Uncovering Role of Information Security Awareness, Compliance Knowledge & Organizational Citizenship Behaviour Towards Information Security Compliance in Chinese Public & Private Universities

GaoShun Tan

Recommended citation:

Tan, GaoShun (2024). "Uncovering Role of Information Security Awareness, Compliance Knowledge & Organizational Citizenship Behaviour Towards Information Security Compliance in Chinese Public & Private Universities". *Profesional de la información*, v. 33, n. 5, e330507.

https://doi.org/10.3145/epi.2024.0507

Article received on June 14th 2024
Approved on September 25th 2024

GaoShun Tan

https://orcid.org/0009-0002-6047-9116
School of Marxism,Jiangxi Normal University
Nanchang Jiangxi, 330022, China
School of Marxism, Qujing Normal University
Qujing Yunnan, 655011, China
ynqjtgs@163.com

Abstract

Information security compliance helps to provide the safety and safeguard of personal and sensitive information from unauthorized access. This has been equally important both in businesses and academic institutions. Considering the organizational significance of information security compliance, this research explores the role of information security awareness, compliance knowledge, and organizational citizenship behaviour towards such information security compliance. A questionnaire-based data was collected from a valid sample of 318 respondents from both public and private sector universities in China. The study applied advanced statistical techniques to investigate data trends, variables' measurement, and reliability in the model. The results support the argument that the outer model is reliable enough in terms of items and latent variables for consideration in the structural model analysis. The study findings through the structural model using the Smart PLS 4 infer that information security awareness, compliance knowledge, and organizational citizenship behaviour are positively and significantly related to information security compliance in both public and private sector universities. The results also suggest that university administrators need to promote compliance knowledge, compliance awareness, and organizational citizenship behaviour, which in return helps to achieve better information security compliance.

Keywords

Information Security Awareness, Compliance Knowledge, and Organizational Citizenship Behaviour Towards Information Security Compliance.

1. Introduction

Information security is essential for organizations today because they depend heavily on digital systems for their work. Due to rapid technological advancement, organizations implement different types of technical measures to mitigate the potential threats linked with information security (**Siponen**, 2000). For instance, as cyber data and threat breaches increase, it is necessary to protect sensitive information and keep running organization operations smoothly through technically advanced systems (**Soomro *et al.***, 2016). In addition, there are a range of non-technical measures to address the concerns related to information security, such as training and awareness about information security and information

security education (**Amankwa *et al.***, 2014; **Hart *et al.***, 2020). In fact, merely focusing on the investment in securing the information is not enough where the human aspects play a major role. This is because a considerable number of organizations have failed to achieve information security compliance due to lack of necessary information security awareness (**Khando *et al.***, 2021).

Information security compliance in an organizations' context means that employees follow the organization's rules and take necessary actions to protect that information (**Guo**, 2013). Such information security compliance is more about people than technology, wherein employees follow the security rules and remain stuck to policy, report any suspicious activity, and avoid risky behavior. Information security compliance also requires employees to follow security rules and report any threats (**Ifinedo**, 2012). Such compliance behavior actions include using strong passwords, reporting emails, and not leaving data on desktops. In view of this concern, information security compliance much depends upon employees' information security awareness. Organizations are constantly making huge amounts of investments on employees' information security awareness to secure their information assets.

One of the best approaches to address the concerns linked with information security awareness is to explore the new body of knowledge and exploit the existing knowledge (**Kim; Kim**, 2017). Focusing on compliance knowledge indicates the fact that insider problems are the most significant part of the security breaches within the organization. Meanwhile, without some compliance-related knowledge, organizations are unable to learn from past compliance or non-compliance experience in order to avoid the repetition of the similar issues. Like other organizational factors, the role of compliance knowledge in information security compliance is compassionate and vital (**Herath; Rao**, 2009). Suppose the organizations either working for profit or not-for-profit motives, unable to focus on the information security and related concerns. In that case, they will face serious threats of losing their business (**Kim; Kim**, 2017).

Organizational Citizenship Behavior (OCB) refers to such voluntary actions that employees take on their own by taking actions, like helping or being extra supportive, without being told to do so. It involves solving problems without waiting for instructions (**Organ**, 1988). The linkage between OCB and information security compliance has been observed with a very little note in the current studies on information security awareness and information security compliance. OCB is different form general compliance of the rules and regulations because it involves doing more than just the bare minimum of what's required (**Organ; Ryan**, 1995). For example, organizations may encourage employees to change their passwords for security reasons (**Vedadi *et al.***, 2024). By complying to such security regulations, employees not only show their commitment to organization's success and safety, but also depict what can be termed as Organizational Citizenship Behavior (**Organ**, 1988).

Universities have essential research data and resources, which make them vulnerable to security risks. The Department of Libraries struggles to create effective policies for digital information security (**Farid *et al.***, 2023). This is because they hold a lot of essential books and electronic materials, and they must have a strict surveillance on the access to this information in order to keep it private and secure (**Hamad *et al.***, 2023). Meanwhile, creating strong security measures is tough for libraries because they often have limited budgets and staff. Technology is essential for keeping information secure, and those who are linked with such responsibilities are equally important (**Amini *et al.***, 2021).

Enhancing employees' awareness about information security has gained much attention in academic literature over the past couple of decades, and theories from both the fields of psychology and criminology have supported the concept of information security (**Ali *et al.***, 2021). Previous studies also support this argument that employees' lack of information security awareness was among the major causes of mishandling of sensitive organizational information (**Abraham**, 2011). However, it has been felt that information security awareness and adherence to security practices have not been studied much in the context of public and private sector universities (**Kavak; Odabaş**, 2023; **Marett; Barnett**, 2021). Most of the past research has concentrated only on technical aspects like cybersecurity and software upgradation. Not much has been discussed about human behavior and its impact on information security. In other words, there is a dearth of studies on how human behaviour can be formed through enhancing employees' information security awareness, developing compliance knowledge, and molding employees' behavior towards information security compliance. In order to fill this research gap, therefore, the current study uncovers the role of information security awareness, compliance knowledge, and organizational citizenship behaviour towards information security compliance, in public & private universities in China.

2. Literature Review

2.1. Information Security Awareness

Information security awareness means that people or organizations know how to protect their information. They understand the risks and know what steps to take to stay safe (**Kavak; Odabaş**, 2023). Information security awareness is about being careful and informed when dealing with information online or in the workplace (**Kavak; Odabaş**, 2023). It also means knowing potential dangers when storing or sharing information. Basically, it helps everyone do their job well while

keeping information secure. Information security awareness also helps to create a workplace where everyone prioritizes protecting information. When people understand the importance of security, they are likely to follow good practices and work together to keep information safe (**Da Veiga *et al.***, 2020; **Ecek; Çakmak**, 2022; **Özdemir; Uluyol**, 2020).

Information security awareness also means that employees know and understand the company rules for keeping information safe. It ensures that they are familiar with how to protect sensitive data and follow the right steps to avoid security risks (**Özdemir; Uluyol**, 2020; **Bulgurcu *et al.***, 2010). Employees with high information security awareness understand their company security rules. They recognize the risks that could harm the company's information. Last, but not the least, information security awareness also refers to the conceptual or cognitive awareness about information security. **Bulgurcu *et al.*** (2010) claim that it is quite complex to know about the cognitive elements and its affective elements, since cognitive awareness is about how employees know about security information; however, affective awareness is to know about how employees feel or think about their work, which complicates this awareness. If someone has both good knowledge and positive attitudes and behavior about information security, they have strong information security awareness.

2.2. Information Security Management

The widespread effects of cyberattacks and data breaches have significantly increased the importance of information security management in today's world. **Whitman and Mattord** (2011) believed that information security management plays a big role in helping organizations stay competitive, protect their reputation, and perform well financially. Information security management covers many areas like identifying threats, monitoring risks, verifying identities, controlling who has access, backing up data and protecting against malware. Both technologies and procedures are used to achieve these goals and keep the information safe (**Whitman and Mattord** (2019). In simple terms, information security management is required for confidentiality, integrity, and accessibility (**Whitman; Mattord**, 2023; **Mattord *et al.***, 2024). Additionally, data misuse and system hacks have shown that it is better to plan for information security management in advance rather than just reacting after some thereat takes place (**Scarfone; Souppaya**, 2009).

The fast development of information and digital data has changed the manner how organizations manage their information security. Such a change was necessitated due to new threats like data breaches and cyberattacks, which are important concerns for information security (**Choobineh *et al.***, 2007). Safeguarding sensitive information like customer details, research, or final records is now a top priority for organizations. As more companies use internet devices, the chances of security weakness have increased, making it necessary to implement strict security against threats. Improper information security management shows security weaknesses, which can cause severe financial losses and damage to an organization's reputation.

