Information security collaboration formation in organisations

Nader Sohrabi Safa1,2, Carsten Maple1, Tim Watson1, Steve Furnell2,3
1Cyber Security Centre at WMG, University of Warwick, Coventry, UK
2Centre for Research in Information and Cyber Security, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
3Centre for Security, Communications and Network Research, University of Plymouth, Plymouth, UK
E-mail: n.sohrabi-safa@warwick.ac.uk

Abstract: The protection of organisational information assets requires the collaboration of all employees; information security collaboration (ISC) aggregates the efforts of employees in order to mitigate the effect of information security breaches and incidents. However, it is acknowledged that ISC formation and its development needs more investigation. This research endeavours to show how ISC forms and develops in the context of an organisation based on social bond factors. The social bond theory and theory of planned behaviour describe the effect of social bond factors on the attitude of employees and finally their behaviour regarding collaboration in the domain of information security. The results of the data analysis reveal that personal norms, involvement, and commitment to their organisation significantly influence the employees’ attitude towards ISC intention. However, contrary to the authors expectation, attachment does not influence the attitude of employees towards ISC. In addition, attitudes towards ISC, perceived behavioural control, and personal norms significantly affect the intention of employees towards ISC. The findings also show that the employees’ intention towards ISC and organisational support positively influence ISC, but that trust does not significantly affect ISC behaviour.

1 Introduction

The proliferation of computer and communication systems has changed the business environment. In the modern environment, information security is the most important and controversial subject among experts [1]. Applying different strategies, such as acting based on information security organisational procedures and policies [2], information security conscious care behaviour [3], sharing information security knowledge [4, 5], and information security collaboration (ISC) in organisations [6], have been acknowledged to be useful in decreasing the vulnerability of information security incidents in companies. A novel conceptual model is presented in this study that depicts how collaboration develops and reduces the risk of information security incidents in organisations.

Collaboration means working together to achieve a goal. In this instance, the goal is providing a secure environment for information assets in organisations [7]. Shared goals, benefits, personal interest, and organisational support are examples of factors that motivate individuals to collaborate. The main subject in learning, project management, organisation, health, business, and so forth is collaboration. Reducing the cost, increasing the chance of achieving the relevant goals, and the sharing of ideas and expertise in order to benefit the organisation, and participating in accurate decision-making are useful outputs of collaboration. Knowledge sharing, learning, and the improvement of productivity and performance are other advantages of inter-organisational collaboration. Collaboration also increases the opportunity for problem solving [8].

Trust between members, relationships, coordination, culture, and the role of administration are important factors in collaboration. Coordination, co-operation, and collaboration are vital activities in the information security domain. The level of commitment and importance of relationships influences collaboration. The responsibility to collaborate refers to the duty of everyone to share his or her knowledge and experience, in order to provide a secure environment for information. Collecting, completing, transferring, and explaining information that relates to information security are examples of collaboration in this domain.

Collaboration is a value that originates from an individuals' activities or the effort of all participants. Proper collaboration brings greater efficiency and has fewer costs [9]. ISC improves social aspects of information security, decreases the cost of attacks, and increases the knowledge and experience of employees in organisations.

ISC refers to all shapes (forms) of effort that purport to mitigate the risk of information security breaches and incidents; these efforts can be manifested in the forms of responding and recovering information security attacks, codification of policies and guidelines, as well as compliance with them, reporting information security incidents, and information security knowledge sharing (ISKS) in order to increase awareness of employees as a basic factor, are all examples of collaboration in the information security realm [10]. In ISC, the security of information assets is the shared goal and organisational information security rules and regulations are shared rules. Although ISC has been acknowledged as an important approach that decreases information security breaches, there needs to be more investigation into the effective factors in this domain, as well as into the development of ISC in organisations.

The structure of this paper is as follows: social bond theory (SBT), theory of planned behaviour (TPB), and the Triandis model constitute the background of the research model. The background theories together with the effective factors are described in Section 2. The applied methodology details the steps of the investigation, which is illustrated in Section 3. The analysis of data, and the results of statistical tests on the measurement model (MM) and structural model (SM) are scrutinised in Section 4. The effect of this research and its implementation are expounded upon in Section 5, and, finally, the conclusion and future work are discussed in Section 6.

