature has highlighted that many organisations fail to properly link information security with threats beyond outside IT-related breaches by not taking human error into account. According to Choi et al. [3], "organisations increasingly focus on implementing information security products such as anti-virus, intrusion detection, and prevention systems, total personal computer (PC) security, database/contents security, total security systems and public key infrastructure". It has also been noted that the concept of information security requires a strategy that focuses on different organisational aspects, including structured actions, policy, and governance, to protect organisations' information assets. Governance in an organizational context is the development of a management framework to strategically drive the business processes and support compliance with regulations. Governance is planning for effective management, where management is the application of operational decisions. Information security policies are a necessity for business survival in the new digital world; its main goals are to protect confidentiality, integrity and availability, and it has an essential role in today's organizations. Information security policies

standards are core fundamentals that control the arrangements of information systems. There are multiple standards for addressing information security policies in organizations (COBIT, ISO 27001/2, etc.), and combinations of multiple standards that can help organizations define roles and govern information security. However, the different aspects of information security, such as economic, financial and management are complements to the technical side and not substitutes.

Despite this apparent necessity, Pérez-González et al. [20] observed that the lack of internal protection results in more negative impacts and losses than the security threats posed by outsiders. Pérez-González et al. [20] also stated that "government programs and grants to help companies improve information security focus on supporting companies in purchasing hardware and software technology solutions, without paying attention to organisational issues". Thus, this study aims to fill the gap between the technical measures of information security and companies' information security policies for users. Recent research in information security has required the consideration of diverse perspectives by analysing both its technical characteristics and organisational variables and then examining issues linked to conformance with information security principles. It also entails developing systems and information security management models and scrutinising certification procedures [21, 22]. These actions are significant because they must focus on information security related to business procedures and the overall contemplation of information security. The development of information security procedures must begin from the strategic level before advancing to other aspects of an organisation [21-24]. Information Security management roles can be defined as follows:

- Defining security roles, responsibilities and applications: relevant when discussing the accountability of users to specific information security occurrences within organizations.
- Defining goals for security: goals should be built using the business model and defined needs. The classification of systems and data could also come into play when defining the security goals; different organizations with different data will have different security goals.
- Strategies for Security: strategies should comply with business needs. This comes to play when planning the future of business services and legal/regulatory compliance.
- Risk assessment and management: especially useful when policies are being developed, it helps in defining and taking ownership of risks to later define the controls to avoid, mitigate/control, accept or transfer the risks. Risk assessment and controls definition are also highly connected to the asset classification.
- Resource management for security: defining the ISG structure needed is important for running safe operations, achieve information security goals, monitor the security status and respond to threats.
- Compliance with regulations and rules: organizations need to comply with regulations to be able to run their business; compliance is needed to ensure the correct security measures and responsibilities are implemented. Investor relations and communications activity (in relation to security goals).

Consequently, it is particularly significant to recognise the organisational aspects that relate to information security. The mechanisms that categorise the organisational features that may impact information security are modern in their approach. These mechanisms differ in methodology and primarily use theoretical approaches, as well as case studies. They also differ in terms of units of inquiry and present an extensive diversity of elements; thus, it is critical to developing this topic by examining the impacts of these mechanisms on information security organisations.

II. Related Work

Information security policies are a prime component of almost every modern organization. Information security is a key component of such organizations, and the governance of information security enables organizations to add value to products and services, reduce costs and meet customer requirements. Information security products and technologies cannot defend an organization without the appropriate strategies and policies. Organizational aspects have a direct impact on the behaviour and efficiency of information security policies. However, it is confirmed, but repeatedly forgotten, that security is not principally a technical matter but a management or business issue. Different challenges for information security management are also detailed in von Solms and von Solms [25].

There are different organizational issues that challenge information security management in organizations. For example, Ashenden and Sasse [26] discuss the struggles that Chief Information Security Officers (CISO) face as representative of organizational information security management when dealing with organizational issues. The research focuses on management issues in the context of information security and investigates the factors that most influence CISO success in an organization: enabling or disabling a healthy information security management status through business strategy and compliance, marketing, employees' engagement, CISO identity in the organization, lack of confidence, effectiveness evaluation, organizational structure, and social responsibility. They also emphasized organizational behaviour, where they prove that employee's reaction to information security management is positive when well informed and educated; however, this cannot always be true because human behaviour cannot be controlled or predicted. They also indicated that autocratic attitude in an organization is highly damaging to the CISO role and is one of the biggest obstacles [27].

There are many other organizational issues that impact information security management in modern organizations that present serious challenges to the information security status. Information technology and information security's strategic alignment with business objectives is one that is well documented in the literature. Chang et al. [28] established its

importance by stating that IT systems become more adopted for core modern enterprise activities. Doing so would stablize systems and smooth operations, enabling better performance. The alignment of the business with IT is also important for external business changes and the introduction of new challenges and business opportunities. That is, rapid technological development can introduce new threats and vulnerabilities to data. The size of the organization is another factor that is documented in the literature to have an impact on the ISM status. Ghobakhloo et al., [29] discuss that organizational size has positive relationship to technological innovation and technology implementation, stating that larger organizations usually have better human, technological and financial resources to better utilize information systems; they are also able to handle information security better with better resources, expertise, and training. In addition, Horvath et al., [30] found that vendors are more willing to cooperate with larger organizations. Industry type has long been used by researchers to investigate quality assurance, information and change management, and using IT systems for competitive behaviour. Johnston et al., found large variations in information security related behaviour in organizations whose type of industry relied more on information security. Hasbini et al., [31] also concluded that financial organizations needed more information security to drive business, and therefore such would have an impact on ISM efforts. IT competencies enable an organization to plan, execute and invest in information security effectively. Various researchers have highlighted the importance of a shared management of IT and ISM between IT professionals and business managers in an organization. While there are a number of researchers who addressed the organizational factors that impact information security management in modern organizations and how these could be developed and maintained, there are few researches focusing on exploring these factors in information security policies. This is an important absence because information security policies are different from information security management. Therefore, such a gap needs to be filled for a better understanding of how organizations can (or should) plan to deal with future information security policies issues.