A robust information security management plan should, therefore, be a top priority for any organization. The main goal of information security management is to protect a company's information from different threats. (**Whitman; Mattord**, 2019). To protect the information, it is essential to analyze risks, choose the right security measures, and regularly check the working methods of different unit of organizations (**Whitman; Mattord**, 2019). In simple terms, insider risks, whether caused by someone's mistake or through an intentional sabotage to cause harm on purpose, can still happen (**Marett; Barnett**, 2021). To reduce these risks, organizations often take strict steps like limiting access of sensitive information, keeping track of what employees do online, and running employee training programs about cybersecurity.

2.3. Information Security Compliance

Information security compliance requires employees to remain proactive to protect information and maintain a strict compliance of organization's rules and regulations (**Guo**, 2013). Information security compliance directs people and not technology; hence, employees must comply with the security rules, policies and remain vigilant to detect any suspicious activity, and refrain from indulging in any risky behavior. Information security compliance also requires employees to follow all security rules such as using strong passwords, reporting emails, and not leaving data on their computers (**Ifinedo**, 2012).

There are several factors that affect information security compliance, such as ambiguity about policies, fear of not following the rules, and lack of commitment to organizations. There is a strong relationship between information security and compliance of rules (**Siponen; Vance**, 2010). The awareness about information security rules helps employees to comply with them. For example, in a library, if employees have high prior information about security measures, they are more likely to comply with information security. Training the staff on information security not only increases their awareness but also encourages them to follow security rules (**Bulgurcu *et al.***, 2010; **Oluwabunmi; Madukoma**, 2022). Studies have explored the link between information security and compliance. It has been proven that as employees become more aware of security rules, they are more likely to follow them (**Oluwabunmi; Madukoma**, 2022). When employees understand why security rules are essential, they are more willing to comply. **Herath and Rao** (2009) looked at how awareness, attitude, and social expectations impact an employee's intentions. **Ifinedo** (2012) built a similar model, relating awareness with overt behavior and social expectations. **Bauer *et al.*** (2017) found that awareness influences compliance indirectly. **Sohrabi Safa *et al.*** (2016) studied the security rules that help to protect information organizations. In other study, it was found that awareness and compliance influence each other (**Siponen; Vance**, 2010).

2.4. Organizational Citizenship Behavior

Organ (1988) pioneed the definition of Organizational Citizenship Behavior (OCB), as voluntary actions taken by employees in an organizational environment, such as helping others or being extra supportive, without being told to do so, and solving problems without waiting for instructions. **Organ** (1997) later added the element of social and psychological behaviors at work in this definition, and broadened the role of employees beyond their job activities. **LePine *et al.*** (2002), too, agreed to this and related OCB with contextual performance rather than merely focusing on how people perform their regular job duties. They argued that OCB is like putting in a lot of enthusiasm to complete tasks successfully. This concept highlights that employees have a comprehensive approach in performing their regular job duties. A truly planned OCB helps to build a framework of environment that supports several task performances. In addition, **Organ and Ryan** (1995) also consider job satisfaction as having a strong connection with OCB.

For workplace behaviors such as OCB, several criteria must be satisfied. For example, any action amounting to OCB must involve personal choice, and that employee chooses to do it without being forced (**Organ**, 1988), for which employees must be paid reward as they do perform a few extra tasks voluntarily (**Organ *et al.***, 2005). OCB thus happens also when an employee goes beyond the basic expectations for the organization (**Organ**, 1990). In its basic form, OCB is grouped in two types: (1) helping others and (2) general compliance. Helping others might also extend to people outside the organizations which can improve their overall performance; general compliance goes along with what is the best for an organization without being asked (**Nielsen *et al.***, 2012). General compliance also means doing more than what's required in their job description (**Organ; Ryan**, 1995), such as remaining vigilant towards information security standards in work place. Those who follow information security standards diligently are incredibly dedicated to the organization's success and safety (**Vedadi *et al.***, 2024).

2.5. Knowledge Compliance and Information Security Compliance

The relationship between knowledge compliance and information security compliance behavior is evident in several studies. **Kim and Kim** (2017), for example, explore how different voluntary compliance behaviors evolve from a knowledge management perspective, especially in the light of growing privacy and security concerns, and due to advancements in big data and artificial intelligence. This motivation pushed the authors to propose a structural model based on the theory of planned behavior and IT-relatedness theory. They surveyed 975 employees from S-OIL, a major Korean energy company that has a compliance support system in place. The respondents were divided into two groups. The first group comprised those who actively used information technology, and the second group consisted of those who used it passively. The findings indicated that both compliance beliefs and social pressure significantly impacted compliance intentions, with compliance knowledge acting as a mediator in both groups. However, the empirical findings also showed that the relationships and effects in the active information technology utilization group were much more robust than in the passive group. The given theoretical backgrounds suggest that beliefs about compliance and social pressure influence both compliance knowledge and intentions. Additionally, the correlation between behavioral beliefs and compliance knowledge, along with the social pressure and compliance knowledge, tends to reflect that level of information technology utilization plays a significant moderating role. Overall, the given research seemed to enhance the understanding of how various factors are influencing voluntary compliance behaviors, while highlighting their relevance to knowledge management practices and compliance support systems within the targeted organization of Korea.

3. Methods, Material, Population and Sample

The study followed a descriptive and quantitative research design to analyze the relationship between information security awareness, compliance knowledge, organization citizenship behaviour, and information security compliance. To collect data, a questionnaire was customized whose items were based on measurements and scales available in previous studies as presented in Table 1.

The questionnaire also captured the demographic properties of respondents, which confirmed a good diversification distributed across their gender, age, education and job title, hours spent in front of the computer, size of the institution, and type of employment, whether regular or contractual.

The target population of this study comprised all the employees working in the information security departments of the public and private sector universities in the South region of China. Due to no specific data available related to the total number of employees as working in the targeted departments, the researchers applied a convenient sampling technique. A time duration of 5 weeks and three days was spent distributing and collecting the questionnaire. Initially, a total of 450 copies were distributed, out of which 342 copies were collected. A total of 24 questionnaires were found with invalid responses, hence they were dropped from the final sample. As a result, the study sample was restricted to 318 questionnaires for final analysis.

The discriminant validity between the study variables information security awareness, compliance knowledge, organization citizenship behaviour, and information security compliance were measured using the three widely adopted

techniques such as Heterotrait-Monotrait Ratio (HTMT), Fornell-Larcker criterion, and loadings and cross-loadings techniques. The subsequent data analyses were performed by testing of the relationships between information security compliance, compliance knowledge, information security awareness, and organization citizenship behaviour. For this purpose, the structural equation model using the Smart PLS, well known for testing the quantitative relationships between the variables, was used to generate path coefficients, relative standard deviation, t-statistics, and p-values.

Table 1: Study Variables.

Variables	Items of the scale	Source(s)
Information Security Awareness (IV1)	1. I am aware about the importance about the security and confidentiality of sensitive data. 2. I understand the importance of password security and regularly update my passwords. 3. I am aware about university's policies and procedures related to information security. 4. I am vigilant and report regularly the information security related incidents to appropriate department. 5. I am aware about cybersecurity threats and take steps to protect university systems. 6. I understand the significance of data backup and recovery for critical university information. 7. I participate in the university's information security training programs regularly.	(**Kavak; Odabaş**, 2023)
Organizational Citizenship Behavior (IV2)	1. I urge my coworkers to comply with security procedures, and volunteer and engage in activities to prevent insecure use of computers. 2. I often make suggestions to enhance the university's information security system. 3. I keep myself abreast with latest rules, policies and procedures related to information security.	(**Turel *et al.***, 2020)
Information Security Compliance (DV)	1. I regularly lock my computer screen when away from my desk. 2. I do not install unauthorized software on university devices. 3. I regularly update passwords and do not share them with others. 4. I report any suspicious activity or security breaches immediately. 5. I participate in information security training provided by the university. 6. I am cautious about sharing sensitive information in emails or attachments. 7. I regularly review and follow the university's information security policies and procedures.	(**Kavak**, 2024)
Compliance Knowledge (IV3)	1. I am aware that there are laws and regulations related to my role/task 2. I have the knowledge of laws and regulations that are related to my role/task 3. I am aware how, when and why the laws and regulations related to my role/task were enacted/amended. 4. I understand what is enacted/amended in those laws and regulations related to my role/task 5. I have the knowledge of how to perform compliance of self-assessment on my work/role 6. I understand the limitations of the laws and regulations that are related to my role/task have 7. I understand compliance practice processes that are related to my role/task	(**Bulgurcu *et al.***, 2010; **Ajzen**, 1991; **Ajzen; Fishbein**, 1980; **Bandura**, 1986)

4. Results and Discussion

Table 2 and Figure 1 reveal the gender distribution of the sample, comprising 246 (77.3%) male and 72 (22.7%) female respondents, hence the male category dominating in this study.

Table 2: Gender Distribution.

