International Journal of Business Innovation and Research

ISSN online: 1751-0260 - ISSN print: 1751-0252
https://www.inderscience.com/ijbir

The security environment in Indian commercial banks: an employee's information security behaviour perspective

S. Prasanna, V. Mariappan, K.A. Asraar Ahmed, V.S. Damodharan

DOI: 10.1504/IJBIR.2022.10050939

Article History:

Received:	25 February 2022
Accepted:	04 August 2022
Published online:	05 June 2024

The security environment in Indian commercial banks: an employee's information security behaviour perspective

S. Prasanna*

Department of Management Studies,
B.S. Abdur Rehman Crescent Institute of Science & Technology,
Tamil Nadu, 600-048, India
Email: prasanna.res@gmail.com
*Corresponding author

V. Mariappan

Department of Banking Technology,
Pondicherry University,
R.V. Nagar, Kalapet, Puducherry, 605-014, India
Email: vmarisinn@gmail.com

K.A. Asraar Ahmed

VIT-AP School of Business,
VIT-AP University,
G-30, Inavolu, Beside AP Secretariat, Amaravati,
Andhra Pradesh, 522-237, India
Email: asraarvit@gmail.com

V.S. Damodharan

Abu Dhabi Vocational Education and Training Institute,
Al Jazirah Institute of Science and Technology,
Post Box No. 95005, Rabdan, Abu Dhabi, United Arab Emirates
Email: sriramdams@gmail.com

Abstract: The drastic changes in technology profoundly influence organisational performance in the ICT-dominated business environment; hence, no organisation can afford to undermine technology adoption in their operations and management. However, while such technologies have benefited organisations immensely, they are not free from concerns, especially related to information security threats from outside and within the organisation, including the employees. The current study explores the information security issues emanating from employees' information security awareness, attitude, policies, and employees' information security behaviour. A structured questionnaire was administered among 420 public and private sector bank employees, and 389 responses were considered for the final analysis. Results from the structured equation modelling analysis indicate that employees' attitudes towards subjective norms and information security profoundly and positively

influence their information security behaviour. Information security policy (ISP) characteristics and awareness have played an important role in shaping employees' attitudes towards ISP compliance. The findings also provide insight into factors that do not influence employees' information security behaviours (ISB) that can help the bank management improve in this area with a suitable policy framework in the future.

Keywords: information security behaviour; ISB; information security policy; ISP; information security awareness; subjective norms; cognitive evaluation theory; theory of planned behaviour.

Reference to this paper should be made as follows: Prasanna, S., Mariappan, V., Ahmed, K.A.A. and Damodharan, V.S. (2024) 'The security environment in Indian commercial banks: an employee's information security behaviour perspective', *Int. J. Business Innovation and Research*, Vol. 34, No. 2, pp.277–298.

Biographical notes: S. Prasanna is an Assistant Professor at the Department of Management Studies, BSA Crescent Institute of Science & Technology, Chennai, Tamil Nadu, India. He has received his Doctorate (PhD) from the Pondicherry University, India in the area of 'Information Security Behaviour'. He is a recipient of National Eligibility Test (NET) certificates by India's University Grants Commission Government. He is a Certified Associate of the Indian Institute of Banker (CAIIB), Certified Compliance Professional, NSE Certified Market Professional V, and Fellow of Insurance Institute of India. He has both teaching and industry experience. He has been an author of articles published in reputed journals. His main area academic activities focus on the management of the human resource, research methodology and analytics.

V. Mariappan is a Professor of Banking Technology, and has over 26 years of experience in teaching. He has published articles in refereed indexed journals and conference proceedings. He has over eight completed funded projects. His main academic streams of interest include accounting and finance, banking regulation and operations, cyber-crimes in banks and IT laws.

K.A. Asraar Ahmed is currently working as an Assistant Professor Senior Grade-1 at the VIT-AP School of Business, VIT-AP University, Amravati, Andhra Pradesh. He received his Doctor of Philosophy from the VIT University, Vellore, India. He has published research articles in Scopus/ABDC-listed journals in the areas of marketing and technology adoption. He is an expert in teaching business analytics, HR analytics, data analytics using Excel/R/SPSS/Tableau, machine learning using R/Python, marketing management, marketing research and analytics and quantitative methods. He has conducted several workshops, faculty development programs and management development programs on structural equation modelling using R, SPSS, AMOS, Smart PLS, and business analytics using Advanced Excel, R and Tableau.

V.S. Damodharan is an academician, professional chartered and management accountant, and data analyst with ACBSP Teaching Excellence Award from the ACBSP, USA. He holds a PhD in Entrepreneurship and Master of Philosophy in Accounting and Finance. He is a qualified Chartered Accountant in the ACCA, UK, Management Accountant, and Certified Management Accountant (CMA) of IMA USA. He is an Associate Cost and Management Accountant (ACMA) from India. He has two decades of experience in education and consulting experience in the MENA and Asia regions. His expertise includes data analytics, finance, accounting, management accounting, CRM, and entrepreneurship.

1 Introduction

The drastic changes in the technological advent in ICT have revolutionised many sectors, and banking has greatly reaped the benefits of such advancement and incorporated many changes in the management of banks, especially banking operations, to benefit the banks and their customers. At the same time, the usage of technology and its features have provided banks with new opportunities and challenges. Technology usage is not without added risk in terms of cyber security threats to the bank (Godbole et al., 2022) and its customers, despite various technological solutions like firewalls, anti-malware and antivirus software. Bank employees are considered the weakest link in the digital banking space as they expose themselves to information security risks through their behaviour (Sasse et al., 2001; Pahnila et al., 2007), like sharing system passwords and downloading attachments from unknown emails and so on, leading to cyber-attacks. Such attacks result in monetary loss and damage the organisation's reputation (Safa and Ismail, 2013). Hackers siphoned off millions of rupees from Indian banks by compromising the SWIFT system due to poor information security behaviour (ISB) exhibited by the bank employees who downloaded malware attachments (Sudarshan, 2018).

Further, over 290,000 security incidents have been reported against the Indian banking industry during 2020 (Press Trust of India, 2021), a severe concern for the banks. A bank's success in protecting information assets and resources depends on how well its employees handle the technology-based solutions in their banks (Vroom and Von Solms, 2004; Shropshire et al., 2015). The only way to effectively mitigate a bank's information security risk is a good employee 'security-aware behaviour' (Ali et al., 2021) combined with a robust technological solution. The major reason for a prominent number of cyber-attacks is due to exploitation of employees (Khando et al., 2021). Organisations shape their employees' ISB through a comprehensive security policy document and arrangement, detailed procedures and rules (Son, 2011; Hu et al., 2011). However, the literature reveals that employees do not follow the rules and guidelines in the policy document (Merhi and Ahluwalia, 2019; Ifinedo, 2012) as other personal and organisational factors impede their behaviours. Some of the studies also reveal that information security awareness among employees plays a significant role in protecting an organisation's information assets by shaping appropriate information behaviour in the employees (Abawajy, 2014; Wu et al., 2017). The information security awareness that stems from learning, training, and experience will shape employee attitudes (Parsons et al., 2014). The understanding also helps employees toward organisation information security, enhances their perception of the capability to conform to organisation information security policy (ISP) (Al-Omari et al., 2012), and improves their ability and skills to handle security incidents (Safa and Ismail, 2013).