III. Research Methodology

A. Data Collection and Sample

The data was gathered from an educational organisation in Saudi Arabia that had been transformed into an e-learning system during the COVID-19 pandemic. Our study used questionnaires to collect data because this method is appropriate for testing both reliability and validity. The study included approximately 400 respondents. Forty-eight incomplete questionnaires were rejected from the collected replies, leaving 352 fully completed questionnaires for analysis. Of these 352 responses, only usable responses were included and converted into an appropriate sample size. Analysis using AMOS was performed to conduct structural equation modelling (SEM), which assessed the proposed model and the final path prototype.

B. Study Instrument

The constructs used in the questionnaire. The survey included a total of 23 items to evaluate the six constructs. All the questions were obtained from preceding studies and incorporated into the research to make them more relatable and logical. Each question that the authors derived from previous studies were altered and attuned to the research framework .A five-point Likert scale has been employed to measure the constructs in the questionnaire, which ranged from “strongly agree” to “strongly disagree”. The respondents were required to select the level that most applied to them while considering each item. The respondents were also asked to provide demographic information.

C. Pre-testing the Questionnaire

A complex pilot phase and pre-tests of the procedure were initiated, during which particular e-learning experts and users were consulted. The authors employed 10% of the entire sample size for the pilot study. Selecting the sample size was undertaken with consideration of average research performance. All the questions used in the survey were pre-tested. Forty randomly identified students took part in the pre-testing exercise. The study’s dependability was established using Cronbach’s alpha; the alpha values of all variables surpassed 0.7. Consequently, this study’s questionnaire was highly reliable. The entire group of respondents conceptualised the final questionnaire to increase the overall survey quality and its reliability.

D. Students’ Demographic Data

Table I presents the survey respondents’ demographic information; most (approximately 83%) were aged 18–25 years old. The percentage of females (56%) was higher than that of males (44%). Lastly, in terms of internet experience, the highest percentage (52.4%) of respondents had 6–10 years’ experience, followed by 29.1% with 1–5 years.

TABLE I. Demographic Information

Variable	Group	Percentage
Age	18–25 years old	83.0
	26–30 years old	14.0
	31–35 years old	3.0
	36–40 years old	0
	Total	100.0
Gender	Male	44.0
	Female	56.0
	Total	100.0
Years of Internet Experience	1–5 years	29.1%
	6–10 years	52.4%
	11–20 years	17.3%
	More than 20 years	1.2%
	Total	100.0

Based on a review of the extant literature, the proposed research model was developed considering both the organisational and individual security factors necessary to reduce the non-compliance of IT users. According to Hwang et al. [5], organisational factors comprise "security systems, security education, and security visibility". In contrast, individual security factors include the impairment of workflow and peers' negative attitudes towards information security and security system anxiety. In addition, the non-compliance of IT users is an antecedent of increasing the intention to comply with security policy. Fig. 1 illustrates the proposed research model and hypotheses, and the following subsections provide further details on each construct.

E. Security Education Systems

Organisational factors are major reasons for unintended data exposure due to inadequate security policies and technologies. Ideally, an educational institution should implement a security system that will prevent external attempts to gain unlawful access to information and simultaneously prevent employees from sharing this information [5, 32]. A recent study by Pérez-González et al. [20] demonstrated that students' lack of education about information security standards is a significant source of unintentional data leaks. Hwang et al. [5] also highlighted that it is the responsibility of educational organisations to educate their students about data security as any person with access to the organisation's internal network can be a potential threat. The integrity of a security education system affects all levels of individual compliance; an easy-to-use system reduces employees' anxiety when interacting with it. Based on this, the first hypotheses were developed as follows:

H1. Security education systems negatively influence work impediments.

H2. Security education systems negatively influence security system anxiety.

H3 Security education systems negatively influence non-compliance behaviours.

F. Information Security Visibility

Another major factor is the visibility of security measures, continuously advertised to remain at the top of students' priorities. Information security visibility refers to the degree that an organisation informs its members about its information security policies [5]. Given these factors, the efforts of each organisation play a crucial role in protecting itself against data breaches. Accordingly, this study proposed the following further hypotheses:

H4. Security visibility negatively influences work impediments.

H5. Security visibility negatively influences security system anxiety.

H6. Security visibility negatively influences non-compliance behaviours.

G. Work Impediments

In terms of individual non-compliance factors, users may ignore specific security policies when completing their tasks due to their unwieldiness. Work impediments are the adverse impacts of implemented security measures on task completion [5]. Other sources of work impediments can stem from insufficient training or data protection policies. As such, this study proposed the following hypothesis:

H7: Work impediments negatively influence users' compliance intention.

H8: Work impediments negatively influence system anxiety.

H. Security System Anxiety

Security system anxiety may derive from a user's unwillingness to report security incidents due to the fear of punishment. Moreover, such anxiety can materialise due to the complexity of information security systems or users' lack of understanding of their functions [5]. Therefore, this led to the following hypothesis:

H9: Security system anxiety negatively influences users' compliance intention.