Gender	Frequency	Percentage (%)	Cumulative Percentage (%)
Male	246	77.3	77.3
Female	72	22.7	100
Total	**318**	**100**	

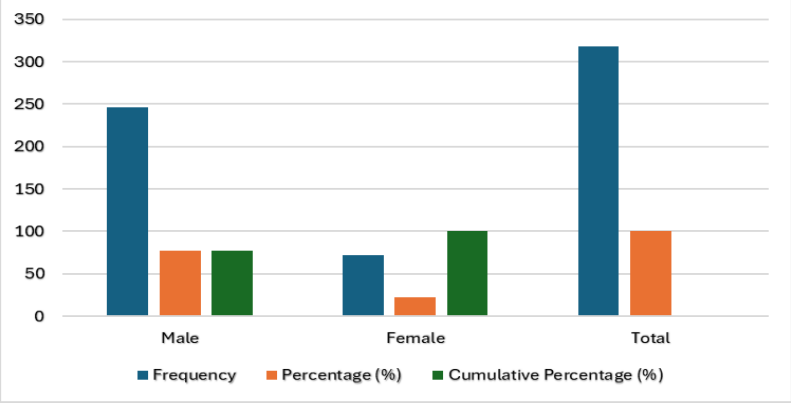

Figure 1: Gender Distribution.

Table 3 and Figure 2 present the education background of the respondents of the study. As per the frequency distribution, 114 (35.8%) respondents had completed 14 years of education, whereas 49 (15.4%) respondents had finished 16 years, and 67 (21%) of the total 318 respondents had more than 16 years of qualification. However, it was also found that 88 (27.8%) respondents had diploma and other qualifications.

Table 3: Educational Background.

Education Level	Frequency	Percentage (%)	Cumulative Percentage (%)
14 Years	114	35.8	35.8
16 Years	49	15.4	51.2
Above 16 Years	67	21	72.2
Diploma & Other	88	27.8	100
Total	**318**	**100**	

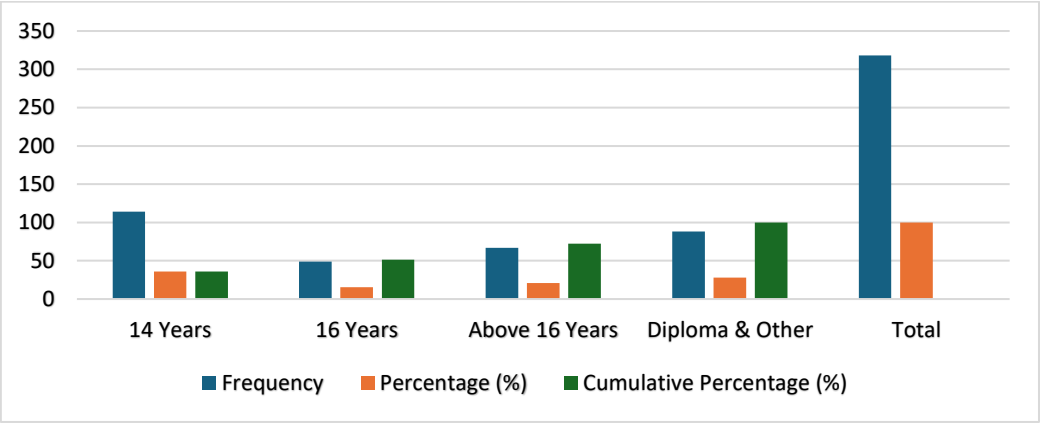

Figure 2: Education of the Respondents.

The computer usage distribution is presented in Table 4 and Figure 3. As per the frequency distribution, 75 (23.5%) respondents used their computer for 0-2 hours daily, while 102 (32%) respondents use it for 3-4 hours daily. Additionally, 85 (26.7%) respondents of the total sample fell into the category of 5-6 hours of computer usage per day. It was also found that 56 (17.8%) respondents used their computer for more than 6 hours daily.

Table 4: Computer Usage (Hours/Day)

Computer Usage (Hours/Day)	Frequency	Percentage (%)	Cumulative Percentage (%)
0-2 Hours	75	23.5	23.5
3-4 Hours	102	32	55.5
5-6 Hours	85	26.7	82.2
Above 6 Hours	56	17.8	100
Total	318	100	

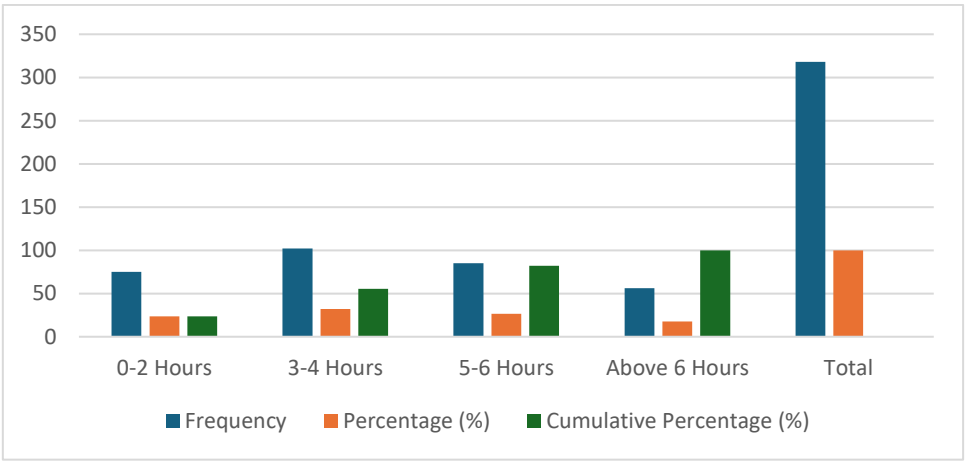

Figure 3: Computer Usage (Hours/Day).

Table 5 shows how institutions are distributed by size, and the same is reported using the graphical presentation in Figure 4. It explains that 45 institutions, or 14.2%, have fewer than 100 members as their employees, making this the smallest and least common size category. The most frequent size category is between 101–and 300, which includes 80 institutions, or 25.1% of the total. Additionally, those institutions with 301 to 600 members comprise 22.0% of the sample, with 70 institutions falling into this range. The institutional size of 601–1000 employees had a total of 55 institutions, representing 17.3%, showing a moderate presence. There are 35 institutions, or 11.0%, in the range of 1001–1500. Finally, 33 institutions, or 10.4%, have more than 1500 members, which is the largest size. The data covers 318 institutions, representing 100% of the sample.

Table 5: Size of Institution.

Size of Institution	Frequency	Percentage (%)	Cumulative Percentage (%)
Under 100 employees	45	14.2	14.2
101–300 employees	80	25.1	39.3
301–600 employees	70	22	61.3
601–1000 employees	55	17.3	78.6
1001–1500 employees	35	11	89.6
Above 1500 employees	33	10.4	100
Total	318	100	---

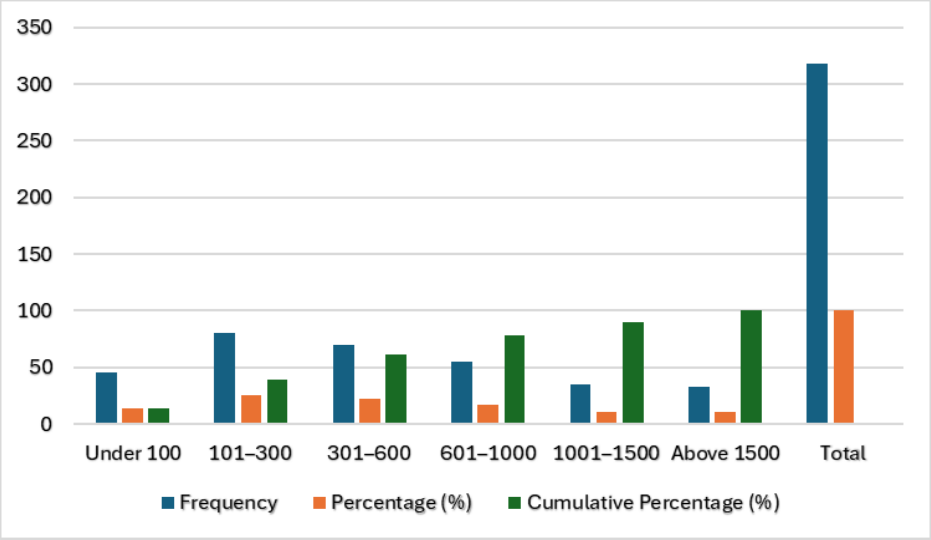

Figure 4: Size of Institution.

Table 6 shows the distribution of institutions based on employment type. According to the frequency distribution, 246 institutions (77.3%) offer regular employment. This category represents the largest proportion of the sample. In contrast, 72 institutions (22.7%) provide contractual employment, demonstrating a smaller proportion. The data includes 318 respondents from different educational institutions, accounting for 100% of the sample. The cumulative percentage reflects the running total of the proportions, with regular employment making up 77.3% and contractual employment bringing the total to 100%, by the end. Figure 5 also depicts the same information for a quick understanding of employment types.