2 Theoretical background and conceptual framework

The conceptual research model encompasses three basic theories. The SBT deals with factors that function to influence employees' attitude in an organisation in ways that are significant from the
point of view of ISC. The TPB shows how the formation of ISC in employees’ behaviour is to be understood. Finally, the Triandis model explains how organisational support and trust between employees expedite ISC in organisations. Fig. 1 shows this process in a concise form.

2.1 Social bond theory

The SBT provides an interesting way to explain some social activities in organisations. The SBT, which was created by Hirschi [11], says that social bonds represent the attachment to an organisation, commitment to a community, involvement, and having an opinion that the kind of behaviour in question (ISC) is important. The SBT focuses on individuals in a group or community. Attachment refers to the feeling that binds one to a person, ideal, thing, or the like. In this research, attachment is a kind of relationship between the employees and the organisational values, in which such values function to provide the safeguard of information assets. Commitment relates to an employees’ effort and the energy expended to secure the information, while involvement refers to the consideration given to the importance of information protection, and the information security policies and procedures in daily activities. Personal norms relate to an employees’ beliefs and views about information security. Securing information assets is a valuable task in organisations.

2.1.1 Attachment: Attachment refers to a deep and durable emotional bond that creates a relationship between a person and another person, organisation, or activities over time and space [12]. The deep relationship between an infant and his/her parents is a tangible example of attachment. Attachment is not necessarily a reciprocal relation. The acceptance of social norms and the improvement of social awareness depends on the attachment of individuals to significant others, such as family members and friends [13]. Attachment can be a motivationally efficacious factor in engaging in a particular behaviour because of its evolutionary pressure on individuals [14]. This pressure can motivate employees to help each other in order to protect information assets. Therefore, we hypothesise:

\[ H1: \text{Attachment positively influences the attitude towards ISC intention.} \]

2.1.2 Involvement: Involvement refers to the energy, time, and participation that individuals spend on a subject. Customer/consumer involvement, employee involvement, student involvement, and information security involvement are instances of involvement in different domains. Sharing knowledge about information protection, attending information security courses and workshops, following information security news in the media, reporting information security incidents to the experts, and complying with organisational information security policies and procedures (OISPs) are all examples of information security involvement in daily activities that affect our attitudes. Rocha Flores et al. [15] asserted that information security involvement positively influences the employees’ awareness and knowledge of information security. Information security involvement refers to the time and effort spent on different activities – ISKS, collaboration, incident reports, and complying with OISPs – that employees spend on protecting the information assets in the organisation. Based on the aforementioned explanations, the following hypothesis is presented:

\[ H2: \text{Involvement positively influences the attitude towards ISC intention.} \]

2.1.3 Commitment: Organisational commitment refers to an individuals’ psychological attachment to the organisation and affects job performance, satisfaction, productivity, or, in other words, organisational success. Organisational commitment also relates to how employees feel about their jobs. Individuals with commitment follow organisational aims and plans and try to remain a part of the organisation. Age, sex, education, and tenure do not have a strong or consistent effect on their commitment [16]. The employees’ experience before joining the organisation influences the employees’ sense of obligation. An employers’ commitment to an employees’ well-being and rewards positively influences normative commitment. Ifinedo [17] asserted that an individuals’ commitment significantly affects their attitude towards compliance with OISPs. In this research, we postulate that the commitment of employees affects their attitude towards ISC commitment:

\[ H3: \text{Commitment positively influences the attitude towards ISC intention.} \]

2.1.4 Personal norms: Personal norms and social norms relate to an individuals’ normative beliefs in which both lead to the sense of obligation to act. However, social norms are enforced through social rewards and sanctions; personal norms stem from an internal sense that comes from moral judgement [18]. Personal values are an important factor in the formation of personal norms. Indeed, internal processes of self-expectation influence personal norms, while external constraints affect social norms. Consequently, an individuals’ evaluation of their personal norms relies on a conceptualisation of the values that affect their behaviour. The relationship between behaviour and personal norms was discussed in the context of the theory of reasoned action [19] and subsequently extended to the TPB [20]. Li et al. [21] showed that personal norms influence the compliance with Internet use policies in organisations. ISC is considered to be a valuable characteristic due to its potential effect on information security threats in firms. Based on the aforementioned explanations, the following hypothesis is presented:
have applied the TPB to explain the behaviour of individuals in organisational narcissism, perceived risk, and perceived severity of organisations. 