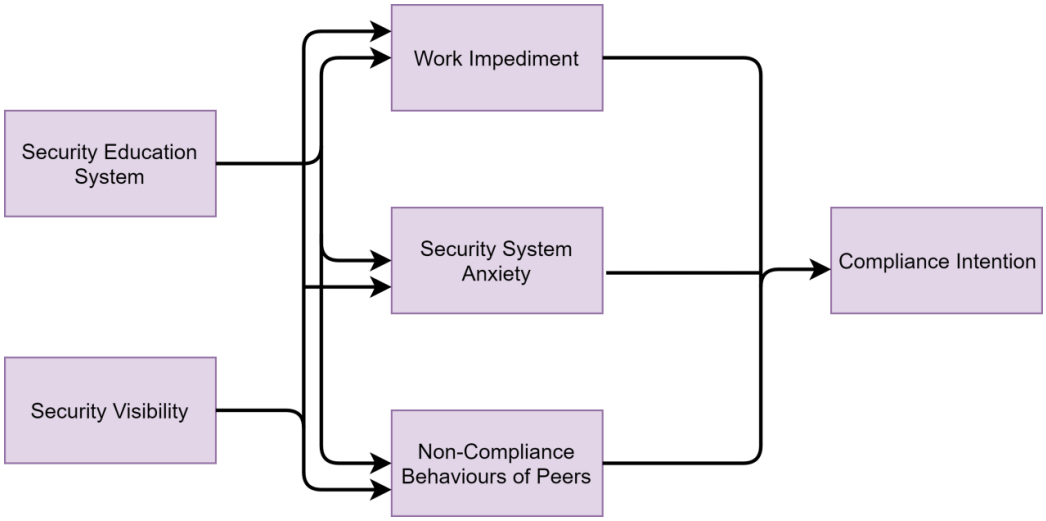

Fig. 1. Proposed Research Model.

I. Non-Compliant Peer Behaviours

The third primary source of non-compliance behaviours is social pressure from others. According to Hwang et al. [5], users' behaviour is affected by peer pressure, including the collective attitude towards information security. Students feel more confident following security instructions when they observe their peers doing the same. Therefore, an institution needs to assess the organisational culture to identify such issues. Accordingly, the present study proposed the following hypothesis:

H10: The non-compliance of peers negatively influences user' compliance.

H11: The non-compliance of peers negatively influences work impediments.

IV. Results

The data analysis was conducted in four steps. First, factor analysis of the collected data was conducted to determine the relationships between the variables. After that, confirmatory factor analysis was performed to confirm the findings. Reliability and validity testing were conducted on the model, followed by SEM. SPSS Statistics 25.0 software was used for factor analysis. SPSS AMOS 22.0 software was used to test the CFA model fit and SEM to estimate the relationships between the independent variables and the dependent variable to accept or reject the proposed hypotheses.

A. Exploratory Factor Analysis

The Kaiser-Meyer-Oklin (KMO) and Bartlett's tests were used to check the suitability of the data for factor analysis. The KMO value was 0.844, exceeding the recommended value of 0.70, and, thus, was considered adequate [33, 34]. Bartlett's test of sphericity reached statistical significance (approximate chi-square 5440.263, df 253 and Sig 0.000), signifying that the data was appropriate for factor analysis. The 23 items were subjected to principal component analysis (PCA), and Varimax Rotation with Kaiser Normalization was used for factor analysis. Any items with a factor loading less than 0.50 were eliminated; however, the factor loadings for each item in the present study's questionnaire were above 0.50, suggesting that the data set was appropriate [35, 36]. Consequently, all 23 items were accepted, and PCA revealed that they were grouped into six components with Eigenvalues exceeding 1 (Table II). The total percentage of variance was 76.825. The individual dimensions of the proposed instrument explained the total variance as exceeding 76%, suggesting the suitability of the process.

B. Confirmatory Factor Analysis

CFA explains the extent to which observed variables are linked to latent factors in a study. CFA postulates the relationships between variables based on theory, empirical research, or both and then statistically tests the hypothesised structure. The present study developed the model based on a priori knowledge, and CFA was used to confirm it, as shown in Fig. 2. The measurement model represents the pattern in which each measure loads on a particular factor. It demonstrates how the measured variables come together to represent the constructs and is used for validation and reliability testing. The covariance between all the latent variables was significant as the P-value was less than 0.05 (Table III).

TABLE II. Factor Extraction Results of Questionnaire Items

Item No.	**Component**	**Eigenvalue**
Security System and Security Education		6.999
Sys1	0.755	
Sys2	0.759	
Sys3	0.720	
Edu1	0.774	
Edu2	0.819	
Edu3	0.791	
Edu4	0.802	
Edu5	0.821	
Security Visibility	Component	Eigenvalue
Vis1	0.909	4.835
Vis2	0.904	
Work Impediment	Component	Eigenvalue
Imp3	0.808	1.989
Imp4	0.841	
Security System Anxiety	Component	Eigenvalue
Anx1	0.708	1.649
Anx2	0.878	
Anx3	0.882	
Anx4	0.768	
Non-Compliance Behaviour of Peers	Component	Eigenvalue
Peer1	0.845	1.186
Peer2	0.831	
Peer3	0.741	
Compliance Intention	Component	Eigenvalue
Int1	0.840	1.011
Int2	0.846	
Int3	0.911	
Int4	0.894	
Total Variance Explained: 76.825		