On the other hand, employee negligence in information security is a serious risk to an organisation's information assets, and employees' attitude plays a significant role in avoiding such negligence. Studies related to the influence of employees' attitudes on their behaviours indicate that attitude has a vital role in shaping their behaviour, and factors like awareness, management support, knowledge sharing, commitment, experience, and personal norms positively influence employee attitude (Anderson and Agarwal, 2010; Pahnila et al., 2007; Hu et al., 2012; Lee and Kozar, 2005; Zhang et al., 2009). Further, when confronted with mandatory measures leading to forced behaviour, the attitude of the employees gets changed, and there is a delay in their action till it is warranted.

Organisations that aim to create conditions that facilitate required behaviour among employees rather than through mandatory requirements can achieve better benefits in the long-term. Similarly, an appropriate reward motivates employees towards acceptable behaviour and plays a crucial role in developing required behaviours among employees. Little rewards may not (Siponen et al., 2010) or negatively influence employees (Vance et al., 2012), leading to unwanted behaviour that exposes the organisation's information security at risk. Similarly, a subjective norm that reflects the influence of one's opinion on others' decisions plays a crucial role in organisational information settings where employees are required to meet the expectations of significant people like managers, supervisors and co-workers (Cheng et al., 2013). Many researchers have developed successful information security models by incorporating theories from various disciplines like sociology, criminology and psychology. Lin et al. (2022) and Nasirpouri Shadbad and Biros (2021) recommended studying more on employee-related aspects that affect ISB. Ali et al. (2021) in their systematic review on compliance towards ISB recommended more investigation on employee ISB.

Hence, this paper attempts to study the ISBs of employees of Indian commercial banks to assess the information security status prevailing in the Indian banking industry. The report is structured as follows. Section 1 provides the backdrop for the study as an introduction. Section 2 discusses the theories that aided the present research model, and the hypothesis developed for the current study. The research methodology employed in the study is discussed in the Section 3. While section 4, discusses the analysis employed, including measurement and structured model, Section 5 discusses the study's findings and contribution to managerial implications. Section 6 provides the conclusions of the study, and Section 7 explained the limitations. Finally, Section 8 provides the scope for future research.

2 Literature review and hypothesis development

2.1 Theoretical foundations

In information security research, three theories are mainly employed: general deterrence theory, theory of planned behaviour and protection motivation theory (Lebek et al., 2014). Integrated models not only provide a more comprehensive explanation than a single theory model, but they also help the researcher gain a better understanding of ISB. The current study combined variables from the theory of planned behaviour and the cognitive evaluation theory to examine the most critical and plausible explanation of employees' ISB.

2.1.1 Theory of planned behaviour

Regarding information security, the theory of planned behaviour is one of the most extensively utilised theories for describing individual behaviour (Lebek et al., 2014; Hazari et al., 2008). The theory of reasoned action explains the impact of social influence (Friedkin, 1998) on individual behaviour, forming the basis for the theory of planned behaviour. The theory of planned behaviour explains variance in individual behaviour based on factors like perceived behavioural controls, subjective norms and attitude. Perceived behavioural control relates to one's beliefs about the efficacy and the resources

required to assist behaviour. Personal views about being approved and supported by the person or group of people who are important to them are reflected in subjective norms. An individual's favourable or unfavourable feelings toward certain items or things that play a substantial role in moulding individual behaviour are defined as an attitude. Attitude can be implicit or explicit. While implicit attitude unconsciously affects an individual's behaviour, a precise attitude consciously influences one's beliefs and behaviour. Ahmed and Damodharan (2021) and Damodharan and Ahmed (2022) stipulated that the application of the theory of planned behaviour as a theoretical background in understanding behaviour is highly recommended in business research. Awareness and knowledge significantly impact individual perspectives, and a specific understanding of the information security threats and their influences on individuals to engage in appropriate behaviour protects them from unnecessary risk (Byrne, 1994b). Further, the impact of subjective norms and attitude factors was significant in most studies undertaken in the information security domain (Wu et al., 2017). Ma (2022) applied TPB to understand the Chinese IT employees' ISB wherein he concluded that all the TPB variables had a significant influence on ISB and recommended more research on the ISB of employees in different sectors. Tam et al. (2022) identified that the subjective norm variable of TPB had a significant influence on ISB. The most critical impact of the theory of planned behaviour factors in explaining individual behaviour in the information security domain, the study incorporated attitudinal and subjective norm factors from TPB to understand its influence on bank employees' ISB.

2.1.2 Cognitive evaluation theory

The impact of external factors on an individual's internal motives is explained by cognitive evaluation theory, a psychological theory. The CET was designed to understand the influence of rewards on one's intrinsic motivation. The theory indicates that rewards will negatively influence one's motivation when individuals see them as a means of controlling their behaviour, especially when the rewards are tangible. However, CET predicted the positive influence of rewards on individual behaviour, especially when the rewards are verbal feedback. The positive and non-coercive feedback will improve employees' perception of performance evaluation and increase their belief in their competency in completing the task. When rewards control behaviour, an individual's perception of autonomy will decrease, resulting in negative consequences.

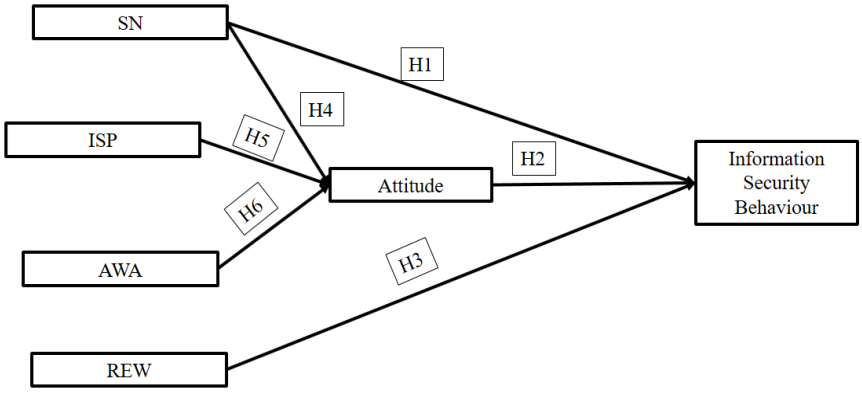
In contrast, if rewards increase their belief in competency, it will positively influence their behaviour. As a result, the researchers believe that rewards will significantly impact employees' ISB in an organisational setting where rewards encourage employees toward expected behaviour. As a result, the study predicts that rewards will considerably impact employee compliance.

2.2 Research hypotheses and model

A good ISB of the employees reduces security breaches and protects the organisation's information assets. Employees' attitudes towards ISP, the management's expectations to follow organisational ISP and rewards for appropriate information security practice will influence the employees' ISB. Employees' attitudes toward compliance with information security guidelines may also be affected by the characteristics of the organisation's ISP and employees' awareness of the risks associated with a security incident, as well as the

importance of protecting information assets to preserve the organisation's reputation. As a result, the current study model depicted in Figure 1 was constructed, considering the influence of the above criteria, available literature support, and expert comments and viewpoints.