Table 6: Type of Employment.

Type of Employment	Frequency	Percentage (%)	Cumulative Percentage (%)
Regular	246	77.3	77.3
Contractual	72	22.7	100
Total	318	100	

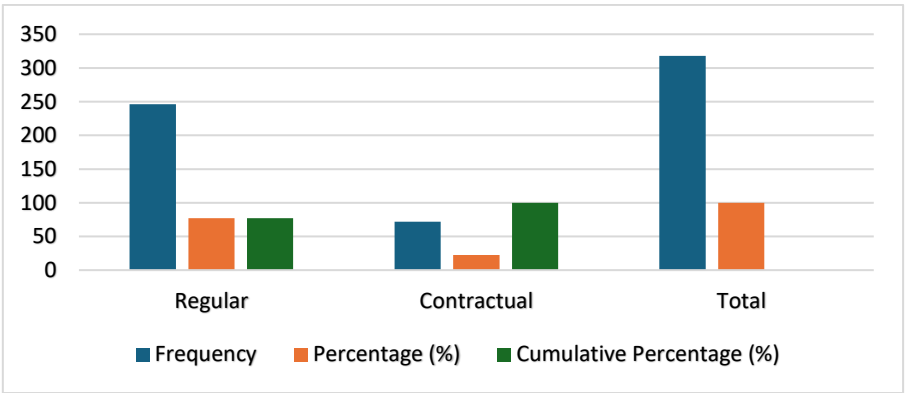

Figure 5: Type of Employment.

The questionnaire's reliability was determined using the alpha score and composite reliability. Besides, convergent validity focused on AVE or average variance extracted (**Farrell**, 2010; **Awais Rashid *et al.***, 2021). Table 7 and Figure 6 show the measures of reliability and convergent validity. The COK represents a measure with a high Cronbach's alpha of 0.920, suggesting it is very reliable. Its composite reliability scores are also high (i.e., 0.924 and 0.935), with an AVE of 0.674. These scores show that COK has captured much of the concept it is supposed to measure.

The second variable, ISA, has a Cronbach's alpha of 0.895, indicating strong reliability. Its composite reliability scores are good (i.e., 0.907 and 0.921 as composite reliability using rho_and rho_c). The AVE of this variable is 0.630, which is acceptable. For the third variable, ISC, the Cronbach's alpha is 0.852, and its composite reliability scores are 0.853 and 0.900 when accounting for rho_and rho_c. It has an AVE of 0.693, which also captures the intended concept of convergent validity well. The fourth variable is OCB, which has a Cronbach's alpha of 0.772, showing decent reliability as observed. Its composite reliability scores are 0.790 and 0.868, and its AVE is 0.687. Therefore, it indicates that OCB has adequately measured the given concept. Overall, all measures are reliable and effectively capture the concepts they are intended to measure.

Table 7: Reliability and Convergent Validity Investigation.

	Cronbach's Alpha	Composite Reliability (rho_a)	Composite Reliability (rho_c)	Average Variance Extracted (AVE)
COK	0.920	0.924	0.935	0.674
ISA	0.895	0.907	0.921	0.630
ISC	0.852	0.853	0.900	0.693
OCB	0.772	0.790	0.868	0.687

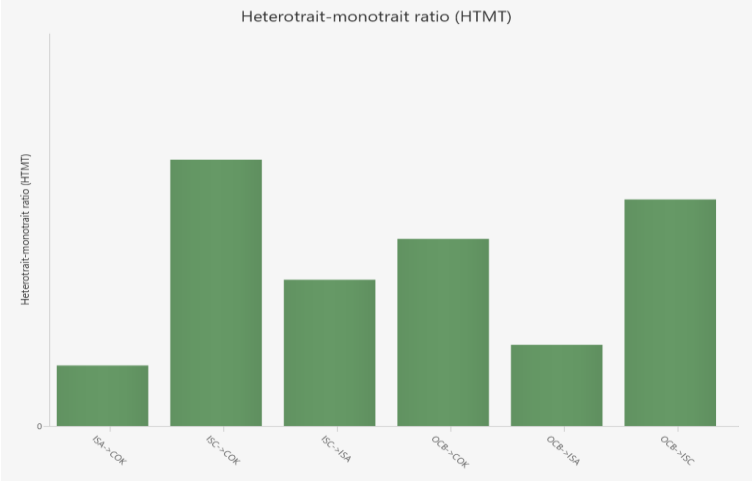

Figure 6: HTMT ratio of the Variables.

The measurement of the discriminant validity, at least between the two different measurement constructs, can be done using the Heterotrait-Monotrait (HTMT) ratio (See Figure 6). The HTMT Ratio is a tool used to check if different constructs (e.g., information security awareness, compliance knowledge, organization citizenship behaviour, and information security compliance) in SEM are distinct from each other, especially when using methods like Partial Least Square technique. Discriminant validity makes sure that each construct really measures something unique and is not too similar to other variables in a similar model. Typically, if the HTMT value is below 0.85 (or sometimes 0.90), it indicates that the constructs are likely distinct from one another (**Li *et al.***, 2022; **Hair *et al.***, 2021).

Table 8 shows that the HTMT ratio between COK and ISA is 0.154; while between COK and ISC, the ratio is 0.679, suggesting a moderate level of correlation but still within acceptable limits for discriminant validity (less than 0.85). The HTMT ratio between ISA and ISC is 0.373, indicating a low correlation and good discriminant validity. The ratio between COK and OCB is 0.477, showing a moderate correlation or less than 0.85, while between ISA and OCB, it is 0.207, reflecting a low correlation and clear discriminant validity. Lastly, the HTMT ratio between ISC and OCB results are 0.577, indicating a moderate correlation, though still within sufficient discriminant validity.

Table 8: HTMT Ratio.

	COK	ISA	ISC	OCB
COK				
ISA	0.154			
ISC	0.679	0.373		
OCB	0.477	0.207	0.577	

The Fornell Larcker method of discriminant validity also yielded interesting results in this study. The Fornell-Larcker criterion is a way to check if different constructs in structural equation modeling are genuinely distinct from each other. It does this by comparing the square root of the average variance extracted (AVE) for each construct with the correlations between that construct and others in the model (**Afthanorhan *et al.***, 2021). For discriminant validity to be confirmed using this method, the square root of the AVE should be higher than the correlation of that construct with any other construct (**Yusoff *et al.***, 2020). Table 9, however, depicts the correlations between all variables are much lower than their square root values. This has led to the inference that discriminant validity is linked with all these variables.

Table 9: Fornell Larcker.

	COK	ISA	ISC	OCB
COK	0.821			
ISA	0.139	0.793		
ISC	0.648	0.317	0.833	
OCB	0.414	0.178	0.479	0.829

The third method of checking the discriminant validity is by focusing on the loadings and cross-loadings. The given method claims that discriminant validity will exist in case the loadings of the items would be above the cross-loadings. The items'

loading for the COK, ISA, ISC, and OCB, along with the VIF of the items, are given in Table 10. The loadings for COK are 0.809, 0.788, 0.787, 0.824, 0.858, 0.849 and 0.831; for ISA, the loadings are 0.869, 0.528, 0.653, 0.886, 0.883, 0.828, and 0.834, for ISC; 0.871, 0.873, and 0.697, and for OCB; 0.788, 0.893, and 0.802. It has been found that these loadings are truly above the 0.50 level and are significantly contributing towards the measurement of the COK, ISA, ISC, and OCB.

Similar evidence can be found when these loadings are compared with the cross-loadings, which are lower than these loadings. As a result, this research accepts that the third piece of evidence for checking the discriminant validity is also available along with the HTMT and Fornell-Larcker criteria. The available approaches entitled HTMT, Fornell-Larcker, and loadings and cross-loadings also have the literature justification (**Ab Hamid *et al.***, 2017; **Rasoolimanesh**, 2022; **Yusoff *et al.***, 2020; **Jianjun *et al.***, 2021).

The last column of Table 10 aims to check the variance inflation factor (VIF) of the selected items. The results show that VIF values are 2.217, 1.954, 2.42, 2.426, 2.813, 2.869, 2.711, 3.863, 1.272, 1.47, 3.632, 4.069, 3.761, 3.969, 3.931, 3.282, 3.814, 1.191, 1.517, 1.925, and 1.566. These values are lower than the prescribed threshold point of 5 as justified in previous studies (**Sharma**, 2010; 2012; **Ye *et al.***, 2022) to claim for the non-presence of the collinearity issue in the data and these items. Therefore, the researchers have finally accepted all of these values as final evidence, which leads to the selection of the items for the measurement of the variables, with the titles COK, ISA, ISC, and OCB, respectively.

Table 10: Items loadings, cross loadings and VIF.