TABLE III. Covariance between Latent Variables

			Estimate	**S.E.**	**C.R.**	**P**
Edusys	<-->	Int	0.172	0.025	6.934	***
Edusys	<-->	Anx	-0.060	0.027	-2.178	0.029
Edusys	<-->	Peer	-0.050	0.024	-2.094	0.036
Edusys	<-->	Vis	0.006	0.028	0.200	0.841
Edusys	<-->	Imp	0.065	0.029	2.256	0.024
Int	<-->	Anx	-0.087	0.034	-2.538	0.011
Int	<-->	Peer	-0.064	0.030	-2.149	0.032
Int	<-->	Vis	0.033	0.035	0.948	0.343
Int	<-->	Imp	0.053	0.036	1.481	0.139
Anx	<-->	Peer	0.443	0.054	8.207	***
Anx	<-->	Vis	-0.236	0.052	-4.487	***
Anx	<-->	Imp	0.244	0.051	4.797	***
Peer	<-->	Vis	-0.229	0.046	-4.981	***
Peer	<-->	Imp	0.203	0.043	4.680	***
Vis	<-->	Imp	-0.337	0.058	-5.838	***

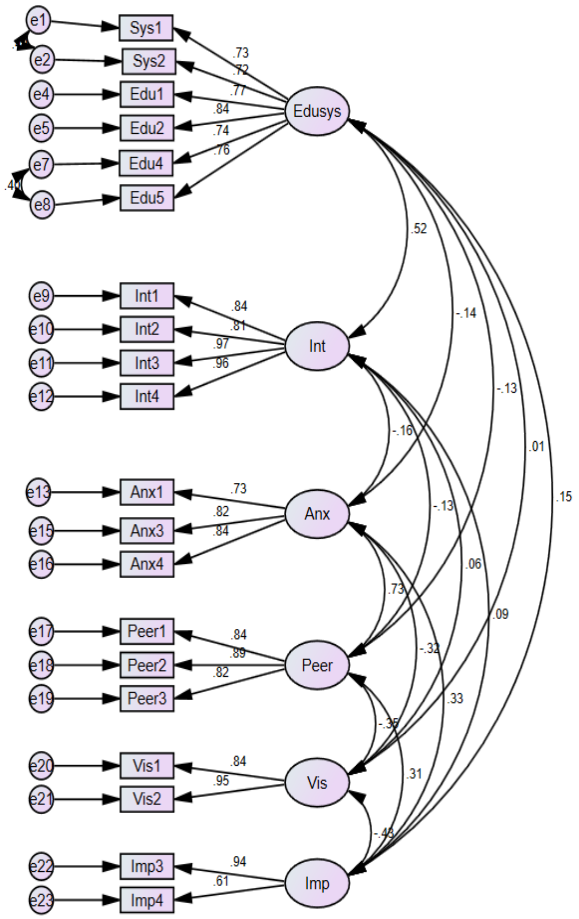

Fig. 2. The Results of Confirmatory Factor Analysis.

There was a high positive correlation of 0.733 between the security system anxiety and peer behaviour variables, followed by security systems and security education and work impediments at 0.522. The correlations between the other variables are shown in Table IV.

TABLE IV. CORRELATION BETWEEN LATENT VARIABLES

			Estimate
Edusys	<-->	Int	0.522
Edusys	<-->	Anx	-0.145
Edusys	<-->	Peer	-0.135
Edusys	<-->	Vis	0.012
Edusys	<-->	Imp	0.146
Int	<-->	Anx	-0.161
Int	<-->	Peer	-0.131
Int	<-->	Vis	0.057
Int	<-->	Imp	0.090
Anx	<-->	Peer	0.733
Anx	<-->	Vis	-0.322
Anx	<-->	Imp	0.335
Peer	<-->	Vis	-0.351
Peer	<-->	Imp	0.311
Vis	<-->	Imp	-0.426

SEM showed that chi-square (CMIN) = 350.635, degree of freedom (DF) = 153, and the probability level was approximately 0.000, evidence that the null hypothesis was not significant at the 0.05 level. CMIN/DF represents the minimum discrepancy, which was 2.292; according to Wheaton et al. [37], a model has a reasonable fit if the minimum discrepancy is less than 5.

Table V shows the values found for each parameter to test the model's fit. In various studies conducted by Bentler and Bonett [38], Jöreskog and Sörbom [39], Bollen's and Bentler [38], it has been suggested that if the index value is greater than 0.9 and if the RMSEA value is less than 0.08, the model has a good fit.

TABLE V. PARAMETER VALUES FOR MODEL FIT

Parameter	**Value**
Goodness of Fit Index (GFI)	0.906
Comparative Fit Index (CFI)	0.955
Root Mean Square Error of Approximation (RMSEA)	0.064

C. Reliability and Validity Tests

All the variables had composite reliability greater than 0.7 (Table VI), which indicated good reliability.

TABLE VI. COMPOSITE RELIABILITY TEST

	CR
Edusys	0.893
Int	0.943
Anx	0.839
Peer	0.888
Vis	0.892
Imp	0.761

All the variables had a convergent validity greater than 0.5 (Table VII), indicating good convergent validity.

TABLE VII. CONVERGENT VALIDITY

	AVE
Edusys	0.582
Int	0.805
Anx	0.635
Peer	0.725
Vis	0.805
Imp	0.624

The discriminant value was greater than the corresponding correlation between the variables, indicating good discrimination between the factors in the analysis (see Table VIII).

D. Structural Equation Modelling

SPSS AMOS 22 software was used to perform CFA via SEM. The model was over-identified, which is a preferable situation for SEM. The path diagram in Fig. 3 specifies the relationship between the observed variables. The model's portion that specifies how the variables are related is

represented by the structural model; the estimates with the largest values represent the most important dimensions in terms of their influence on dependent variables. The findings of the regression weight estimates are summarised in Table IX. P-values demonstrate the significance of estimation: if the P-value is less than 0.05, then the independent variable has a significant effect on the dependent variable (P-values with *** indicate 0.000). All the impacts were significant except for information security visibility acting on security system anxiety, which did not significantly impact as the p-value was 0.036 (i.e. less than 0.05). Table X presents the results of standardised regression weight estimates.