Figure 1 Proposed hypotheses framework



2.2.1 Subjective norms

Individual beliefs about being approved and supported by the person or group of people who are important to them are reflected in subjective norms. Social pressure and motivation from others will drive individuals to behave in a particular manner (Safa et al., 2015). The subjective norms that reflect the influence of a person's opinion on others' decisions play a crucial role in organisational information settings where employees are required to meet the expectations of significant people like managers, supervisors, and co-workers (Cheng et al., 2013). Though subjective norms seem to influence one's behavioural intention (Safa et al., 2015; Grimes and Marquardson, 2019), some studies have established weaker associations and conflicting outcomes (Krueger et al., 2000). Tam et al. (2022) recommended for more investigations on the impact of subjective norms on employee ISB. Tam et al. (2022), Ma (2022) and Ali et al. (2021) recommended more investigations on the impact of subjective norms on employee ISB. Thus, to understand the influence of subjective norms in predicting employees' behaviours, the current study hypothesised that:

H1 Subjective norms positively influence employees' ISB.

2.2.2 Attitude

Attitude influences individuals' emotions and shapes their behaviour. An attitude which reflects an individual's positive or negative feelings about a specific object or thing plays a significant role in shaping their behaviour. Attitude is the primary component in the theory of planned behaviour, which explains the relationship between beliefs and behaviour (Safa et al., 2015). Further, the theory of planned behaviour indicates that a favourable attitude influences an individual's behaviour intention (Kumar and Dash, 2015; Bajaj et al., 2021) and an unfavourable attitude weakens such intentions. In the

context of organisational information security, employees' attitude toward ISP compliance influences their actual compliance behaviour (Pahnila et al., 2007). Employee behaviour, in turn, is affected by factors like awareness, subjective norms, threat appraisal, perceived fairness of ISP requirements, reward, punishments, and other facilitating conditions (Pahnila et al., 2007; Wu et al., 2017; Hu et al., 2012; Bulgurcu et al., 2009; Herath and Rao, 2009). A positive attitude towards ISP compliance leads to better ISB (Sasse et al., 2001) whilst an unfavourable attitude results in behaviour that affects organisational information security. Further, several studies have proved that employees' positive attitudes towards information security compliance result in inappropriate ISB (Ifinedo, 2012; Wu et al., 2017; Hu et al., 2012; Cox, 2012). Tam et al. (2022), Ma (2022) and Ali et al. (2021) recommended for more investigating the impact of attitude on employee ISB. Hence, understanding employees' attitude toward ISP compliance gains much attention from the employees' and organisational perspectives. Thus, the researchers hypothesised that:

H2 Employees' attitudes towards information security positively influence their ISB.

2.2.3 Rewards

In the workplace, rewards have been used as motivators to influence employee behaviour, as they anchor the organisation and the individual (Urban and Verachia, 2019). Rewards and recognition remain among the five most important organisational high involvement work practices (HIWE) (Kee and Rubel, 2021). Employee motivational rewards can be of a tangible or intangible nature and can include financial or non-financial rewards, personal mentions or appreciation from superiors. The significance of rewards in motivating employees towards desired behaviour depends on the task the employees are expected to perform. Generally, any rewards (Cameron et al., 2005) will motivate and improve the employees' performance on a task of low interest, but in the case of tasks of high interest in nature, appreciation and tangible rewards play an essential role in creating a positive effect. The study of Liu et al. (2021) revealed that there was no significant relationship between rewards and employee ISB among the employees of Chinese organisations and recommended more research on the impact of rewards on employee ISB in future studies. Ali et al. (2021) in their systematic review also revealed that there is a need for more investigation to understand the impact of rewards on employee ISB in future studies.

Further, non-significant rewards negatively influence employees' attitudes and can direct them towards unwarranted behaviours. Thus, by preventing the negative impact and improving the positive effect of the rewards, the organisation can drive their employees to the required ISB. Hence, the study hypothesised that:

H3 Rewards positively and significantly influence employees' behaviour on ISPs compliance.

2.2.4 Awareness

Awareness is a state of consciousness that helps individuals know, perceive and exhibit various behaviours. Individuals gain awareness through information from different sources like newspapers, workshops, policy documents, and direct experience. Training programs, games, and posters enhance one's awareness and knowledge level

(Albrechtsen and Hovden, 2010). Information security awareness relates to the state of consciousness where users understand and recognise the importance of rules and responsibilities and act prudently in safeguarding their information assets (Siponen et al., 2010). The critical dimensions of employees' information security awareness are general information security awareness. The employee relates to employees' knowledge and understanding of potential information threats and consequences. ISP awareness refers to employees' knowledge and experience of ISP compliance. Thus, employee information security awareness focuses on understanding the relevance of information security in the company and their commitment to safeguarding the organisation's information security assets (Kruger and Kearney, 2006). The information security awareness of the employee mainly affects the users' attitude and behaviour (Abawajy, 2014; Tam et al., 2022; Ma, 2022; Ratna and Mehra, 2015) and plays an influential role in organising information security management (Cavusoglu et al., 2009). Hadlington et al. (2020) recommended investigating more on the impact of awareness of employees on ISB. The current study attempts to comprehend the impact of employees' information security awareness on their attitude and subsequent behaviour. Hence, we hypothesised that:

H4 Information security awareness of the employees positively influences their attitudes toward information security.

2.2.5 Information security policy

An ISP encompasses policies, rules, and procedures to ensure that the organisation's network and its users meet at least the minimum-security requirements for protecting its information technology and data assets (Bulgurcu et al., 2010). ISP plays a significant role in creating positive employee attitudes towards organisation information security, leading to constructive ISB. The up-to-date, unfazed, clear, easy-to-understand and quickly accessible ISP will positively influence employees' attitudes rather than the confusing or outdated security policy. The findings of Parsons et al. (2014) reveal that the better the employees' knowledge of ISP, the better their attitude towards it. The studies of Alshaikh (2020), Hadlington et al. (2020), Nasirpouri Shadbad and Biros (2021) and Lin et al. (2022) concluded that a strong ISP had a significant positive influence on ISB. Shahbaznezhad et al. (2021) recommended more investigation on organisational factors that affect ISB. The present study aims to explore the impact of ISP on employees' attitudes on bank information security, which influences their behaviour, as ISP is a critical factor in protecting organisational information assets. Thus, the researchers hypothesised that:

H5 Organisation ISP characteristics have a significant and positive influence on employees' attitudes towards information security.

To sum up, the employees' behaviour in the form of complying with the organisation's ISP plays a vital role in managing information security incidents in the organisation. Whenever the employees are confronted with a situation that warrants behaviour against the organisation's ISP, the employees' awareness and knowledge of dos and don'ts in the organisation's ISP will remind them about the consequences of such behaviours and direct them not to get involved in such behaviours.

Thus, this study aims to understand why:

- Information security awareness and the characteristics of ISPs influence user attitudes regarding whether or not they want to follow information security guidelines.
- Subject norms, rewards, and attitudes influence employees' ISB.