2.2 Theory of planned behaviour

The TPB, which was developed by Ajzen and Madden [20], considers the attitude, perceived behavioural control, and subjective norms upon an individuals' behaviour. Diverse studies have applied the TPB to explain the behaviour of individuals in different domains. The authors in [17, 22] utilised the TPB to show how the disposition to comply with OISPs is formed in the organisations. Safa et al. [3] also used the TPB to explain the formation of information security conscious care behaviour in organisations. In another study, Cox [23] used the TPB to investigate the disregard of information security policies by users, even though they know the policies. In this research, the TPB shows how commitment, involvement, attachment, and personal norms influence the attitude of an employee, and how perceived behavioural control, subjective norms, and attitude affect an individuals’ intention to collaborate in information security. Further explanation about these factors will be presented in subsequent sections.

2.2.1 Attitude towards ISC: Attitude is a favourable or unfavourable evaluation of different objects, such as a person, place, idea, event, or activity. It encompasses a wide spectrum of an individuals’ opinion from very bad to very good. Attitude is derived from an employees’ past and present experience. Attitude comes from a person's evaluation; when criteria change, the evaluation and attitude will change. In other words, the formation of attitude is a dynamic process. Attitude can be affected by the attachment, commitment, involvement, and personal norms of an individual [17]. In another study, Cox [23] showed that organisational narcissism, perceived risk, and perceived severity of vulnerability influence an individuals’ attitude towards observing security precautions. In this study we postulate:

H5: Attitude towards ISC positively influences ISC intention.

2.2.2 Perceived behavioural control: Perceived behavioural control (PBC) is attributed to the individual depending on whether they have an insight into their capability to conduct and control a particular behaviour [24]. In this line, beliefs can facilitate the performance of the behaviour. Perceived behavioural control also shows a persons’ opinion concerning the easiness or hardness of engaging in the behaviour in question. Employees with more behavioural control incline towards being more involved in their job [25]. Workman et al. [26] showed that perceived behavioural control significantly affects staff disposition to follow OISPs. This research endeavours to show that PBC has a significant effect on an employee's intention to collaborate in the domain of information security in order to safeguard organisational information assets:

H6: Perceived behavioural control positively influences ISC intention.

2.2.3 Subjective norms: The expectation of important persons and social normative beliefs have an important effect on the formation of subjective norms. Strong normative beliefs positively influence motivation to perform the relevant kind of behaviour [27]. Subjective norms are also assigned to perceived social pressure to conduct or not conduct a behaviour. The belief of a person, weighted by the importance that one attributes to each view, will influence one's behavioural intention to collaborate with him/her. Research by Shibchurn and Yan [28] revealed that subjective norms influence the disclosure of information on social networks through perceived usefulness and perceived risk. In another study, Tamjidymcholo et al. [29] asserted that social norms positively influence the ISKS in virtual communities. This research aims to show that subjective norms significantly influence ISC intention in organisations:

H7: Subjective norms positively influences ISC intention.

2.2.4 ISC intention: Intention shows a commitment to fulfil a plan as well as the forethought to achieve a goal. Intention refers to a mental state that originates from human beliefs and desire [30]. There are relationships among the desire, beliefs, intentions, and behaviours carried out by individuals in order to attain a goal; the goal in this instance is the safeguarding of information assets in the relevant organisation. Intention is one of the main factors in the TPB and has been discussed in many studies. Intention plays an important role in terms of complying with OISPs [31]. In another study, Shropshire et al. [32] used intention to show the adoption of information security behaviour in organisations. Park et al. [33] showed that intention changes the employees’ behaviour towards sharing their knowledge in firms. In this research, we postulated that the employees’ intention towards ISC significantly influence their ISC-related behaviour:

H8: ISC intention positively influences ISC behaviour.

2.3 Triandis model

Between attitude and the formation of behaviour, intention plays an important role [20]. Jeon et al. [34] asserted that behaviour may not materialise when there is an obstacle to engaging in the behaviour, despite the presence of a strong intention. Facilitating conditions play an important role, along with the other factors in the formation of a particular behaviour [35]. In this research, organisational support and trust are considered to be facilitating conditions that positively influence the formation of ISC in organisations.