Table X highlights that both the security education system and system visibility had a significant negative impact on peers' non-compliant behaviour. In addition, this study highlights that both the security education system and peer' non-compliant behaviour had significant positive impacts on work impediments. In contrast, the system's visibility had a significant negative impact on it. Considering the factors influencing system anxiety, this study highlights that the security education system had a significant negative impact on security system anxiety. In contrast, the work impediments had a significant positive impact of 0.995 on security system anxiety. However, system visibility had no significant impact on security system anxiety. Finally, regarding the compliance intention, the findings of this research present that both security system anxiety and peer' non-compliant behaviour had a significant negative impact on compliance intention. In contrast, work impediments had a significant positive impact on compliance intention.

TABLE VIII. DISCRIMINANT VALIDITY

	Edusys	**Int**	**Anx**	**Peer**	**Vis**	**Imp**
Edusys	0.763					
Int	0.522	0.897				
Anx	-0.145	-0.161	0.797			
Peer	-0.135	-0.131	0.733	0.851		
Vis	0.012	0.057	-0.322	-0.351	0.897	
Imp	0.146	0.09	0.335	0.311	-0.426	0.790

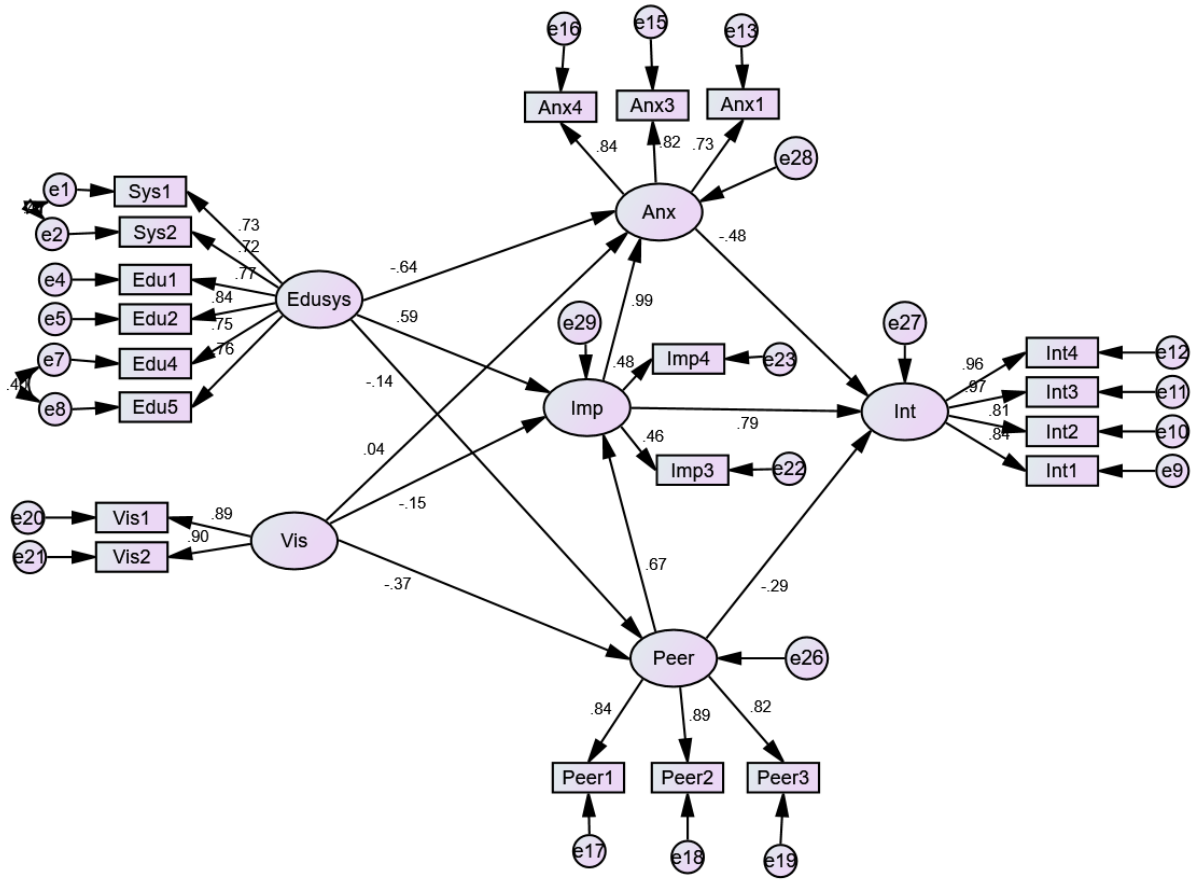

Fig. 3. SEM Path Diagram with Standardised Parameters.

TABLE IX. UNSTANDARDISED REGRESSION WEIGHT ESTIMATES

		Estimate	S.E	C.R.	.P	Supported?
H1	Edusys -> imp	0.516	0.093	5.571	***	Yes
H2	Edusys -> anx	-1.046	0.196	-5.335	***	Yes
H3	Edusys -> peer	-0.207	0.089	-2.333	0.020	Yes
H4	vis-> imp	-0.067	0.032	-2.125	0.034	Yes
H5	vis -> anx	0.031	0.065	0.476	0.634	No
H6	vis -> peer	-0.286	0.049	-5.803	***	Yes
H7	Imp -> int	1.185	0.223	5.309	***	Yes
H8	Imp -> anx	1.847	0.308	5.989	***	Yes
H9	Anx -> int	-0.388	0.119	-3.270	0.001	Yes
H10	Peer -> int	-0.261	0.121	-2.161	0.031	Yes
H11	Peer -> imp	0.397	0.064	6.210	***	Yes