3 Research methodology

The current study aims to understand the ISB of bank employees, who are considered the weakest link in an organisation's cyberspace and whose actions can result in a cyber risk for the banks. As poor ISB is the root cause of several organisations' information security threats, identifying factors influencing employees' ISB can help the bank management overcome cyber threats. ISB of employees is influenced by organisational factors like poor ISPs, lack of motivation and support, social norms, and individual factors like low awareness and the nasty attitude of individuals. Thus, understanding the influence of these factors will help the banks manage their employees' ISB and improve the information security environment.

As the research model portrayed in Figure 1 includes different factors with particular and interdependence relations, the SEM technique has been used for the analysis. Further fitness of the data to the hypothesised model and relationships among dependent and independent variables are tested through confirmatory factor analysis and structural modelling, respectively, using AMOS 20 software. Finally, the model's fitness has been tested through parameters like comparative fit index (CFI), goodness of fit index (GFI), root mean square error of approximation (RMSEA), normative fit index (NFI) and incremental fit index (IFI).

3.1 Questionnaire design

This study focuses on the ISB of commercial bank employees of different cadres working at public and private sector banks in the southern states of India. A structured questionnaire that includes questions on demographic profiles and the factors that influence and constitute employees' ISB has been designed based on the literature reviews and expert opinions. Further, to test the instrument adequacy in measuring the required constructs before drafting the final questionnaire, a pilot study was conducted among 40 bank employees belonging to different cadres. Based on the pilot study results and feedback, some questions that did not yield the desired reliability were altered. Based on the input, the seven-point Likert scale initially used in the survey was reduced to a five-point Likert scale for respondents' convenience. The refined questionnaire is administered again for testing with the same respondents to ensure clarity. The amended version of the questionnaire is considered the final version, with 37 questions measuring the employees' demographic profile and the factors considered in the study. The number of items representing each construct is shown in Table 1. Further, things used to describe the construct, along with the mean, standard deviation value, factor loading, and critical ratio, are presented in Table 3.

Table 1 Constructs and related number of items

Constructs	*Number of items*
Information security behaviour	5
Information security awareness	5
Information security policy characteristics	5
Attitude	5
Rewards	4
Subjective norm	5

Table 2 Demographic profile

Profile	*Factors*	*Classification*	*Frequency*	*Percentage*
Personal profile	Gender	Male	242	62.2
		Female	147	37.8
	Age	Below 30 years	205	52.7
		30–40 years	104	26.7
		41–50 years	39	10.0
		Above 50 years	41	10.5
	Educational qualification	Graduates	238	61.2
		Postgraduates	144	37.0
		Others	7	1.8
	Education stream	Engineering	147	37.8
		Non-engineering	242	62.2
Bank related profile	Sector	Public sector	211	54.2
		Private sector	178	45.8
	Branch location	Metro	74	19.0
		Urban	181	46.5
		Semi-urban	85	21.9
		Rural	49	12.6
	Designation	Clerk	154	39.6
		Officer	171	44.0
		Manager	64	16.4
	Experience	Below 5 years	189	48.6
		5–10 years	96	24.7
		11–15 years	40	10.3
		Above 15 years	64	16.4

Table 3 Latent variables and corresponding items

Latent variable	*Items*	*Mean*	*Std. dev.*	*Loadings*	*CR*
Attitude	Following organisation information security policy is a necessity	3.76	1.15	0.80	0.890
	Following organisation information security policy is beneficial	3.66	1.06	0.83	
	Following organisational information security policy is a good idea	3.88	1.16	0.88	
	Following organisational information security policy is important	3.59	1.11	0.80	
	Following organisation information security policy is valuable	3.76	0.97	0.61	
Information security behaviour	I abide with the organisation ISP to protect the organisation's information security	3.65	1.12	0.78	0.900
	I follow organisation information security policies in a prudent manner	3.76	1.14	0.80	
	I carry out my responsibilities as prescribed in the ISP of my organisation	3.66	1.05	0.84	
	I aid others in complying with organisation ISP	3.72	1.08	0.82	
	I will adhere to the organisation Information security policy strictly	3.74	1.07	0.77	
Subjective norm	Top management officials expects me to follow organisational ISPs	3.52	1.16	0.82	0.937
	My superior expects me to follow organisational information security policies	3.70	1.23	0.88	
	My peers expect me to follow organisational IS policies	3.74	1.21	0.89	
	My manager expects me to follow organisation IS policies	3.64	1.18	0.87	
	Information security personnel in the organisation expects me to follow with ISPs	3.78	1.21	0.86	
Rewards	I will get appreciation for following organisation information security policy	2.47	1.11	0.77	0.905
	If I comply with the information security policy of the organisation, I will receive personal mention in assessment reports	2.49	1.18	0.86	
	If I comply with the Information security policy of the organisation, I will get monetary rewards	2.48	1.16	0.84	
	I will get a non-monetary reward for complying organisation information security policy	2.64	1.15	0.88	
Information security policy characteristics	Information security guidelines and directives of my banks are generally clear	4.00	1.05	0.80	0.923
	My bank information security guidelines are easily accessible	3.97	0.95	0.84	
	My bank information security procedure is practicable for all levels	4.02	0.95	0.85	
	The responsibility associated with information security guidelines is indicated by banks	4.01	0.98	0.86	
	My organisation ISP is up to date	4.02	0.96	0.86	
Information security awareness	I am aware of potential security threats related to organisation information assets	3.89	1.15	0.79	0.918
	I have adequate knowledge about the cost of information security breaches	4.18	1.17	0.89	
	I understand the risk of information security incidents	3.90	1.12	0.80	
	I am aware of the importance of information security in protecting organisation information assets	3.94	1.13	0.81	
	I am aware that violation of organisational ISP will affect the organisation reputation	4.01	1.12	0.87	

3.2 Data collection

While an online survey can yield quicker responses and support faster data collection, it suffers from some drawbacks in the form of a lack of support from the researcher to the respondents while answering the question, as well as a higher probability of receiving responses from unintended respondents (Potoglou and Kanaroglou, 2007). Hence, the researchers mainly used personal surveys for data collection from the respondents and online surveys in a very minimal context where respondents lacked access. A model with seven or fewer constructs, each with more than three items, and lower communalities values of less than 0.45 necessitates a sample size of 150. In contrast, a model with modest communalities values of 0.5 requires a sample size of 300 (Hair et al., 2010). The present study has a sample of 420 bank employees covering public and private sector bank branches in southern India, such as Tamil Nadu, Andhra Pradesh, Telangana, Karnataka and Kerala. The study's respondents were selected using a stratified random sampling technique, considering several bank branches in the respective states as a factor for stratification. The state-wise sample distribution is as follows: Tamil Nadu (109), Andhra Pradesh (68), Telangana (51), Karnataka (99), and Kerala (62) for data collection. The authors have received 400 responses, 95.23% of the total sample size. During data cleaning, 11 answers were rejected due to unengaged responses and missing data, making the final sample size 389.