Items	COK	ISA	ISC	OCB	Items	VIF
COK1	**0.809**	*0.151*	*0.605*	*0.377*	**COK1**	2.217
COK2	**0.788**	*0.136*	*0.606*	*0.412*	**COK2**	1.954
COK3	**0.787**	*0.109*	*0.446*	*0.276*	**COK3**	2.42
COK4	**0.824**	*0.112*	*0.513*	*0.350*	**COK4**	2.426
COK5	**0.858**	*0.128*	*0.545*	*0.359*	**COK5**	2.813
COK6	**0.849**	*0.090*	*0.502*	*0.322*	**COK6**	2.869
COK7	**0.831**	*0.056*	*0.461*	*0.241*	**COK7**	2.711
ISA1	*0.113*	**0.869**	*0.272*	*0.173*	**ISA1**	3.863
ISA2	*0.157*	**0.528**	*0.199*	*0.042*	**ISA2**	1.272
ISA3	*0.121*	**0.653**	*0.255*	*0.216*	**ISA3**	1.47
ISA4	*0.174*	**0.886**	*0.304*	*0.203*	**ISA4**	3.632
ISA5	*0.116*	**0.883**	*0.246*	*0.130*	**ISA5**	4.069
ISA6	*0.024*	**0.828**	*0.238*	*0.104*	**ISA6**	3.761
ISA7	*0.052*	**0.834**	*0.218*	*0.068*	**ISA7**	3.969
ISC4	*0.407*	0.300	**0.876**	*0.414*	**ISC4**	3.931
ISC5	*0.423*	0.338	**0.871**	*0.370*	**ISC5**	3.282
ISC6	*0.430*	0.328	**0.873**	*0.389*	**ISC6**	3.814
ISC7	*0.768*	0.123	**0.697**	*0.394*	**ISC7**	1.191
OCB1	*0.251*	0.148	*0.359*	**0.788**	**OCB1**	1.517
OCB2	*0.403*	0.145	*0.455*	**0.893**	**OCB2**	1.925
OCB3	*0.363*	0.152	*0.370*	**0.802**	**OCB3**	1.566

Figure 7 covers the measurement model by showing the loadings of the items and the R-square of the main outcome variable.

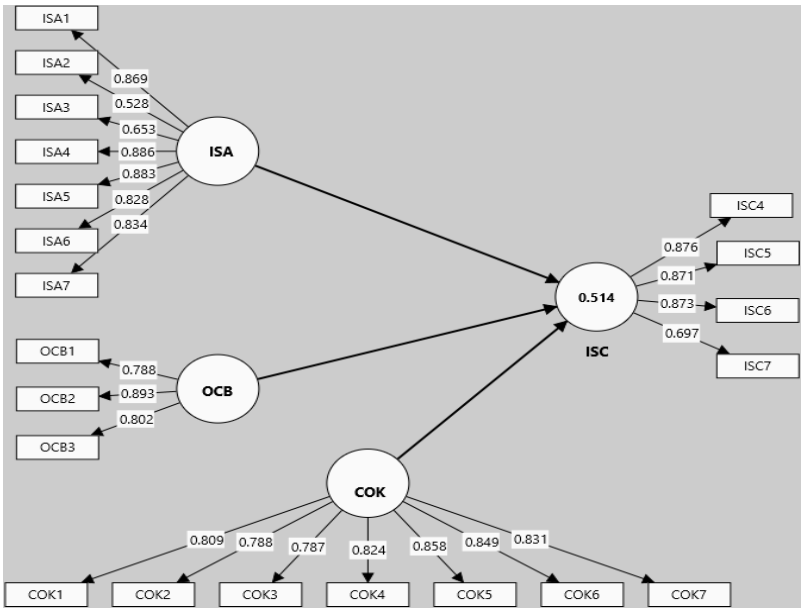

Figure 7: Measurement Model Output using the Items' Loadings and R-square.

The output of the structural equation model by applying the Smart PLS version 4 is given in Table 9. The study investigated the following three paths: COK -> ISC, ISA -> ISC, and OCB -> ISC. More specifically, the first step was to check the impact of the COK on the ISC for respondents from different public and private sector universities in China. The original sample and the sample mean represent the path coefficients as observed. However, for the simplicity of the analysis, the study goes with the coefficients found using the original sample output. The coefficient for the COK to ISC is 0.527, reflecting a positive impact of the COK on the ISC, provided that rest of the factors were constant when accounting for this change in the ISC. The standard deviation of this coefficient is 0.044, leading to a t-statistics of 12.031 and a p-value of 0.000. Both the t-value and the p-value favor keeping the level of significance at 1%. Overall, the results state that COK or compliance knowledge is positively associated with information security compliance.

A positive role of compliance knowledge for higher information security compliance reflects many dimensions. For example, understanding compliance knowledge is crucial for effectively performing one's role (in our case, the university employees either working through contractual job or regular), especially when navigating laws and regulations. When university employees are well aware of the specific laws that apply to their tasks, they can approach their responsibilities with greater confidence. This foundational understanding enables them to adapt to changes, such as new regulations or amendments. For such purposes, knowing what has been enacted or altered can reasonably help the employees to align their actions with current legal standards. As a result, there is an improvement in the employees' ability to manage information security compliance. Moreover, a deeper understanding of the practices of information security compliance helps empower individuals to take responsibility for maintaining compliance in their roles and duties.

Table 9: Path Coefficients.

Variables	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
COK -> ISC	0.527	0.526	0.044	12.031	0.000
ISA -> ISC	0.204	0.207	0.048	4.241	0.000
OCB -> ISC	0.225	0.225	0.054	4.154	0.000

The second path aims to examine the impact of the ISA on the ISC using the coefficient of the original sample as 0.204 and the standard deviation of 0.048. The given t-statistics for this relationship is 4.241 and p-value is 0.000, observing a significant result at 1%. This means that ISA is leading towards an increase in information security compliance for the public and private sector universities when observed through structural equation modeling techniques. The study results can be explained in different perspectives.

From an organizational perspective, increased information security awareness among university employees, whether working through contract or through regular title, aims to foster a culture of compliance where such respondents become more aware of security policies and practices. This greater awareness can help reduce non-compliance and strengthen the institution's overall security. The additional debate further claims that from an educational viewpoint, the findings suggest universities should consider implementing thorough training programs focused on information security awareness. By providing individuals with the knowledge and skills to identify and respond to security threats, educational institutions like universities can build a more resilient environment to improve information security compliance. Furthermore, the results emphasize the need for ongoing communication and reinforcement of security policies, making compliance a collective responsibility throughout public and private sector universities. Ultimately, this comprehensive approach can lead to lasting improvements in information security compliance within the academic sector of China.

The third relationship as presented in Table 9 explored the impact of the OCB on the ISC for the given educational institutions in China. The results confirm that both the OCB and ISC are positively and significantly connected. This statement is well justified when the researcher has examined the direction of the coefficient and the p-value achieved. The coefficient under original sample is 0.225 and the p-value is 0.000, showing that a level of citizenship behaviour of the respondents means more compliance of information security and vice versa. The statements like taking proactive steps to enhance information security, including telling coworkers to follow security rules and procedures, addressing insecure computer usage, making suggestions for improvement, and staying informed about relevant security guidelines have well justified the measurement of the organizational citizenship behaviour; however, fourth item of the model was removed due to lower factor loadings. The results show that the remaining three items have collectively played a significant role in measuring the entire construct of the OCB and determining a positive and significant change in the information security compliance.

Additionally, employees who demonstrate Organizational Citizenship Behavior are crucial for improving university information security compliance. Their inclination to communicate openly helps to create a transparent environment where information about security policies and best practices is easily shared. The other beneficial outcomes include such openness, which encourages the employees to stay well-updated about the compliance requirements. As a result, OCB also fosters a supportive culture within the organization where colleagues from different departments and in the same departments can assist one another in understanding and applying security measures. When individuals remind and motivate each other to follow security protocols as set by the organization, it builds a sense of shared responsibility that boosts compliance efforts.

Moreover, those employees who aim to exhibit OCB often take the initiative to spot potential security risks and suggest improvements, tackling vulnerabilities before they become serious compliance issues. A workplace that values organizational citizenship behaviour also tends to have higher job satisfaction and morale. Moreover, when employees feel appreciated and engaged, they are more likely to recognize the importance of compliance for information security towards the organizational success. Furthermore, employees who practice organization citizenship behaviour set a positive example for their peers and, ultimately, demonstrate a commitment to ethical behavior and adherence to security protocols. Finally, organization citizenship behaviour encourages involvement in training programs and the exchange of knowledge about information security, which enhances awareness and skills. At the end such skill development also boosts and strengthens the organization's compliance capabilities.