TABLE X. STANDARDISED REGRESSION WEIGHT ESTIMATES

				Estimate	Supported
Peer	<---	Edusys		-0.140	Yes
Peer	<---	Vis		-0.367	Yes
Imp	<---	Edusys		0.587	Yes
Imp	<---	Vis		-0.145	Yes
Imp	<---	Peer		0.667	Yes
Anx	<---	Edusys		-0.641	Yes
Anx	<---	Imp		0.995	Yes
Anx	<---	Vis		0.036	No
Int	<---	Anx		-0.481	Yes
Int	<---	Peer		-0.292	Yes
Int	<---	Imp		0.792	Yes

V. DISCUSSION

This study analysed the relationship between organisational security factors and users' non-compliance behaviours in one higher education institution's transformation to online systems during the COVID-19 pandemic. A proposed model was developed based on a recent study by Hwang et al. [5]. In total, six constructs were selected for the model: two organisational security factors (security education systems and security visibility), three individual non-compliance causes (work impediments, security system anxiety and the non-compliance behaviours of peers) and compliance intention. The proposed model was tested using SEM. The negative link between study impediments and compliance was significant. This result is similar to previous findings, as work impairments diminish compliance [40, 41]. Users' compliance increases when they identify security actions as impediments to achieving the goals of a distinct task.

The hypothesis that security system anxiety exhibits a significant negative impact on compliance intent was supported, an outcome that was similar to previous research demonstrating that employees' anxiety decreases their intent to comply [42, 43]. Users' anxiety regarding security systems, triggered by an institution's imprecise security guidelines, thus, has an undesirable effect on their compliance. The hypothesis that peers' non-compliance behaviours have an undesirable impact on compliance intent was also supported. Generally, people tend to follow the behaviours of others if they are in the same group. Consequently, as students working on an online system obey the same security guidelines, there is a higher chance that other individuals in the same group will embrace comparable behavioural patterns. Therefore, information security actions are necessary at a university's personal, departmental, and team levels. Meanwhile, the hypothesis is that security education negatively impacts users' non-compliance with information security policies. This demonstrates limited equivalency with previous findings that security education systems decrease the non-compliance of workforces [12]. Security education systems effectively lessened work impairments and were significant in decreasing non-compliance behaviours and security system anxiety. Lastly, the hypothesis suggesting the negative link between security discernibility and users' non-compliance. This outcome is similar to preceding studies that have demonstrated that security visibility augments employees' compliance intent at work [13]. Security visibility can be heightened by suggesting approaches for security actions and public relations packages, for example, visual advertisements regarding an organisation's information safety requirements.

We previously discussed the importance of users' compliance with information security policies and suggested methods to have that accomplished. Such measures are expected to be even more pressing as information security issues could be the cause of large-scale damage. Users' compliance with policies and regulations is an important matter and a major worry for modern organizations. A different number of challenges could be behind the lack of sufficient users' compliance, also going back to the literature around employee engagement part of an organizational culture. Hu et al. [44] emphasized the critical importance of top management's commitment and participation towards the influence on the organizational compliance culture and shaping the intention of employees to comply with information security policies. Puhakainen and Siponen [45] emphasized the need for the adoption of information security awareness training and continued communication processes to motivate the employees' systematic cognitive processing of the information they receive and achieve the best development of employees' compliance results. Another influencer of employees engagement is their perception of trainings and career development inside the organization, which highly reflect on smart cities requirements which demand smart people, though such cannot be achieved without strong skills development techniques employed in the workplace and presented in different forms of modern training methods like wargames or simulations [46].

VI. RESEARCH IMPLICATIONS

This study's findings highlight some significant implications for both practitioners and academics. First, the

study confirmed that the intent to comply with an organisation's information security policy is undesirably impacted by the mediators of work impediments, the non-compliance of peers, and security system anxiety. A study impediment denotes the limitations on working processes and activities caused by conforming to established security guidelines. Education processes involve particular tasks, and completing these tasks is a more significant goal than complying with information security guidelines. Each time information security actions impede or conflict with their tasks, students can identify rational reasons for compliance but demonstrate non-compliance intents. Consequently, organisations should convince students that constructive security conduct is among the most important performance elements. Security system anxiety denotes an individual's hesitation or fear regarding information security guidelines. If these guidelines are severe and complex, users can experience anxiety regarding their security behaviours. In various cases, users may comply, although, in reality, they are more prone to non-compliance. Consequently, organisations should offer users support to better comprehend the systems and policies affecting information security. The non-compliance actions of peers encompass the belief that peers do not conform to the organisation's security procedure. Users exhibit tendencies to act like their peers. Comparable tendencies were demonstrated in this study, emphasising the need to promote a security atmosphere that stimulates peer compliance.

Secondly, the study's findings highlight that organisations' security efforts impact users' non-compliance. Security education systems increase work impairments, reducing peers' non-compliance and security system anxiety. Homogeneous security structures increase work impairments; for instance, organisations encourage users to use proficient USB drives and activate cloud-oriented security structures to systemise their safety configurations: security structures and security education system, anxiety, and non-compliant peer behaviour. Comprehensive education on matters linked to security procedures, performance, and behaviours may decrease users' system anxiety concerning required security actions, as well as peers' non-compliance tendencies. Moreover, security visibility was shown to decrease security system anxiety and peers' non-compliance behaviours; therefore, exhaustive promotion of security campaigns and guidelines may decrease these negative outcomes. Information security and protection controls should only be introduced when a risk is confirmed; they need to be cost-effective. Information security roles and responsibilities should be made public to all employees through the utilization of the information security policy. The information/asset owner is responsible for the monitoring and control of the information/asset usage in addition to the authorization of the users. They should also verify compliance with the information security policy and ensure that the system is appropriately secured. Information protection requires a comprehensive approach that follows a system development lifecycle. Information security should be periodically re-assessed and verified, based on objectives and requirements. In addition, information protection is directly impacted by the organizational culture. Information security management should be involved with business units to best understand their needs and determine the solutions that best protect assets.