2.3.1 Organisational support: The extent to which a company appreciates and values its staffs’ effort and considers their well-being manifests its support towards its employees [32]. A well-designed team with good people can perform poorly if an organisation does not provide appropriate support and the necessary resources. Reid et al. [36] asserted that organisational support influences the acceptance and use of information technology. A high level of organisational support causes a feeling of obligation among the staff, whereby employees will support the relevant organisational goals. In other words, organisational support leads to a reciprocal reaction and facilitates a particular behaviour in an organisation. Cheng et al. [37] showed that perceived organisational support is considered to be a commitment towards employees and that staff reciprocate through a commitment towards relevant organisational goal and policies. This commitment can safeguard information assets through ISC. Hence, the following hypothesis is presented:

H9: Organisational support positively influences ISC behaviour.

2.3.2 Trust: Trust is a belief about another person concerning their reliability, honesty, and effectiveness. The perception of, or desire towards, depending on a person or thing manifests an attitude of trust towards that person or thing [38]. Trust affects social systems and influences relationships among people. Trust influences the individual relationship in different social communities such as families, friends, and organisations. Trust also affects the disclosure of personal information in online interactions [39], and significantly influences the transfer of knowledge as a kind of collaboration among individuals in companies [8]. This study intends to examine the effect of trust as a factor that facilitates ISC in the domain of information security:

H10: Trust positively influences ISC behaviour.

Fig. 1 depicts the formation of ISC in organisations in a concise form. Hypotheses 1–4 correspond to the bonding variables that affect attitude. The next three hypotheses relate to the TPB that depicts the effect of subjective norms, attitude, and perceived behavioural control on ISC intention. Hypotheses 8–10 illustrate the effect of ISC intention, trust, and organisational support on the ISC behaviour.

3 Research methodology

This research targets reducing the effect of information security incidents by enriching ISC in organisations. ISC aggregates staff effort directed towards safeguarding information assets [23]. A
review of the literature, in addition to the context of SBT, revealed that commitment, attachment, involvement, and personal norms influence the attitude of employees regarding the intention to conduct security-conducive behaviour. In addition, the TPB helps us to describe how ISC forms in response to attitude, perceived behavioural control, subjective norms, and intention.

The mix mode methodology – qualitative and quantitative – was considered in this study. Initially, the influential factors were collected from previous studies in this domain, while interviews with experts using the Delphi method improved the quality of the research model. Confirmatory factor analysis was used in order to investigate whether our understanding of the nature of the factors is consistent with the MM. Structural equation modelling (SEM) is considered to be the most suitable method for this kind of research to test the plausible relationships among the dependent, independent, and mediating variables [40].

3.1 Data collection

The employees of different organisations in South Africa functioned as a focus group for collecting data. They were active in the domain of information technology, banking, manufacturing, and education. The constructs in the research model were measured using several items (questions). A five-point Likert scale was used to answer the questions. The purpose of the research was explained to the participants before they were requested to complete the questionnaire. The questionnaire was only presented to them once they consented to participate in this research. In order to be confident regarding the understandability and unique interpretation of the questions by respondents, the questions were pilot tested among 42 participants. Their emotions, descriptions, and any instances of hesitation were observed, and, subsequently, some words and sentences were revised to improve the understandability of the items.

3.2 Demography

The facilities in Google Drive (electronic questionnaire) and a paper-based questionnaire were used to decrease the time of data collection. Three hundred and eighty-five participants engaged in the data collection process, and of those 142 used the paper-based questionnaire and 243 used Google Drive. To reduce the number of incomplete questionnaires in the paper-based approach, we checked the responses immediately and kindly asked them to provide answers to any questions that had been left blank. Nonetheless, eight questionnaires (5.6%) were omitted due to incomplete answers or because the same answer was supplied to all questions. The electronic questionnaire was emailed to participants for whom we had email addresses using Google Drive. Of the 243 electronic questionnaires, 33 (13.5%) were omitted from the data set either because of incomplete answers or because the same responses were given to all questions. Finally, 344 completed records were transferred to the main data set. Table 1 shows the demography of the participants.

4 Results

The effective factors in the research model are usually unobservable. Commitment, involvement, attachment, and personal norms are examples of the unobservable variables that need to be measured using several items. The MM and SM are two components that are developed based on the observable and unobservable variables in the research model [40]. The MM shows the relationships among the factors (unobservable variables) and the items (observable variables). The reliability and validity of the indicators (items) are tested before the MM is fitted to the data. The relationships between the unobservable variables are examined in the SM. SEM encompasses MM and SM and has been mentioned as a suitable statistical approach for this kind of research.