The presentation of the structural model output using Figure 8 has well covered the nexus between the variables along with the R-square of the model as linked with information security compliance. The given model shows that the R-square is 0.51 or 51%, which claims that all the independent variables have reflected this change in the ISC above the moderate level. However, by adding more variables into the model, it is anticipated that this value of R-square will be increased on substantial grounds. For this purpose, the researchers for the upcoming studies are instructed to properly review the past studies linked with the key determinants of information security compliance in different economies. Moreover, any theoretical background can provide enough justification to add more variables to this model. The other graphical presentation of the study coefficients using the bell-shaped diagram has been provided using Figures 9 to Figure 11.

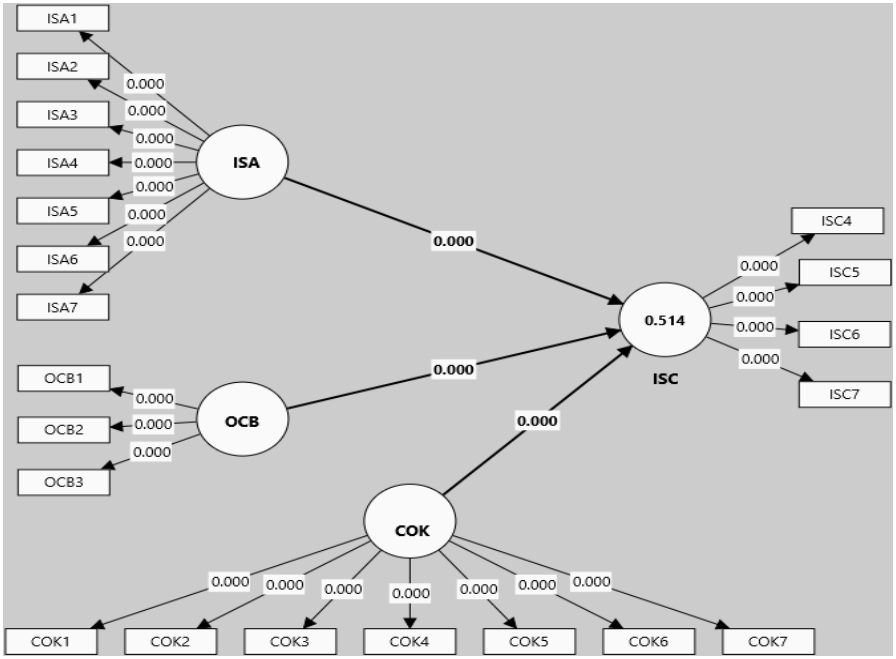

Figure 8: SEM Output (Inner Model; P-values), ISC; R-square.

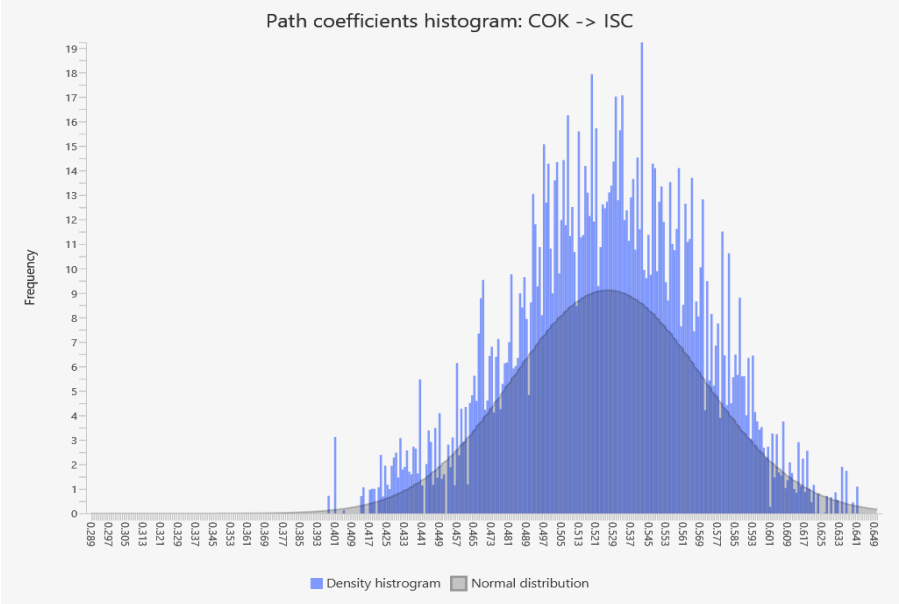

Figure 9: Path Coefficient Histogram for COK> ISC.

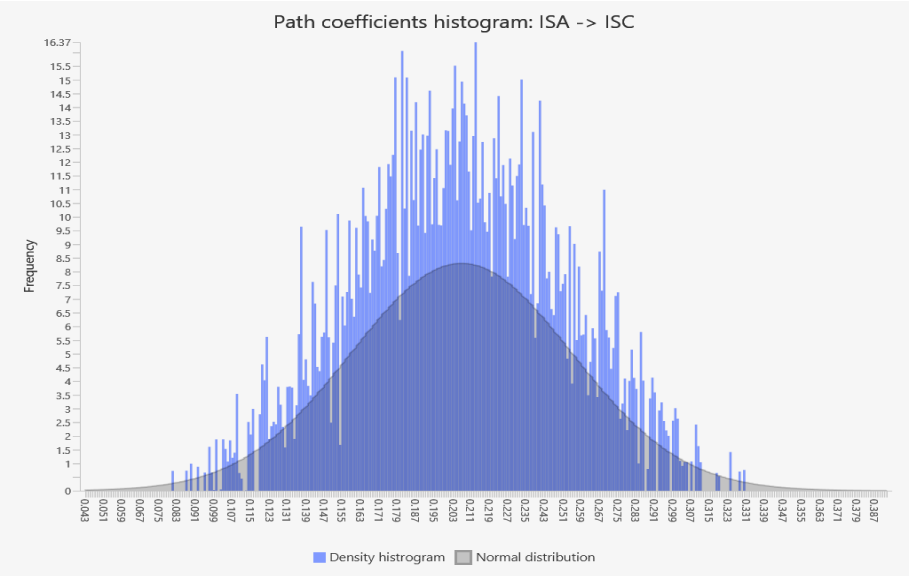

Figure 10: Path Coefficients for ISA→ ISC.

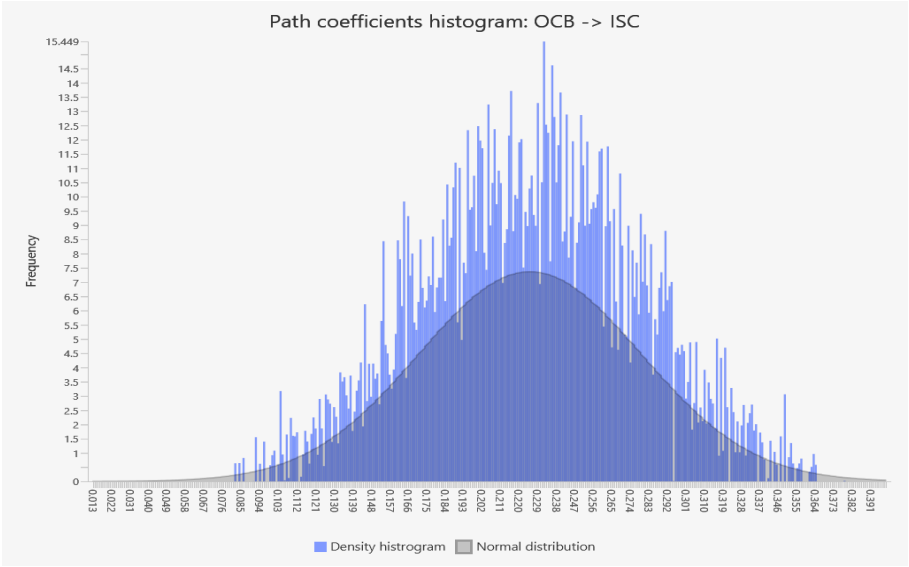

Figure 11: Path Coefficients for OCB→ ISC.

5. Conclusion and Recommendations

This study was conducted in China using a sample of employees from both public and private sector universities. The results have been presented using the inner and outer model testing under Smart PLS version 4. The main findings reveal that compliance knowledge, information security awareness and organization citizenship behaviour are leading determinants of information security compliance for the respondents. The given results are based on testing the reliability, convergent validity, and discriminant validity of the variables using the most relevant and reliable items. For practical implications, the study has several outstanding policies to be implemented by the public sector universities in China and other regions of the world.

In the first step, it is recommended that universities (both public and private) implement regular training sessions for their contractual and regular employees to increase awareness of security threats, data protection, and compliance standards. These workshops should focus on practical applications to emphasize the importance of following security policies and rules defined by the organization. Universities should also develop and share clear information security policies based on consequences of non-compliance. However, it is important to note that keeping and considering these policies updated and ensuring they are communicated across different organizational levels is essential for staying aligned with current security standards. The other possible suggestions indicate the inclusion of information security topics in academic courses, especially in IT-related fields. This step would help to create a security-conscious mindset among students while engaging the teachers and other staff at the same point of time. Additionally, university leadership should promote a security culture by setting a good example. Besides, a regular communication from top management about the importance of information security compliance would encourage greater participation across the institution and within the departments.