This research expands the protection motivation model by suggesting discrete non-compliance causes and recommends organisational strategies for universities to help alleviate non-compliance with information security measures. The investigation recommends administrative variables for security improvement, including security education, security systems, and security visibility, as important constituents in reducing students' non-compliance with information security strategies. For establishments in which study impairments are a main cause of non-compliance, the institutions should invest primarily in security structures. In organisations with increased non-compliance levels and security system anxiety, an appropriate assortment of security systems, visibility, and education can result in satisfactory users' compliance.

VII. Conclusion

This study aimed to establish a causal link between organisational security efforts and the reasons for users' non-compliance with information security policy during the COVID-19 pandemic. Specifically, the study scrutinised the influence of organisational countermeasures, including security education systems and security visibility, on the causes of users' non-compliance, including work impairments, security system anxiety, and peers' non-compliance behaviours. SEM was used to test the suggested hypotheses with data collected from students at a business college. The findings showed that users' compliance intent is negatively impacted by the mediators of security system anxiety and the non-compliance of peers, while it is also positively influenced by work impairments. Meanwhile, the independent variables of security education systems and security visibility negatively impact security system anxiety and the non-compliance behaviour of peers. Nevertheless, only security education systems were found to positively impact the work impairment of the identified independent variables. The study's outcomes indicate the significance of security visibility and education in decreasing non-compliance, although security education systems seem to increase it. This study has some limitations. First, it is restricted in that we measured students' reflections on the reasons for individuals' non-compliance and organisational security efforts without discerning real activities. Consequently, future research should observe real behaviours related to information security objectives via controlled research laboratory experiments. Second, this study used SEM to examine the reasons behind users' non-compliance and organisational efforts to alleviate these reasons. In the future, we plan to discover the theoretical factors behind compliance intent that are highlighted by education belief theory and safeguard the motivation model, which can impact the instigators of non-compliance with the data security policy and procedures employed in higher education. Lastly, this study was situated in a precise time and location. It may be reinforced by longitudinal studies that observe diverse nations for a more robust overview of information security outcomes.

REFERENCES

[1] A. Nasir, K. Shaukat, I. A. Hameed, S. Luo, T. M. Alam, and F. Iqbal, "A Bibliometric Analysis of Corona Pandemic in Social Sciences: A Review of Influential Aspects and Conceptual Structure," IEEE Access, vol. 8, pp. 133377-133402, 2020.

[2] E. A. Miller, "Protecting and improving the lives of older adults in the COVID-19 era," Journal of Aging & Social Policy, vol. 32, pp. 297-309, 2020.

[3] S. Choi, J. T. Martins, and I. Bernik, "Information security: Listening to the perspective of organisational insiders," Journal of information science, vol. 44, pp. 752-767, 2018.

[4] G. D. Moody, M. Siponen, and S. Pahnila, "Toward a unified model of information security policy compliance," MIS quarterly, vol. 42, 2018.

[5] I. Hwang, D. Kim, T. Kim, and S. Kim, "Why not comply with information security? An empirical approach for the causes of non-compliance," Online Information Review, 2017.

[6] T. M. Alam, M. Mushtaq, K. Shaukat, I. A. Hameed, M. Umer Sarwar, and S. Luo, "A Novel Method for Performance Measurement of Public Educational Institutions Using Machine Learning Models," Applied Sciences, vol. 11, p. 9296, 2021.

[7] T.-M. Alam, K. Shaukat, A. Khelifi, W.-A. Khan, H.-M.-E. Raza, M. Idrees, et al., "Disease Diagnosis System Using IoT Empowered with Fuzzy Inference System," Computers, Materials \& Continua, vol. 70, pp. 5305--5319, 2022.

[8] S. Shakir, M. S. Asif, A. Talha Mahboob, and R. Zeeshan, "Early Prediction of Malignant Mesothelioma: An Approach towards Non-invasive Method," Current Bioinformatics, vol. 16, pp. 1-1, 2021.

[9] T. M. Alam, K. Shaukat, M. Mushtaq, Y. Ali, M. Khushi, S. Luo, et al., "Corporate bankruptcy prediction: An approach towards better corporate world," The Computer Journal.

[10] K. Shaukat, S. Luo, N. Abbas, T. Mahboob Alam, M. Ehtesham Tahir, and I. A. Hameed, "An analysis of blessed Friday sale at a retail store using classification models," pp. 193-198.

[11] R. Willison and M. Warkentin, "Beyond deterrence: An expanded view of employee computer abuse," MIS quarterly, pp. 1-20, 2013.

[12] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," Information systems research, vol. 20, pp. 79-98, 2009.

[13] M. Siponen, S. Pahnila, and M. A. Mahmood, "Compliance with information security policies: An empirical investigation," Computer, vol. 43, pp. 64-71, 2010.

[14] N. S. Safa and R. Von Solms, "An information security knowledge sharing model in organizations," Computers in Human Behavior, vol. 57, pp. 442-451, 2016.

[15] W. R. Flores, E. Antonsen, and M. Ekstedt, "Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture," Computers & security, vol. 43, pp. 90-110, 2014.

[16] Z. A. Soomro, M. H. Shah, and J. Ahmed, "Information security management needs more holistic approach: A literature review," International Journal of Information Management, vol. 36, pp. 215-225, 2016/04/01/ 2016.