3.3 Respondent's profile

The respondents' profile includes respondents' personal and bank-associated information. While the personal profile includes age, gender, educational qualification, and stream of study, the bank-related profile has bank and branch category, designation and experience. Table 2 shows the descriptive statistics of the respondents whose responses are considered for the final analysis. Out of 389 responses considered for the study, 62.2% of responses are male employees, and the remaining 37.8% were female employees. While 52.4% of the respondents fall in the age group of fewer than 30 years, 40% hold post-graduation degrees. About 37.8% of the respondents are engineering graduates. The profile of the employees indicates that the banking industry today has young, well-qualified employees with good technological knowledge. Besides, the bank-related profile demonstrates that the majority of respondents are from public sector banks (54.2%), belong to urban branches (46.5%), and work either as clerks or officers (83.6%) in the bank. In terms of experience, the majority of the respondents have less than five years of experience (48.6%), reflecting the view of the young workforce in the banking sector.

4 Data analysis and results

The research model, which includes a series of separate but dependent relationships, requires techniques that estimate multiple relationships simultaneously. Hence, AMOS is used to perform confirmatory factor analysis that explains the relationship between the indicators and unobserved variables and models the structural relation among latent variables like information security awareness, reward, ISB, ISP characteristics, attitudes and social norms.

4.1 Assessing measurement model for reliability and validity

The measurement model, which defines constructs through observed variables, is examined for internal consistency and convergent and discriminant validity parameters. Considering an adequate item loading of 0.5, as suggested by Hair et al. (2010), any item with a value of less than 0.5 is removed from the scale. The analysis includes the composite reliability for each model's constructs. It reflects the internal consistency of the assessed data, which is well above the threshold limit of 0.7 (Hair et al., 2010). Convergent validity, which demonstrates the extent to which two measures capture a familiar construct, is assessed through the average variance extracted criterion. Though researchers suggest an AVE value of more than 0.5 (Chin et al., 1997; Chin, 1998) is acceptable as it indicates that the constructs can explain more than half of their indicators' variance. The AVE values of the current study shown in Table 4 are adequate to ensure convergent validity. The following parameter, discriminant validity, explains the uniqueness of each construct in capturing the particular phenomena (Fornell and Larcker, 1981). The other constructs do not demonstrate that the extent to which each construct differs from the remaining constructs is assured when the AVE value is more significant than 0.5. Their square root value is more extensive than other cross-correlations. The analysis of the study shows that the AVE values range from 0.53 to 0.76. Their square root values are more significant than cross-correlation, ensuring the required discriminant validity for the model (Fornell and Larcker, 1981). Thus, the findings indicate that the measures are adequate to proceed with further analysis.

Table 4 Discriminant validity

Constructs	*SN*	*ATT*	*REW*	*ISPC*	*AWA*	*ISB*	*AVE*
SN	0.865						0.748
ATT	0.254	0.788					0.621
REW	–0.074	–0.101	0.839				0.704
ISPC	0.135	0.266	–0.064	0.840			0.705
AWA	0.323	0.377	–0.122	0.153	0.832		0.693
ISB	0.361	0.463	–0.014	0.149	0.199	0.802	0.643

4.2 Common method bias

The common method bias, which artificially inflates the relation among the variable, is the result of the survey research, which measures the variables of interest (predictors and criterion variable) using the same method (Podsakoff and Organ, 1986). Harman's one-factor test has been used in this study to understand the presence of standard method variance. Harman's one-factor test, which predicts whether a single factor explains the majority of variance, is conducted using SPSS 20.0. The test result indicates that only 23.74% of the variance is described by a single element, thus implying that the current study does not suffer from common method variance bias (Kock, 2015).

4.3 Assessing structural model validity

Structural equation modelling, which explains the relations among unobserved variables, was used to examine the direct or indirect relationship among latent variables. The maximum likelihood method was employed to estimate the model parameters and check the data fit the conceptual model. The model fitness is assessed through different parameters like chi-square and associated degree of freedom, absolute fit measures, IFI and parsimony fit index. The chi-square and its associated degree of freedom expressed in terms of chi-square/degree of freedom indicate how good the data fit the hypothesised model. Any chi-square/degree of freedom value of less than 3.0 indicates a better model fit (Hair et al., 2010). The absolute fit index assesses how well sample data matches the researcher's theory. To examine absolute fit measures in the current study, the GFI assesses how well the model fits the population covariance matrix if unknown but the optimally chosen parameter is available. RMSEA, which quantifies how well the model fits the population covariance matrix if obscure but the optimally chosen parameter is known, is used (Byrne, 2010). Any values greater than 0.9 for GFI (Hu and Bentler, 1995) and values less than 0.08 (Browne and Cudeck, 1992) are considered better for the study model. Incremental fit indices analyse the difference between the estimated model and the alternative baseline model to know the soundness of the estimated model concerning the null model – normative, comparative, and incremental fit indices as measures for incremental fit indices in the current study. CFI, NFI, and IFI values more significant than the threshold limit of 0.90 (Bentler, 1992; Byrne, 1994a) represent a good model fit. The parsimony fit indices classify the best model from competing models based on the relative level of complexity.

Table 5 represents model fit indices along with the acceptable and derived values.

Table 5 Model fit indices

Measures	*Fit indices*	*Model value*	*Acceptable range*
Chi-square related measure	$\chi 2$	568.823	-
	$\chi 2$/Df	1.571	< 3.0
Absolute fit index	GFI	0.909	> 0.9
	RMSEA	0.038	< 0.08
Incremental fit index	CFI	0.974	> 0.9
	NFI	0.932	> 0.9
	IF	0.974	> 0.9
Parsimony measures	PRATIO	0.892	> 0.9

The result of the hypothesis depicting cause and effect relations is explained in Table 6. The study's finding shows that all the other hypotheses are mainly substantiated except for the hypothesis relating to reward for ISB. Significant relationships were found between subjective norm (= 0.29, p = 0.000), attitude (= 0.46, p = 0.000), and ISB, as well as between ISP characteristics (= 0.18, p = 0.001) and information security awareness (= 0.33, p = 0.000).

Table 6 Results of cause-and-effect relations

Path	*Hypothesis*	*Estimates*	*SE*	*CR*	*p-value*	*Supported/not supported*
SN -------> ISB	Subject norms positively influence employees' information security behaviour	0.278	.033	6.486	0.000	Supported
ATT ----> ISB	Employees attitude towards information security positively influence their information security behaviour	0.440	.059	10.28	0.000	Supported
REW -----> ISB	Rewards positively and significantly influence employees' behaviour on information security policies compliance	0.055	.034	1.29	0.194	Not supported
ISPC ----> ATT	Organisational information security policy characteristics have a significant and positive influence on employees' attitudes towards information security	0.227	.032	4.97	0.000	Supported
AWA ---> ATT	Information security awareness of the employees positively influence their attitudes towards information security	0.371	.027	8.13	0.000	Supported