4.1 Measurement model

To examine the data fit to the hypotheses and relationships between the items and factors in the model, SEM has been used. SEM has the ability to isolate errors when measuring unobservable variables with items (observable variables) and estimating regression among unobserved variables. The normal distribution of data was tested in the first step of data analysis. The results of standard skewness and kurtosis were between −2 and +2, which indicate the normal distribution of data. The research model was developed based on SBT, TPB, and previous studies. In this case, confirmatory factor analysis is acknowledged to be an appropriate approach to test whether the constructs or factors are consistent with the items that measure them [41].

The convergent validity was tested by factor loading; 0.5 is a threshold for convergent validity. Factor loading greater than this threshold shows convergent validity [40]. Therefore, the items with a factor loading of less than the threshold were dropped from the model.

The correlations between each pair of factors were tested in order to investigate the discriminant validity of the model. The results showed that the correlations between each pair of factors were less than the 0.9 threshold which indicates the discriminant validity of the model [42].

4.2 Testing the SM

SEM reveals the relationships among the variables and presents reliable measurements. SEM was applied to determine the relationships among the dependent, independent, mediating, and moderating variables in the model. IBM Amos version 20, using the maximum likelihood method, was applied to estimate the model based on different measures. The important statistical indices with their acceptable measures have been presented in Table 2.

Table 1 Demography of participants

| Measure | Items | Frequency | Per cent |
|---------|-------|-----------|----------|
| gender  | male  | 192       | 55.7     |
|         | female| 152       | 44.3     |
| age     | 21–30 | 111       | 32.2     |
|         | 31–40 | 143       | 41.46    |
|         | 41–50 | 67        | 19.63    |
|         | >50   | 23        | 6.71     |
| education | diploma | 23     | 6.8      |
|          | bachelor | 223    | 64.85    |
|          | master | 77       | 22.35    |
|          | PhD    | 21       | 6.0      |
| position | employee | 305    | 88.8     |
|          | chief employee | 30   | 8.7      |
|          | management | 9     | 2.5      |
| industry | telecoms/IT | 66    | 19.2     |
|          | banking | 98       | 28.5     |
|          | manufacturing | 81   | 23.5     |
|          | education | 99    | 28.8     |
| work experience | 1–2 years | 98  | 28.5     |
|          | 3–5 years | 170  | 49.4     |
|          | >5 years | 76       | 22.1     |

Table 2 Statistical indices

| Fit indices | Model value | Acceptable standard |
|-------------|-------------|---------------------|
| χ²/DF       | 988.89      | —                   |
| GFI         | 0.912       | >0.9                |
| AGFI        | 0.918       | >0.9                |
| CFI         | 0.902       | >0.9                |
| IFI         | 0.916       | >0.9                |
| NFI         | 0.928       | >0.9                |
| RMSEA       | 0.078       | <0.08               |
Table 3 Hypotheses tests

| Path  | Standardised estimate | SE   | r-value | Results |
|-------|------------------------|------|---------|---------|
| ATT → ATI | 0.521 | 0.079 | 0.509   | not-supported |
| INV → ATI | 0.721 | 0.102 | 0.014   | supported |
| COM → ATI | 0.685 | 0.067 | 0.010   | supported |
| PNO → ATI | 0.628 | 0.086 | 0.032   | supported |
| ATI → IIS | 0.802 | 0.074 | 0.012   | supported |
| PBC → IIS | 0.656 | 0.089 | 0.004   | supported |
| SNO → IIS | 0.714 | 0.091 | 0.022   | supported |
| IIS → ISC | 0.799 | 0.074 | 0.003   | supported |
| TRU → ISC | 0.517 | 0.134 | 0.301   | not-supported |
| OSU → ISC | 0.718 | 0.094 | 0.026   | supported |

Table 3 shows the results of the hypotheses testing.