[17] K. Shaukat, F. Iqbal, T. M. Alam, G. K. Aujla, L. Devnath, A. G. Khan, et al., "The Impact of Artificial intelligence and Robotics on the Future Employment Opportunities," Trends in Computer Science and Information Technology, vol. 5, pp. 050-054, 2020.

[18] L. Alzahrani and K. P. Seth, "The Impact of Organizational Practices on the Information Security Management Performance," vol. 12, p. 398, 2021.

[19] S. Kwon, S. Jang, J. Lee, and S. Kim, "Common defects in information security management system of Korean companies," Journal of Systems and Software, vol. 80, pp. 1631-1638, 2007.

[20] D. Pérez-González, S. T. Preciado, and P. Solana-Gonzalez, "Organizational practices as antecedents of the information security management performance: An empirical investigation," Information Technology & People, 2019.

[21] J. May and G. Dhillon, "A holistic approach for enriching information security analysis and security policy formation," 2010.

[22] M. Siponen and R. Willison, "Information security management standards: Problems and solutions," Information & management, vol. 46, pp. 267-270, 2009.

[23] R. Werlinger, K. Hawkey, and K. Beznosov, "An integrated view of human, organizational, and technological challenges of IT security management," Information Management & Computer Security, 2009.

[24] A. N. Singh, M. Gupta, and A. Ojha, "Identifying factors of "organizational information security management"," Journal of Enterprise Information Management, 2014.

[25] B. Von Solms, R. J. C. Von Solms, and security, "The 10 deadly sins of information security management," vol. 23, pp. 371-376, 2004.

[26] D. Ashenden, A. J. C. Sasse, and Security, "CISOs and organisational culture: Their own worst enemy?," vol. 39, pp. 396-405, 2013.

[27] I. Javed, X. Tang, K. Shaukat, M. U. Sarwar, T. M. Alam, I. A. Hameed, et al., "V2X-Based Mobile Localization in 3D Wireless Sensor Network," Security and Communication Networks, vol. 2021, p. 6677896, 2021/02/11 2021.

[28] K. Piwowar-Sulej and R. J. I. J. o. C. M. Mroziewski, "MANAGEMENT BY VALUES: A CASE STUDY OF A RECRUITMENT COMPANY," vol. 19, 2020.

[29] M. Ghobakhloo and M. J. J. o. M. T. M. Fathi, "Corporate survival in Industry 4.0 era: the enabling role of lean-digitized manufacturing," 2019.

[30] D. Horváth, R. Z. J. T. f. Szabó, and s. change, "Driving forces and barriers of Industry 4.0: Do multinational and small and medium-sized companies have equal opportunities?," vol. 146, pp. 119-132, 2019.

[31] M. A. Hasbini, T. Eldabi, A. J. W. J. o. E. Aldallal, Management, and S. Development, "Investigating the information security management role in smart city organisations," 2018.

[32] K. Shaukat, T. M. Alam, M. Ahmed, S. Luo, I. A. Hameed, M. S. Iqbal, et al., "A Model to Enhance Governance Issues through Opinion Extraction," in 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2020, pp. 0511-0516.

[33] B. K. Nkansah, "On the Kaiser-meier-Olkin's measure of sampling adequacy," Math. Theory Model, vol. 8, pp. 52-76, 2011.

[34] T. M. Alam, K. Shaukat, H. Mahboob, M. U. Sarwar, F. Iqbal, A. Nasir, et al., "A Machine Learning Approach for Identification of Malignant Mesothelioma Etiological Factors in an Imbalanced Dataset," The Computer Journal.

[35] D. W. Stewart, "The application and misapplication of factor analysis in marketing research," Journal of marketing research, vol. 18, pp. 51-62, 1981.

[36] T. M. Alam, K. Shaukat, I. A. Hameed, W. A. Khan, M. U. Sarwar, F. Iqbal, et al., "A novel framework for prognostic factors identification of malignant mesothelioma through association rule mining," Biomedical Signal Processing and Control, vol. 68, p. 102726, 2021.

[37] B. Wheaton, B. Muthen, D. F. Alwin, and G. F. Summers, "Assessing reliability and stability in panel models," Sociological methodology, vol. 8, pp. 84-136, 1977.

[38] P. M. Bentler, "Comparative fit indexes in structural models," Psychological bulletin, vol. 107, p. 238, 1990.

[39] K. G. Jöreskog and D. Sörbom, "Recent developments in structural equation modeling," Journal of marketing research, vol. 19, pp. 404-416, 1982.

[40] R. West, "The psychology of security," Communications of the ACM, vol. 51, pp. 34-40, 2008.

[41] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," MIS quarterly, pp. 523-548, 2010.

[42] V. Venkatesh, "Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model," Information systems research, vol. 11, pp. 342-365, 2000.

[43] T. M. Alam, K. Shaukat, I. A. Hameed, S. Luo, M. U. Sarwar, S. Shabbir, et al., "An investigation of credit card default prediction in the imbalanced datasets," IEEE Access, vol. 8, pp. 201173-201198, 2020.

[44] Q. Hu, T. Dinev, P. Hart, and D. J. D. S. Cooke, "Managing employee compliance with information security policies: The critical role of top management and organizational culture," vol. 43, pp. 615-660, 2012.

[45] P. Puhakainen and M. J. M. q. Siponen, "Improving employees' compliance through information systems security training: an action research study," pp. 757-778, 2010.

[46] S. N. A. Hamid and K. K. Yahya, "Relationship between person-job fit and person-organization fit on employees' work engagement: A study among engineers in semiconductor companies in Malaysia," in Annual Conference on Innovations in Business and Management London, 2011, pp. 1-30.