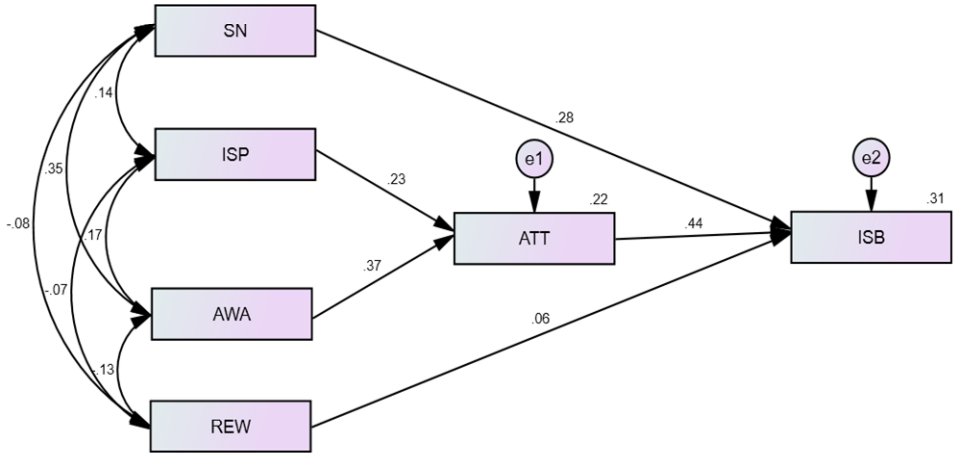
Attitude plays a significant role in influencing one's behaviour. The study's findings also indicated that employees' attitudes towards ISP compliance positively impact their ISB. This finding is in line with previous studies (Ifinedo, 2014; Lebek et al., 2014; Safa et al., 2015). As hypothesised, the subjective norms positively influenced employees' ISB, which is on par with the previous studies' findings (Anderson and Agarwal, 2010; Hazari et al., 2008; Herath and Rao, 2009; Guo et al., 2011).

Surprisingly, the rewards, considered to be the motivating factor in influencing employees' behaviour, have not influenced employees' behaviour in the current model. It may be due to either the employees' not being aware of such a rewards system in the bank or the fact that there is no such reward system in the bank (Siponen et al., 2014). Attitude relates to individual beliefs and feelings about objects and ideas and is influenced by factors like experience, prejudice, and instructions received through different mediums that create awareness.

Awareness, as a factor which can influence attitude, finds support in the current model with information security awareness of employees positively impacting employees' attitude towards organisation information security and is also in line with findings of previous studies (Bulgurcu et al., 2009; Dinev and Hu, 2007; Haeussinger and Kranz, 2013). Further, an up-to-date, clear, and quickly accessible organisation ISP of the bank can significantly influence employees' attitudes towards organisation information security. The current study findings concur with the previous studies.

ISB of the employees relates to compliance with the organisation's ISP that helps the organisation protect its information assets. Employees' good ISB protects themselves and their organisation from cyber-attacks like stealing confidential organisational data and siphoning individual money. Thus, the current study tried to understand the factors influencing bank employees' ISB and found that factors like subjective norms and attitude significantly affect one's ISB. In contrast, reward did not have any considerable impact. Further awareness and ISP characteristics significantly shaped employees' attitudes to ISB.

Figure 2 Path model (see online version for colours)



5 Discussion and managerial implications

Though many research studies were undertaken on employees' ISB, the current study considered the influence of organisational ISP characteristics in shaping employees' attitudes, which is the first of its kind to the best of the researchers' knowledge. With emerging technologies and extensive use of them across various aspects of banking activities and management, the probability of information security incidents is high in the future in the banking systems, warranting a practical approach to protecting organisations' information assets and customers. Thus, in the current study, the researchers have explained the impact of the fundamental factors related to secure banking like awareness, attitude, and reward system for employee ISB. The ISP's awareness, development, and implementation can help the banking system prove security by managing employees' ISB.

The impact the awareness had on attitude, which in turn affected employees' ISB. The bank management must regularly provide security awareness training programs to employees at all levels to update their knowledge and understanding. It will improve the employees' awareness level, which can positively shape their attitude towards organisation information security, leading to better ISB. Further, considering the impact of bank's ISP characteristics has on employees' attitudes, the bank management should keep their ISP as simple as possible, besides its easy accessibility to the employees. Finally, bank management should consider implementing rewards systems for good ISB of the employees periodically by designing a mechanism to capture the same and encourage them to follow without compromising. In case of no such system exists at present, the bank management must develop an ISP and standard operating procedure (SOP) protocol for the bank and revamp the existing system with a suitable reward system for the benefit of the bank customers.

Banks can make several technological solutions to bring down security breaches and incidents. Still, the success of any such efforts depends on the behaviour of the users, employees, and customers, who are considered the weakest link in organisation cyberspace. The present study explained the influence of organisational factors like social norms, reward systems, organisational ISP characteristics, and individual factors like awareness and attitude on employees' ISB. ISB of the employees is the foremost and significant determinant for security incidents in the bank. The study considers mainly the awareness and attitude of the employees play a dominant role in an information security system. It also recommends enhancing the employees' awareness and creating a positive attitude to avert security-related breaches, besides developing better social norms and reward systems for good security behaviour.

6 Conclusions

Banks are organisations that prioritise information security (Albrechtsen and Hovden, 2010), which provides context to our research. Poor ISB is a major determinant of the level of security incidents the banks confront. Although banks make several efforts in terms of technological solutions to combat cyber crimes, employees' behaviour plays a critical role. Hence, this study focussed on the human behaviour of Indian bank employees concerning information security, built on the theory of planned behaviour and

cognitive evaluation theory. The study's findings demonstrate that banks may reap the greatest benefits in terms of information security.

Among various factors investigated in our study, ISP characteristics were found to have an impending impact on the attitude of employees' ISB, along with individual awareness. While attitude and subjective norms of employees significantly affected the ISB, surprisingly rewards did not. These contributing elements might be prioritised by the organisation as these are found to positively influence employees' ISB.

7 Limitations

Though efforts have been made to make this study more reliable, comprehensive and valid, certain limitations cannot be overruled. The following are limitations of the current study. Firstly, the study has considered only the employees of the public and private sector banks situated in the region of Tamil Nadu, Andhra Pradesh, Karnataka, Kerala and Puducherry banks which requires future researchers to include subjects from the whole of India as well as the employees of foreign sector bank and regional rural bank to make the findings of the study more generalisable in nature. Secondly, the study is of a self-reporting nature where the variables of interest in the study are measured through respondents' responses to the predefined set of questions rather than being directly observed. Hence, there is a chance of bias in the responses, which might impact on findings of the study. Though such a possibility is meagre, their presence cannot be overruled.

8 Future research

Considering the present limitation, the future researcher can extend the scope by covering respondents of regional rural banks and foreign sectors in India. Further, future studies can consider the impact of interventional factors like organisational culture, structure and environment to understand its influence on employee ISB, as the current study has considered only a few of the individual and organisational factors in explaining the employee's ISB. As the current study has limited its scope to the banking sector of financial industries, future studies can cover the whole of financial industries like non-banking financial companies, payment banks, investment banks, etc. A researcher can also study the influence of cross-cultural differences on ISB through multi-ethnic groups.

References

Abawajy, J. (2014) 'User preference of cyber security awareness delivery methods', *Behaviour & Information Technology*, Vol. 33, No. 3, pp.237–248.

Ahmed, K.A. and Damodharan, V.S. (2021) 'Antecedents of travel intention in rental taxi services post coronavirus-19 lockdown', *International Journal of Management and Enterprise Development*, Vol. 20, No. 4, pp.363–379.