In the second step, based upon the positive relationship between compliance knowledge and information security compliance, the study would like to suggest the following recommendations for the administration at both public and private universities. The university demonstration is recommended to introduce an information security certification program for all the staff members, specifically those directly connected with the computer systems. The program should be based on the idea that every university employee needs to reach a specific level of knowledge entitled as security compliance. The linkage of these certification programs with performance and job appraisal should be directly connected to achieve better results over a longer time. The other possible suggestions and practical implications cover the appointment of the information security ambassadors from different departments who would be a major role player for promoting such programs within and outside the organizations. The administration of the universities can also create a dashboard system that gives staff real-time updates on their ISC. Each employee could have a personal dashboard that shows their progress in the form of completed compliance activities, their level of knowledge and understanding, and any security risks they need to be aware of. All of the above suggestions would reasonably help the staff members and administration stay informed and take action to maintain security standards efficiently.

In the third step, the study suggests policy recommendations for promoting organizational citizenship behaviour toward higher information security compliance. It is recommended that universities foster a culture of "responsible employees" where the employees are responsible not only for their actions but also for supporting their colleagues for higher information security compliance. However, not recognizing and rewarding those employees who are reflecting such type of productive behaviour will discourage and demotivate the same individuals. Therefore, the organizational culture should be based upon recognizing and rewarding those employees who are performing for improved organizational citizenship behaviour. Besides other possible suggestions include promoting transparent communication, providing regular training and involvement, and leading by example regarding organizational citizenship behaviour, respectively.

References

Ab Hamid, Mohd Rashid; Sami, Waqas; Sidek, M H Mohmad. (2017). "Discriminant validity assessment: Use of Fornell & Larcker criterion versus HTMT criterion". *Journal of Physics: Conference Series,* v. 890, n. 1, pp. 012163. *https://doi.org/10.1088/1742-6596/890/1/012163*

Abraham, Sherly. (2011). "Information Security Behavior: Factors and Research Directions". *AMCIS 2011 Proceedings - All Submissions,* pp. 462. *https://aisel.aisnet.org/amcis2011_submissions/462*

Afthanorhan, Asyraf; Ghazali, Puspa Liza; Rashid, Norfadzilah. (2021). "Discriminant Validity: A Comparison of CBSEM and Consistent PLS using Fornell & Larcker and HTMT Approaches". *Journal of Physics: Conference Series,* v. 1874, n. 1, pp. 012085. *https://doi.org/10.1088/1742-6596/1874/1/012085*

Ajzen, I.; Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behavior*. Englewood Cliffs, NJ: Prentice-Hall.

Ajzen, Icek. (1991). "The Theory of Planned Behavior". *Organizational Behavior and Human Decision Processes,* v. 50, n. 2, pp. 179-211. *https://doi.org/10.1016/0749-5978(91)90020-T*

Ali, Rao Faizan; Dominic, P D D; Ali, Syed Emad Azhar; Rehman, Mobashar; Sohail, Abid. (2021). "Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance". *Applied Sciences,* v. 11, n. 8, pp. 3383. *https://doi.org/10.3390/app11083383*

Amankwa, Eric; Loock, Marianne; Kritzinger, Elmarie. (2014). "A Conceptual Analysis of Information Security Education, Information Security Training and Information Security Awareness Definitions." In: *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014).* pp. 248-252. IEEE. *https://doi.org/10.1109/ICITST.2014.7038814*

Amini, Masoumeh; Vakilimofrad, Hossein; Saberi, Mohammad Karim. (2021). "Human Factors Affecting Information Security in Libraries". *The Bottom Line,* v. 34, n. 1, pp. 45-67. *https://doi.org/10.1108/BL-04-2020-0029*

Awais Rashid, Hafiz Muhammad; Ghazzali, Muhammad; Waqas, Umer; Malik, Adnan Anwar; Abubakar, Muhammad Zubair. (2021). "Artificial Intelligence-Based Modeling for the Estimation of Q-Factor and Elastic Young's Modulus of Sandstones Deteriorated by a Wetting-Drying Cyclic Process". *Archives of Mining Sciences,* v. 66, n. 4, pp. 635-658. *https://doi.org/10.24425/ams.2021.138944*

Bandura, A. (1986). *Social Foundations of Thought and Action: A Cognitive Social Theory*. Englewood Cliffs, NJ: Prentice-Hall.

Bauer, Stefan; Bernroider, Edward W N; Chudzikowski, Katharina. (2017). "Prevention is Better Than Cure! Designing Information Security Awareness Programs to Overcome Users' Non-compliance with Information Security Policies in Banks". *Computers & Security,* v. 68, pp. 145-159. *https://doi.org/10.1016/j.cose.2017.04.009*

Bulgurcu, Burcu; Cavusoglu, Hasan; Benbasat, Izak. (2010). "Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness". *MIS Quarterly,* v. 34, n. 3, pp. 523-548. *https://doi.org/10.2307/25750690*

Choobineh, Joobin; Dhillon, Gurpreet; Grimaila, Michael R; Rees, Jackie. (2007). "Management of Information Security: Challenges and Research Directions". *Communications of the Association for Information Systems,* v. 20, n. 1, pp. 57. *https://doi.org/10.17705/1CAIS.02057*

Da Veiga, Adele; Astakhova, Liudmila V; Botha, Adéle; Herselman, Marlien. (2020). "Defining organisational information security culture—Perspectives from academia and industry". *Computers & Security,* v. 92, pp. 101713. *https://doi.org/10.1016/j.cose.2020.101713*

Ecek, Nurgül; Çakmak, Ahmet Ferda. (2022). "Çalışanların Bilgi Güvenliği Önlemlerine Dair Tutumları: Ampirik Bir Değerlendirme". *International Journal of Applied Economic and Finance Studies,* v. 7, n. 2, pp. 26-44. *http://www.ijaefs.com/wp-content/uploads/2022/12/02_ECE-CAKMAK.pdf*

Farid, Ghulam; Warraich, Nosheen Fatima; Iftikhar, Sadaf. (2023). "Digital Information Security Management Policy in Academic Libraries: A Systematic Review (2010–2022)". *Journal of Information Science,* pp. 01655515231160026. *https://doi.org/10.1177/01655515231160026*

Farrell, Andrew M. (2010). "Insufficient Discriminant Validity: A Comment on Bove, Pervan, Beatty, and Shiu (2009)". *Journal of Business Research,* v. 63, n. 3, pp. 324-327. *https://doi.org/10.1016/j.jbusres.2009.05.003*

Guo, Ken H. (2013). "Security-Related Behavior in Using Information Systems in the Workplace: A Review and Synthesis". *Computers & Security,* v. 32, pp. 242-251. *https://doi.org/10.1016/j.cose.2012.10.003*

Hair, Joseph F.; Hult, G. Tomas M.; Ringle, Christian M.; Sarstedt, Marko; Danks, Nicholas P.; Ray, Soumya. (2021). "Evaluation of Reflective Measurement Models." In: *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook.* Hair Jr, Joseph F.; Hult, G. Tomas M.; Ringle, Christian M.; Sarstedt, Marko; Danks, Nicholas P.; Ray, Soumya (Eds.), pp. 75-90. Cham:Springer International Publishing. *https://doi.org/10.1007/978-3-030-80519-7_4*

Hamad, Faten; Al-Fadel, Maha; Fakhouri, Hussam. (2023). "The Provision of Smart Service at Academic Libraries and Associated Challenges". *Journal of Librarianship and Information Science,* v. 55, n. 4, pp. 960-971. *https://doi.org/10.1177/09610006221114173*

Hart, Stephen; Margheri, Andrea; Paci, Federica; Sassone, Vladimiro. (2020). "Riskio: a Serious Game for Cyber Security Awareness and Education". *Computers & Security,* v. 95, pp. 101827. *https://doi.org/10.1016/j.cose.2020.101827*

Herath, Tejaswini; Rao, H Raghav. (2009). "Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organisations". *European Journal of Information Systems,* v. 18, n. 2, pp. 106-125. *https://doi.org/10.1057/ejis.2009.6*

Ifinedo, Princely. (2012). "Understanding Information Systems Security Policy Compliance: an Integration of the Theory of Planned Behavior and the Protection Motivation Theory". *Computers & Security,* v. 31, n. 1, pp. 83-95. *https://doi.org/10.1016/j.cose.2011.10.007*

Jianjun, Hou; Yao, Yi; Hameed, Javaria; Kamran, Hafiz Waqas; Nawaz, Muhammad Atif; Aqdas, Ramaisa; Patwary, Ataul Karim. (2021). "The role of artificial and nonartificial intelligence in the new product success with moderating role of new product innovation: a case of manufacturing companies in China". *Complexity,* v. 2021, n. 1, pp. 8891298. *https://doi.org/10.1155/2021/8891298*