5 Contribution and implementation

Experts have acknowledged that complying with organisational information security policies and procedures [2, 31], ISKS [43, 44], and information security conscious care behaviour [3] are effective and efficient approaches to mitigating the risk of information security breaches and incidents in organisations. ISC has also been identified as an effective and efficient approach that decreases the risk of information security incidents in organisations. However, there is a scarcity of studies that investigate collaboration in the domain of information security in organisations. As far as we know, this research is among the first investigations into whether ISC formation in organisations constitutes an effective and efficient approach to decreasing the risk of information security incidents.

The novelty of this research originates from its important subject (ISC) and its effect on decreasing the influence of information security breaches and incidents, as well as the adoption of two basic theories – SBT and TPB. These theories explain how social bond factors as well as attitude towards ISC perceived behavioural control, and subjective norms influence the employees’ intention to collaborate in information security tasks. Contrary to our expectations, the results of the data analysis revealed that attachment to the organisation does not significantly influence the employees’ attitude towards ISC in organisations. This outcome is in line with the study of Ifinedo [17]; the output of his study also showed that attachment does not influence the attitude of employees towards complying with OISPs. Casper and Harris [14] mentioned that self-interest and individual benefits are among the possible causes of such discord. The findings showed that involvement in information security, commitment to organisational plans and policies, and the personal belief that ISC is necessary to minimise the effect of attacks have a significant effect on the attitude of employees towards ISC intention. The outcome of the statistical tests also revealed that attitude towards ISC, perceived behavioural control, and personal belief influence the intention of employees towards ISC in organisations. Organisational support has a significant effect on ISC, but that trust does not have a significant effect on ISC formation in organisations. The outputs of this research provide clues to management in organisations which are suggestive as to how to go about mitigating the risk of information security incidents.

6 Conclusion

In this research, a novel model has been presented that shows the formation of ISC based on social factors and perceived behavioural control, subjective norms, attitude, and intention. In addition, the results of the data analysis showed that organisational support has a significant effect on the formation of ISC. ISC alone cannot safeguard information assets, but it plays a vital role in this domain when employees report information security breaches and incidents on time, when they contribute in capturing, submitting, interpreting, commenting, reviewing, and sharing their experience in the domain of information security, and when they comply with OISPs and procedures. In this case, the safeguarding of information assets is a shared goal. ISC is a valuable culture that brings many advantages if cultivated in a proper way.

Mace et al. [45] mentioned that collaboration helps experts to obtain, complete, disseminate, and share their knowledge with others; collaboration is an important part of development. They identified the main factors for successful collaborative ontology development: ‘These include synchronous/asynchronous communication; proposed content agreement policy; annotation of content and changes; content provenance; concurrency and version control; and personalised views of ontology content’. These are all clues for the management of organisations to improve ISC within the organisation.

We were faced with some limitations in this study. The samples in this research were gathered from various companies in the Eastern Cape of South Africa. This can be extended to more companies in other parts of this country or even in other countries to improve the generality of the findings. The other limitation stems from the lack of control on double responses by participants who filled out the electronic questionnaire. Such a concern can be addressed by controlling the respondents’ IP address; in this way, participants with two or more responses can be detected.