Albrechtsen, E., and Hovden, J. (2010) 'Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study', *Computers & Security*, Vol. 29, No. 4, pp.432–445.

Ali, R.F., Dominic, P.D.D., Ali, S.E.A., Rehman, M. and Sohail, A. (2021) 'Information security behavior and information security policy compliance: a systematic literature review for identifying the transformation process from noncompliance to compliance', *Applied Sciences*, Vol. 11, No. 8, p.3383.

Al-Omari, A., El-Gayar, O. and Deokar, A. (2012) 'Information security policy compliance: the role of information security awareness', *AMCIS 2012 Proceedings*, p.16 [online] https://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/16.

Alshaikh, M. (2020) 'Developing cybersecurity culture to influence employee behavior: a practice perspective', *Computers & Security*, Vol. 98, p.102003, DOI: 10.1016/j.cose.2020.102003.

Anderson, C.L. and Agarwal, R. (2010) 'Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions', *MIS Quarterly*, Vol. 34, No. 3, pp.613–643.

Bajaj, P., Almugari, F., Tabash, M.I., Alsyani, M. and Saleem, I. (2021) 'Factors influencing consumer's adoption of internet of things: an empirical study from Indian context', *International Journal of Business Innovation and Research*, Vol. 24, No. 3, pp.315–338.

Bentler, P.M. (1992) 'On the fit of models to covariances and methodology to the bulletin', *Psychological Bulletin*, Vol. 112, No. 3, pp.400–404.

Browne, M.W. and Cudeck, R. (1992) 'Alternative ways of assessing model fit', *Sociological Methods & Research*, Vol. 21, No. 2, pp.230–258.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2009) 'Roles of information security awareness and perceived fairness in information security policy compliance', *AMCIS 2009 Proceedings*, p.419 [online] https://aisel.aisnet.org/amcis2009/419.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) 'Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness', *MIS Quarterly*, Vol. 34, No. 3, pp.523–548.

Byrne, B.M. (1994a) 'Burnout: testing for the validity, replication, and invariance of causal structure across elementary, intermediate, and secondary teachers', *American Educational Research Journal*, Vol. 31, No. 3, pp.645–673.

Byrne, B.M. (1994b) *Structural Equation Modeling with EQS and EQS/Windows: Basic Concepts, Applications, and Programming*, Sage, California, USA.

Byrne, B.M. (2010) *Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming (Multivariate Applications Series)*, Vol. 396, No. 1, p.7384, Taylor & Francis Group, New York.

Cameron, J., Pierce, W.D., Banko, K.M. and Gear, A. (2005) 'Achievement-based rewards and intrinsic motivation: a test of cognitive mediators', *Journal of Educational Psychology*, Vol. 97, No. 4, pp.641–655.

Cavusoglu, H., Raghunathan, S. and Cavusoglu, H. (2009) 'Configuration of and interaction between information security technologies: the case of firewalls and intrusion detection systems', *Information Systems Research*, Vol. 20, No. 2, pp.198–217.

Cheng, L., Li, Y., Li, W., Holm, E. and Zhai, Q. (2013) 'Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory', *Computers & Security*, Vol. 39, pp.447–459, DOI: 10.1016/j.cose.2013.09.009.

Chin, W.W. (1998) 'Commentary: issues and opinion on structural equation modelling', *MIS Quarterly*, Vol. 22, No. 1, pp.7–16.

Chin, W.W., Gopal, A. and Salisbury, W.D. (1997) 'Advancing the theory of adaptive structuration: the development of a scale to measure faithfulness of appropriation', *Information Systems Research*, Vol. 8, No. 4, pp.342–367.

Cox, J. (2012) 'Information systems user security: a structured model of the knowing-doing gap', *Computers in Human Behavior*, Vol. 28, No. 5, pp.1849–1858.

Damodharan, V.S. and Ahmed, K.A. (2022) 'Exploring the Emirati female student entrepreneurs in the UAE through the theory of planned behaviour', *Transnational Marketing Journal*, Vol. 10, No. 1, pp.139–153.

Dinev, T. and Hu, Q. (2007) 'The centrality of awareness in the formation of user behavioral intention toward protective information technologies', *Journal of the Association for Information Systems*, Vol. 8, No. 7, p.23.

Fornell, C. and Larcker, D.F. (1981) 'Evaluating structural equation models with unobservable variables and measurement error', *Journal of Marketing Research*, Vol. 18, No. 1, pp.39–50.

Friedkin, N.E. (1998) *A Structural Theory of Social Influence*, Cambridge University Press, London.

Godbole, T., Gochhait, S. and Ghosh, D. (2022) 'Developing a framework to measure cyber resilience behaviour of Indian bank employees', in *ICT with Intelligent Applications*, pp.299–309, Springer, Singapore.

Grimes, M. and Marquardson, J. (2019) 'Quality matters: evoking subjective norms and coping appraisals by system design to increase security intentions', *Decision Support Systems*, Vol. 119, pp.23–34, DOI: 10.1016/j.dss.2019.02.010.

Guo, K.H., Yuan, Y., Archer, N.P. and Connelly, C.E. (2011) 'Understanding nonmalicious security violations in the workplace: a composite behavior model', *Journal of Management Information Systems*, Vol. 28, No. 2, pp.203–236.

Hadlington, L., Binder, J. and Stanulewicz, N. (2020) 'Fear of missing out predicts employee information security awareness above personality traits, age, and gender', *Cyberpsychology, Behavior, and Social Networking*, Vol. 23, No. 7, pp.459–464.

Haeussinger, F. and Kranz, J. (2013) 'Information security awareness: its antecedents and mediating effects on security compliant behavior', *International Conference on Information Systems 2013*, Milano, Italy [online] https://aisel.aisnet.org/icis2013/proceedings/SecurityOfIS/.

Hair, J.F., Black, W.C. and Babin, B.J (2010) *Multivariate Data Analysis: A Global Perspective*, Pearson Education, London, UK.

Hazari, S., Hargrave, W. and Clenney, B. (2008) 'An empirical investigation of factors influencing information security behavior', *Journal of Information Privacy and Security*, Vol. 4, No. 4, pp.3–20.

Herath, T. and Rao, H.R. (2009) 'Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness', *Decision Support Systems*, Vol. 47, No. 2, pp.154–165.

Hu, L-T. and Bentler, P.M. (1995) 'Evaluating model fit', in Hoyle, R.H. (Ed.): *Structural Equation Modeling: Concepts, Issues, and Applications*, pp.76–99, Sage Publications, Inc., Thousand Oaks.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012) 'Managing employee compliance with information security policies: the critical role of top management and organizational culture', *Decision Sciences*, Vol. 43, No. 4, pp.615–660.

Hu, Q., Xu, Z., Dinev, T. and Ling, H. (2011) 'Does deterrence work in reducing information security policy abuse by employees?', *Communications of the ACM*, Vol. 54, No. 6, pp.54–60.

Ifinedo, P. (2012) 'Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory', *Computers & Security*, Vol. 31, No. 1, pp.83–95.

Ifinedo, P. (2014) 'Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition', *Information & Management*, Vol. 51, No. 1, pp.69–79.