Kavak, Ali. (2024). "Impact of information security awareness on information security compliance of academic library staff in Türkiye". *The Journal of Academic Librarianship,* v. 50, n. 5, pp. 102937. *https://doi.org/10.1016/j.acalib.2024.102937*

Kavak, Ali; Odabaş, Hüseyin. (2023). "The impact of information security management guide utilization on technological and institutional information security measures in university libraries in Türkiye". *The Journal of Academic Librarianship,* v. 49, n. 6, pp. 102800. *https://doi.org/10.1016/j.acalib.2023.102800*

Khando, Khando; Gao, Shang; Islam, Sirajul M.; Salman, Ali. (2021). "Enhancing employees information security awareness in private and public organisations: A systematic literature review". *Computers & Security,* v. 106, pp. 102267. *https://doi.org/10.1016/j.cose.2021.102267*

Kim, Sang Soo; Kim, Yong Jin. (2017). "The Effect of Compliance Knowledge and Compliance Support Systems on Information Security Compliance Behavior". *Journal of Knowledge Management,* v. 21, n. 4, pp. 986-1010. *https://doi.org/10.1108/JKM-08-2016-0353*

LePine, Jeffrey A; Erez, Amir; Johnson, Diane E. (2002). "The Nature and Dimensionality of Organizational Citizenship Behavior: a Critical Review and Meta-analysis". *Journal of Applied Psychology,* v. 87, n. 1, pp. 52-65. *https://doi.org/10.1037/0021-9010.87.1.52*

Li, Jin; Zhang, Liwen; Zhou, Jiani; Wang, Geng; Zhang, Rui; Liu, Jiaqing; Liu, Shili; Chen, Yong; Yang, Song; Yuan, Quan; Li, Ying. (2022). "Development and validation of self-management scale for tuberculosis patients". *BMC Infectious Diseases,* v. 22, n. 1, pp. 502. *https://doi.org/10.1186/s12879-022-07483-3*

Marett, Kent; Barnett, Tim. (2021). "Information Security Practices in Small-to-Medium Sized Businesses: A Hotspot Analysis." In: *Research Anthology on Small Business Strategies for Success and Survival.* pp. 576-596. IGI Global. *https://doi.org/10.4018/978-1-7998-9155-0.ch029*

Mattord, Herbert; Kotwica, Kathleen; Whitman, Michael; Battaglia, Evan. (2024). "Organizational Perspectives on Converged Security Operations". *Information & Computer Security,* v. 32, n. 2, pp. 218-235. *https://doi.org/10.1108/ICS-03-2023-0029*

Nielsen, Tjai M; Bachrach, Daniel G; Sundstrom, Eric; Halfhill, Terry R. (2012). "Utility of OCB: Organizational Citizenship Behavior and Group Performance in a Resource Allocation Framework". *Journal of Management,* v. 38, n. 2, pp. 668-694. *https://doi.org/10.1177/0149206309356326*

Oluwabunmi, Mabawonku Temitope; Madukoma, Ezinwanyi. (2022). "Information Security Awareness and Information Security Compliance in University Libraries in South-West, Nigeria". *Library Philosophy and Practice (e-journal),* pp. 7215. *https://digitalcommons.unl.edu/libphilprac/7215*

Organ, Dennis W. (1988). "A Restatement of the Satisfaction-Performance Hypothesis". *Journal of Management,* v. 14, n. 4, pp. 547-557. *https://doi.org/10.1177/014920638801400405*

Organ, Dennis W. (1990). "The Motivational Basis of Organizational Citizenship Behavior". *Research in Organizational Behavior,* v. 12, n. 1, pp. 43-72. *http://ereserve.library.utah.edu/Annual/MGT/7800/Tenney/organ.pdf*

Organ, Dennis W; Podsakoff, Philip M; MacKenzie, Scott B. (2005). *Organizational Citizenship Behavior: Its Nature, Antecedents, and Consequences*. Sage Publications. *https://doi.org/10.4135/9781452231082*

Organ, Dennis W; Ryan, Katherine. (1995). "A Meta-Analytic Review of Attitudinal and Dispositional Predictors of Organizational Citizenship Behavior". *Personnel Psychology,* v. 48, n. 4, pp. 775-802. *https://doi.org/10.1111/j.1744-6570.1995.tb01781.x*

Organ, Dennis W. (1997). "Organizational Citizenship Behavior: It's Construct Clean-Up Time". *Human Performance,* v. 10, n. 2, pp. 85-97. *https://doi.org/10.1207/s15327043hup1002_2*

Özdemir, Ayşe; Uluyol, Çelebi. (2020). "Kamu Kurum ve Kuruluslarında Bilgi Güvenligi Farkındalıgı". *Türkiye Sosyal Araştırmalar Dergisi,* v. 25, n. 1, pp. 649-666. *https://doi.org/10.20296/tsadergisi.815635*

Rasoolimanesh, S Mostafa. (2022). "Discriminant validity assessment in PLS-SEM: A comprehensive composite-based approach". *Data Analysis Perspectives Journal,* v. 3, n. 2, pp. 1-8. *https://scriptwarp.com/dapj/2022_DAPJ_3_2/Rasoolimanesh_2022_DAPJ_3_2_DiscriminantValidity.pdf*

Scarfone, Karen; Souppaya, Murugiah. (2009). "Guide to Enterprise Password Management (Draft)". *NIST Special Publication,* v. 800, n. 118, pp. 800-118. *https://www.tier3md.com/media/800-118.pdf*

Sharma, Japuji K. (2010). *Fundamentals of Business Statistics*. Vikas Publishing House. *https://www.vikaspublishing.com/books/business-economics/economics/business-statistics/9789353387273*

Sharma, Japuji K. (2012). *Business Statistics*. Pearson Education India.

Siponen, Mikko T. (2000). "A Conceptual Foundation for Organizational Information Security Awareness". *Information Management & Computer Security,* v. 8, n. 1, pp. 31-41. *https://doi.org/10.1108/09685220010371394*

Siponen, Mikko; Vance, Anthony. (2010). "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations". *MIS Quarterly,* v. 34, n. 3, pp. 487-502. *https://doi.org/10.2307/25750688*

Sohrabi Safa, Nader; Von Solms, Rossouw; Furnell, Steven. (2016). "Information Security Policy Compliance Model in Organizations". *Computers & Security,* v. 56, pp. 70-82. *https://doi.org/10.1016/j.cose.2015.10.006*

Soomro, Zahoor Ahmed; Shah, Mahmood Hussain; Ahmed, Javed. (2016). "Information Security Management Needs More Holistic Approach: a Literature Review". *International Journal of Information Management,* v. 36, n. 2, pp. 215-225. *https://doi.org/10.1016/j.ijinfomgt.2015.11.009*

Turel, Ofir; Xu, Zhengchuan; Guo, Ken. (2020). "Organizational Citizenship Behavior Regarding Security: Leadership Approach Perspective". *Journal of Computer Information Systems,* v. 60, n. 1, pp. 61-75. *https://doi.org/10.1080/08874417.2017.1400928*

Vedadi, Ali; Warkentin, Merrill; Straub, Detmar W; Shropshire, Jordan. (2024). "Fostering Information Security Compliance as Organizational Citizenship Behavior". *Information & Management,* v. 61, n. 5, pp. 103968. *https://doi.org/10.1016/j.im.2024.103968*

Whitman, Michael E; Mattord, Herbert J. (2011). *Roadmap to Information Security: For IT and Infosec Managers*. Delmar Learning. *https://digitalcommons.kennesaw.edu/facpubs/1443*

Whitman, Michael E; Mattord, Herbert J. (2019). *Management of Information Security*. Cengage Learning. *https://thuvienso.hoasen.edu.vn/handle/123456789/9285*

Whitman, Michael; Mattord, Herbert. (2023). "Meeting the Challenges of Large Online Graduate Cybersecurity Classes in the Age of COVID". *Journal of The Colloquium for Information Systems Security Education,* v. 10, n. 1, pp. 1-6. *https://doi.org/10.53735/cisse.v10i1.165*

Ye, Maoran; Hao, Feng; Shahzad, Mohsin; Kamran, Hafiz Waqas. (2022). "How Green Organizational Strategy and Environmental CSR Affect Organizational Sustainable Performance Through Green Technology Innovation Amid COVID-19". *Frontiers in Environmental Science,* v. 10, pp. 959260. *https://doi.org/10.3389/fenvs.2022.959260*

Yusoff, Ahmad Shidki Mat; Peng, Fan Siong; Abd Razak, Fahmi Zaidi; Mustafa, Wan Azani. (2020). "Discriminant Validity Assessment of Religious Teacher Acceptance: The Use of HTMT Criterion". *Journal of Physics: Conference Series,* v. 1529, n. 4, pp. 042045. *https://doi.org/10.1088/1742-6596/1529/4/042045*