7 References

[1] Roumani, Y., Nwanpka, J.K., Roumani, Y.F.: ‘Examining the relationship between firm’s financial records and security vulnerabilities’, Int. J. Inf. Manage., 2016, 36, (6, Part A), pp. 987–994
[2] Siponen, M., Adam Mahmood, M., Pahlina, S.: ‘Employees’ adherence to information security policies: an exploratory field study’, Inf. Manag., 2014, 51, (2), pp. 217–224
[3] Safa, N.S., Sookhak, M., Von Solms, R., et al.: ‘Information security conscious care behaviour formation in organisations’, Comput. Secur., 2015, 53, pp. 65–78
[4] Hassan, N.I., Imazil, Z., Maarop, N.: ‘A conceptual model for knowledge sharing towards information security culture in healthcare organisation’. 2013 Int. Conf. on Research and Innovation in Information Systems (ICRIIS), 2013
[5] Feledzi, D., Fenu, S., Lechner, L.: ‘Toward web-based information security knowledge sharing’, Information Security Technical Report, 2013, 17, (4), pp. 199–209
[6] Tondel, I.A., Line, M.B., Jautun, M.G.: ‘Information security incident management: current practice as reported in the literature’, Comput. Secur., 2014, 45, pp. 42–57
[7] Imperial, M.T.: ‘Using collaboration as a governance strategy: lessons from six watershed management programs’, Adm. Soc., 2005, 37, (3), pp. 281–320
[8] Chen, Y.-H., Lin, T.-P., Yen, D.C.: ‘How to facilitate inter-organizational knowledge sharing: the impact of trust’, Inf. Manag., 2014, 51, pp. 568–578
[9] Austin, J.E., Setiandari, M.M.: ‘Collaborative value creation: a review of partnering between nonprofits and businesses: part I. Value creation spectrum and collaboration stages’, Nonprofit Volunt. Sect. Q., 2012, 41, (5), pp. 726–758
[10] Ahmad, A., Maynard, S.B., Shankx, G.: ‘A case analysis of information systems and security incident responses’, Int. J. Inf. Manage., 2015, 35, (6), pp. 717–723
[11] Hirschi, T.: ‘Causes of delinquency’ (University of California Press, London, England, 1969)
[12] Mesch, G.S.: ‘Social bonds and internet pornographic exposure among adolescents’, J. Adolescence, 2009, 32, (2), pp. 197–218
[13] Reed, L.A., Tolman, R.M., Safyer, P.: ‘Too close for comfort: attachment insecurity and electronic intrusion in college students’ dating relationships’, Comput. Hum. Behav., 2015, 50, pp. 431–438
[14] Casper, W.J., Harris, C.M.: ‘Work-life benefits and organizational attachment: self-interest utility and signaling theory models’, J. Vocat. Behav., 2008, 72, (1), pp. 95–109
[15] Rocha Flores, W., Antonesen, E., Ekstedt, M.: ‘Information security knowledge sharing in organizations: investigating the effect of behavioral
| Construct       | Items                                                                 | Mean   | SD    | Loading | Composite reliability |
|-----------------|------------------------------------------------------------------------|--------|-------|---------|-----------------------|
| attachment      | ATT1 I am glad to work with this company                               | 4.32   | 0.86  | 0.706   | 0.721                 |
|                 | ATT2 I like to spend the rest of my career with this company           | 3.86   | 0.78  | 0.686   |                       |
|                 | ATT3 I really think the organisation's problems are my concern         | 4.02   | 0.82  | 0.566   |                       |
|                 | ATT4 I like to exert my effort to safeguard the organisational information assets | 3.96   | 0.96  |         | dropped               |
| involvement     | INV1 I actively involve myself in information security activities       | 4.32   | 0.74  | 0.714   | 0.802                 |
|                 | INV2 I follow OISPs                                                    | 4.16   | 0.87  | 0.782   |                       |
|                 | INV3 I attend information security training courses                     | 3.98   | 1.02  | 0.689   |                       |
|                 | INV4 I think about the consequences of my behaviour in risky situations | 4.26   | 0.94  | 0.568   |                       |
| commitment      | COM1 I have commitment to safeguard organisational information assets  | 4.28   | 0.84  | 0.704   | 0.734                 |
|                 | COM2 I am willing to exert my effort to collaborate in the information security domain | 3.98   | 0.72  |         | 0.726                 |
|                 | COM3 I am willing to help others to safeguard the information security assets in this firm | 4.02   | 0.83  | 0.684   |                       |
| personal norms  | PNO1 ISC is a serious matter for me                                   | 4.28   | 0.98  | 0.696   | 0.769                 |
|                 | PNO2 I believe that my ISC affects the organisational success          | 3.86   | 1.05  | dropped |                       |
|                 | PNO3 The lack of ISC is not acceptable to me                           | 4.21   | 0.98  | 0.526   |                       |
|                 | PNO4 Information security knowledge sharing and incident reporting are important issues to me | 4.34   | 0.86  | 0.748   |                       |
| attitude        | AT11 ISC is valuable to me                                            | 4.65   | 0.87  | 0.696   | 0.831                 |
|                 | AT12 ISC is always beneficial                                         | 4.31   | 0.76  | 0.724   |                       |
|                 | AT13 ISC is an enjoyable experience for me                             | 3.98   | 0.88  | dropped |                       |
|                 | AT14 ISC is a good idea                                               | 4.29   | 0.79  | 0.698   |                       |
| perceived behavioural control | PB1 I can collaborate in the information security domain                | 3.92   | 0.106| 0.768   | 0.794                 |
|                 | PB2 I have enough experience and knowledge for ISC                    | 4.02   | 0.79  | 0.684   |                       |
|                 | PB3 I have enough resources and opportunity for ISC                   | 3.89   | 0.93  | 0.742   |                       |
| subjective norms| SNO1 my colleagues think I should collaborate in terms of information security | 4.16   | 0.76  | 0.618   | 0.819                 |
|                 | SNO2 The head of department thinks I should collaborate in the domain of information security | 4.23   | 0.99  | 0.586   |                       |
|                 | SNO3 my subordinates think I should collaborate in the domain of information security | 4.14   | 0.83  | 0.726   |                       |
| intention to ISC| IIS1 I am willing to collaborate with others in terms of information security | 4.26   | 0.79  | 0.738   | 0.837                 |
|                 | IIS2 I look forward to collaborating in information security           | 4.35   | 0.84  | 0.664   |                       |
|                 | IIS3 I intentionally collaborate with others to safeguard information assets | 4.18   | 0.91  | 0.589   |                       |
|                 | IIS4 I deliberately collaborate with others to decrease the chance of information security breaches | 3.84   | 1.06  | 0.725   |                       |
| Trust           | TRU1 Trust in my colleagues influences my ISC                         | 4.35   | 0.88  | 0.635   | 0.729                 |
|                 | TRU2 I rely on other staff for ISC                                     | 3.88   | 0.78  | 0.792   |                       |
|                 | TRU3 I can trust the security experts and collaborate with them in terms of information security | 4.36   | 0.98  | 0.802   |                       |
| organisational support | OSU1 I collaborate in terms of information security when my company values my efforts | 4.14   | 0.83  | 0.669   | 0.868                 |
|                 | OSU2 I collaborate in terms of information security when my workplace acknowledges my efforts | 4.22   | 0.81  | 0.586   |                       |
|                 | OSU3 I collaborate in terms of information security when my company encourages me | 3.92   | 0.79  | 0.764   |                       |
|                 | OSU4 I collaborate in terms of information security when my company respects my efforts | 3.94   | 0.83  | 0.586   |                       |
| ISC behaviour   | ISC1 I collaborate with others to have a secure environment for information security | 4.54   | 0.92  | 0.683   | 0.709                 |
|                 | ISC2 I assist other colleagues in terms of information security        | 4.42   | 0.97  | 0.765   |                       |
|                 | ISC3 I help other staff when they need my help in terms of information security | 3.88   | 0.75  | 0.638   |                       |
|                 | ISC4 I report information security incidents to the experts in my company | 4.24   | 0.71  | 0.722   |                       |
|                 | ISC5 I share my information security knowledge with other colleagues   | 4.06   | 0.83  | 0.768   |                       |