Kee, D.M.H. and Rubel, M.R.B. (2021) 'Technology adaptation is on its way: the role of high involvement work practice', *International Journal of Business Innovation and Research*, Vol. 25, No. 1, pp.35–50.

Khando, K., Gao, S., Islam, S.M. and Salman, A. (2021) 'Enhancing employees information security awareness in private and public organisations: a systematic literature review', *Computers & Security*, Vol. 106, p.102267, DOI: 10.1016/j.cose.2021.102267.

Kock, N. (2015) 'Common method bias in PLS-SEM: a full collinearity assessment approach', *International Journal of e-Collaboration (IJEC)*, Vol. 11, No. 4, pp.1–10.

Krueger Jr., N.F., Reilly, M.D. and Carsrud, A.L. (2000) 'Competing models of entrepreneurial intentions', *Journal of Business Venturing*, Vol. 15, Nos. 5–6, pp.411–432.

Kruger, H.A. and Kearney, W.D. (2006) 'A prototype for assessing information security awareness', *Computers & Security*, Vol. 25, No. 4, pp.289–296.

Kumar, A. and Dash, M.K. (2015) 'Effectiveness of electronic service dimensions on consumers' electronic buying behaviour and exploration of different groups', *International Journal of Business Innovation and Research*, Vol. 9, No. 1, pp.81–99.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. and Breitner, M.H. (2014) 'Information security awareness and behavior: a theory-based literature review', *Management Research Review*, Vol. 37, No. 12, pp.1049–1092, DOI [online] https://doi.org/10.1108/MRR-04-2013-0085.

Lee, Y. and Kozar, K.A. (2005) 'Investigating factors affecting the adoption of anti-spyware systems', *Communications of the ACM*, Vol. 48, No. 8, pp.72–77.

Lin, C., Wittmer, J.L. and Luo, X.R. (2022) 'Cultivating proactive information security behavior and individual creativity: the role of human relations culture and IT use governance', *Information & Management*, Vol. 59, No. 6, p.103650.

Liu, C., Liang, H., Wang, N. and Xue, Y. (2021) 'Ensuring employees' information security policy compliance by carrot and stick: the moderating roles of organizational commitment and gender', *Information Technology & People*, Vol. 35, No. 2, pp.802–834, DOI: 10.1108/ITP-09-2019-0452.

Ma, X. (2022) 'IS professionals' information security behaviors in Chinese IT organizations for information security protection', *Information Processing & Management*, Vol. 59, No. 1, p.102744.

Merhi, M.I. and Ahluwalia, P. (2019) 'Examining the impact of deterrence factors and norms on resistance to information systems security', *Computers in Human Behavior*, Vol. 92, pp.37–46, DOI: 10.1016/j.chb.2018.10.031.

Nasirpouri Shadbad, F. and Biros, D. (2021) 'Understanding employee information security policy compliance from role theory perspective', *Journal of Computer Information Systems*, Vol. 61, No. 6, pp.571–580.

Pahnila, S., Siponen, M. and Mahmood, A. (2007) 'Employees' behavior towards IS security policy compliance', in *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, IEEE, January, p.156b.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014) 'Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)', *Computers & Security*, Vol. 42, pp.165–176, DOI: 10.1016/j.cose.2013.12.003.

Podsakoff, P.M. and Organ, D.W. (1986) 'Self-reports in organizational research: problems and prospects', *Journal of Management*, Vol. 12, No. 4, pp.531–544.

Potoglou, D. and Kanaroglou, P.S. (2007) 'Household demand and willingness to pay for clean vehicles', *Transportation Research Part D: Transport and Environment*, Vol. 12, No. 4, pp.264–274.

Press Trust of India (2021) *Over 290,000 Cyber Security Incidents Related to Banking Reported in 2020* [online] https://www.business-standard.com/article/finance/over-290-000-cyber-security-incidents-related-to-banking-reported-in-2020-121020401220_1.html (accessed 13 June 2021).

Ratna, P.A. and Mehra, S. (2015) 'Opinion leaders for increasing the market for non-life insurance products in India', *International Journal of Business Innovation and Research*, Vol. 9, No. 2, pp.210–228.

Safa, N.S. and Ismail, M.A. (2013) 'A customer loyalty formation model in electronic commerce', *Economic Modelling*, Vol. 35, pp.559–564, IEEE, DOI: 10.1016/j.econmod.2013.08.011.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. and Herawan, T. (2015) 'Information security conscious care behaviour formation in organizations', *Computers & Security*, Vol. 53, pp.65–78, DOI: 10.1016/j.cose.2015.05.012.

Sasse, M.A., Brostoff, S. and Weirich, D. (2001) 'Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security', *BT Technology Journal*, Vol. 19, No. 3, pp.122–131.

Shahbaznezhad, H., Kolini, F. and Rashidirad, M. (2021) 'Employees' behavior in phishing attacks: what individual, organizational, and technological factors matter?', *Journal of Computer Information Systems*, Vol. 61, No. 6, pp.539–550.

Shropshire, J., Warkentin, M. and Sharma, S. (2015) 'Personality, attitudes, and intentions: predicting initial adoption of information security behavior', *Computers & Security*, Vol. 49, pp.177–191, DOI: 10.1016/j.cose.2015.01.002.

Siponen, M., Mahmood, M.A. and Pahnila, S. (2014) 'Employees' adherence to information security policies: an exploratory field study', *Information & Management*, Vol. 51, No. 2, pp.217–224.

Siponen, M., Pahnila, S. and Mahmood, M.A. (2010) 'Compliance with information security policies: an empirical investigation', *Computer*, Vol. 43, No. 2, pp.64–71.

Son, J.Y. (2011) 'Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies', *Information & Management*, Vol. 48, No. 7, pp.296–302.

Sudarshan, V. (2018) *India Bank Hack 'Similar' to $81 Million Bangladesh Central Bank Heist*, *Thomson Reuters Publication*, 19 February [online] https://www.reuters.com/article/us-city-union-bank-swift-idUSKCN1G319K (Accessed on April 2nd 2021)

Tam, C., de Matos Conceição, C. and Oliveira, T. (2022) 'What influences employees to follow security policies?', *Safety Science*, Vol. 147, p.105595, DOI: 10.1016/j.ssci.2021.105595.

Urban, B. and Verachia, A. (2019) 'Organisational antecedents of innovative firms: a focus on entrepreneurial orientation in South Africa', *International Journal of Business Innovation and Research*, Vol. 18, No. 1, pp.128–144.

Vance, A., Siponen, M. and Pahnila, S. (2012) 'Motivating IS security compliance: insights from habit and protection motivation theory', *Information & Management*, Vol. 49, Nos. 3–4, pp.190–198.

Vroom, C. and Von Solms, R. (2004) 'Towards information security behavioural compliance', *Computers & Security*, Vol. 23, No. 3, pp.191–198.

Wu, S.M., Guo, D. and Wu, Y.C. (2017) 'The effects of bank employees' information security awareness on performance of information security governance', in *International Conference on Intelligent and Interactive Systems and Applications*, Springer, Cham, June, pp.657–663.

Zhang, J., Reithel, B.J. and Li, H. (2009) 'Impact of perceived technical protection on security behaviors', *Information Management & Computer Security*, Vol. 17, No. 4, pp.330–340.