SD, standard deviation; ISC, information security collaboration; OISPs, organisational information security policies and procedures.

The items with <0.5 factor loading were dropped from the model.
Table 5  Correlation matrices and discriminant validity

|   | Mean | SD  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 |
|---|------|-----|----|----|----|----|----|----|----|----|----|----|----|
| 1 | 3.95 | 1.23| 0.821|
| 2 | INV  | 4.11| 0.87| 0.524| 0.768|
| 3 | COM  | 4.01| 0.95| 0.303| 0.615| 0.749|
| 4 | PNO  | 4.00| 1.21| 0.511| 0.369| 0.422| 0.763|
| 5 | ATI  | 3.91| 1.12| 0.292| 0.249| 0.199| 0.385| 0.762|
| 6 | PBC  | 3.97| 1.30| 0.188| 0.256| 0.279| 0.275| 0.208| 0.836|
| 7 | SNO  | 3.99| 0.98| 0.267| 0.527| 0.436| 0.238| 0.194| 0.378| 0.782|
| 8 | IIS  | 4.02| 1.23| 0.199| 0.236| 0.192| 0.269| 0.203| 0.298| 0.365| 0.723|
| 9 | TRU  | 3.91| 1.32| 0.361| 0.319| 0.269| 0.198| 0.197| 0.267| 0.268| 0.213| 0.842|
| 10| OSU  | 3.96| 0.86| 0.216| 0.268| 0.293| 0.296| 0.263| 0.196| 0.236| 0.296| 0.468| 0.722|
| 11| ISC  | 4.04| 0.92| 0.302| 0.289| 0.216| 0.288| 0.199| 0.202| 0.198| 0.386| 0.468| 0.826|