

Original citation:

Sohrabi Safa, Nader, Maple, Carsten, Watson, Tim and Furnell, Steven. (2017) Information security collaboration formation in organisations. IET Information Security .

Permanent WRAP URL:

<http://wrap.warwick.ac.uk/96351>

Copyright and reuse:

The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions. Copyright © and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable the material made available in WRAP has been checked for eligibility before being made available.

Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

Publisher's statement:

This paper is a postprint of a paper submitted to and accepted for publication in IET Information Security and is subject to Institution of Engineering and Technology Copyright. The copy of record is available at IET Digital Library

Published version: <https://doi.org/10.1049/iet-ifs.2017.0257>

A note on versions:

The version presented here may differ from the published version or, version of record, if you wish to cite this item you are advised to consult the publisher's version. Please see the 'permanent WRAP URL' above for details on accessing the published version and note that access may require a subscription.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk

Information security collaboration formation in organisations

Nader Sohrabi Safa^a, Carsten Maple^b, Tim Watson^c, Steve Furnell^d

Cyber Security Centre at WMG, University of Warwick, Coventry, United Kingdom^{a,b,c}
Centre for Research in Information and Cyber Security, Nelson Mandela Metropolitan University,
Port Elizabeth, South Africa^{a,d}

Centre for Security, Communications and Network Research, Plymouth University,
United Kingdom^d

Email: n.sohrabi-safa@warwick.ac.uk^a, cm@warwick.ac.uk^b, tw@warwick.ac.uk^c,
s.furnell@plymouth.ac.uk^d

Abstract

Collaboration between employees in the domain of information security efficiently mitigates the effect of information security attacks on organisations. Collaboration means working together to do or to fulfil a shared goal, the target of which in this paper is the protection of the information assets in organisations. Information Security Collaboration (ISC) aims to aggregate the employees' contribution against information security threats. This study clarifies how ISC is to be developed and how it helps to reduce the effect of attacks. The socialisation of collaboration in the domain of information security applies two essential theories: Social Bond Theory (SBT) and the Theory of Planned Behaviour (TPB). The results of the data analysis revealed that personal norms, involvement, and commitment significantly influence the employees' attitude towards ISC intention. However, contrary to our 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 towards ISC. The findings also show that the intention for ISC and organisational support positively influence ISC, but that trust does not significantly affect ISC behaviour.

Keywords: Information security, organisation, employee, collaboration, risk

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 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, sharing the ideas and expertise in order to enhance benefit, 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, corporation and collaboration are vital tasks in the information security domain. The level of commitment and severity 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 [9]. Collaboration is a value that originates from an individual's activities or the efforts of all participants. Proper collaboration brings greater efficiency and has fewer costs that are valuable output of collaboration [10]. ISC improve social aspects of information security, decrease the cost of attacks and increase the knowledge and experience of employees in organisations.

Participating in responding and recovering information security attacks, codification of policies and procedures that increase information security, reporting information security incidents, and sharing knowledge about information security are all ways in which ISC might manifest itself [11]. In this concept, 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, however, this domain needs more investigation into the effective factors and the development of ISC in organisations.

The structure of this paper is as follows: SBT, TPB and the Triandis Model constitute the background of the research model. The background theories together with the effective factors are described in section two. The applied methodology details the steps of the investigation, which is illustrated in section three. The analysis of data, and the results of statistical tests on the measurement model and structural model are scrutinised in section four. The effect of this research and its implementation are expounded upon in section five, and, finally, the conclusion and future work are discussed in section six.

2. Theoretical background and Conceptual Framework

The conceptual research model encompasses three basic theories. Figure 2 depicts how social bond factors influence employees' attitude, intention and their behaviour in order to collaborate and protect information assets.

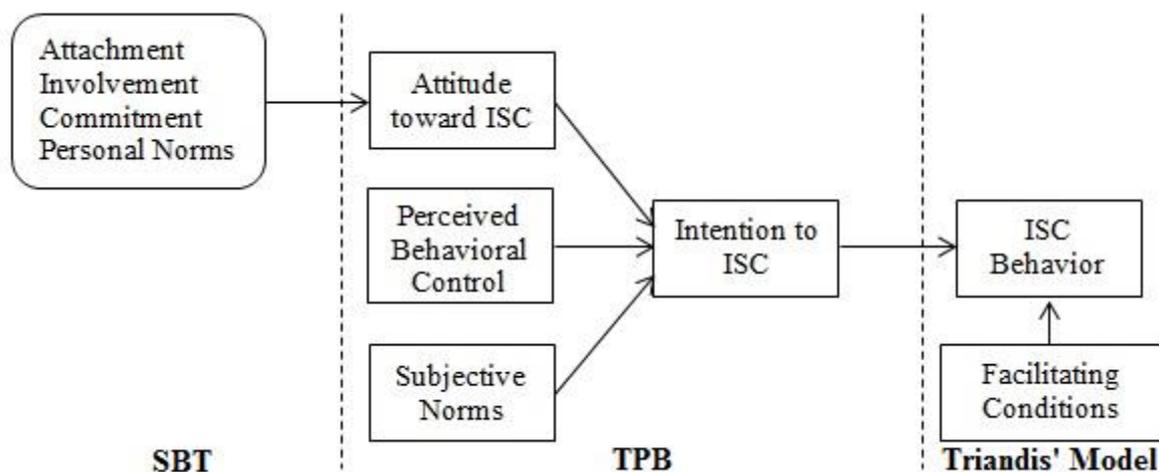


Figure 1: The research conceptual framework

2.1. Social Bond Theory

The Social Bond Theory (SBT) provides an interesting way to explain some social activities in organisations. The SBT, which was created by [12], says that social bonds represent the attachment to a firm, commitment to a community, involvement, and having an opinion that the kind of behaviour in question (information security collaboration) 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 [13]. 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 [14]. Attachment can be a motivationally efficacious factor in engaging in a particular behaviour because of its evolutionary pressure on individuals [15]. This pressure can motivate employees to help each other in order to protect information assets. Therefore, we hypothesise:

H1: 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 OISPs are all examples of our information security involvement in daily activities that affect our attitudes. Rocha Flores, Antonsen [16] 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 – information security knowledge sharing (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: 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 [17]. The employees' experience before joining to the organisation influences the employees' sense of obligation. An employers' commitment to an employees' well-being and rewards positively influences normative

commitment. Ifinedo [18] and 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 intention:

H3: 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 judgment [19]. 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 (TRA) [20] and subsequently extended to the TPB [21]. Li, Zhang [22] 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:

H4: Personal Norms positively influence the attitude towards ISC intention.

2.2. Theory of Planned Behaviour

The TPB, which was developed by Ajzen and Madden [21], 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. [18, 23] utilised the TPB to show how the disposition to comply with OISPs is formed in the organisations. Safa, Sookhak [3] also used the TPB to explain the formation of information security conscious care behaviour in organisations. In another study, Cox [24] 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 expression to 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 [18]. In another study, Cox [24] 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 [25]. 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 [26]. Workman, Bommer [27] 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 employees' 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 [28]. 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 [29] revealed that subjective norms influence the disclosure of information on social networks through perceived usefulness and perceived risk. In another study, Tamjidyamcholo, Bin Baba [30] 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 [31]. 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 [32]. In another study, Shropshire, Warkentin [33] used intention to show the adoption of information security behaviour in organisations. Park, Gu [34] showed that intention changes the employees' behaviour toward 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 [21]. Jeon, Kim [35] 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 [36]. 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 [33]. A well-designed team with good people can perform poorly if an organisation does not provide appropriate support and the necessary resources. Reid, Riemenschneider [37] asserted that organisational support influences the acceptance and use of information technology. A high level of organisational support causes a feeling of obligation amongst 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, Yang [38] 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 [39]. 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 [40], 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.

Figure 2 depicts the formation of the ISC in organisations in a concise form. The hypotheses one to four 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. The hypotheses eight to ten illustrate the effect of ISC intention, trust and organisational support on the ISC behaviour.

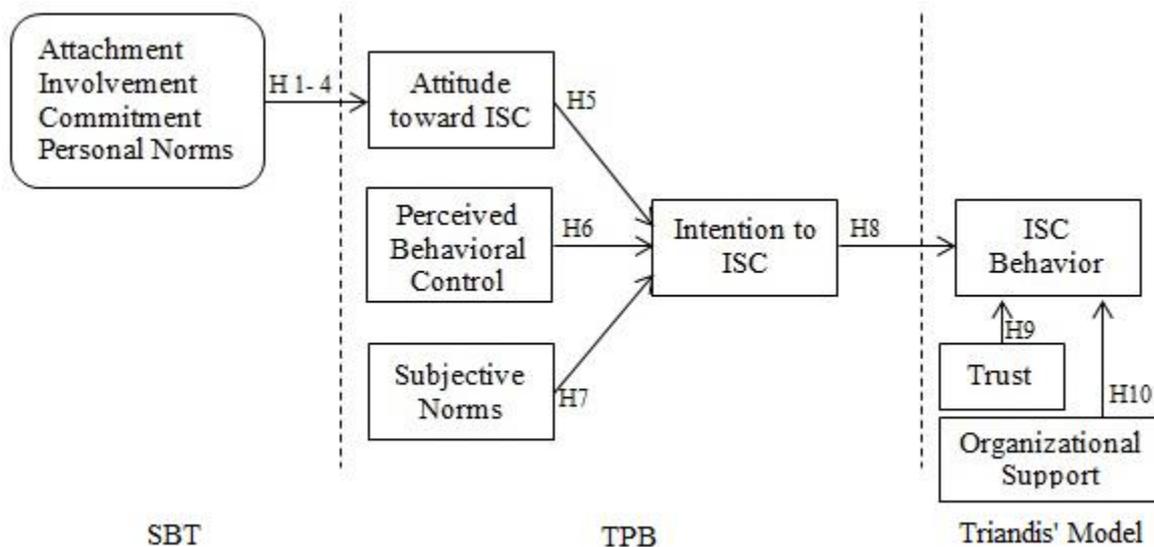


Figure 2: The research model and hypotheses

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 [24]. A review of the literature, in addition to the context of Social Bond Theory, 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 measurement model. 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 [41].

3.1. Data Collection

The employees of different organisations in South Africa functioned as 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 by 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 one hundred and forty-two used the paper-based questionnaire and two hundred and forty-three 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 two hundred and forty-three electronic questionnaires, thirty-three (13.5%) were omitted from the dataset either because of incomplete answers or because the same responses were given to all questions. Finally, three hundred and forty-four completed records were transferred to the main dataset. Table 1 shows the demography of the participants.

Table 1: Demography of participants

Measure	Items	Frequency	Per cent
<i>Gender</i>	Male	192	55.7
	Female	152	44.3
<i>Age</i>	21 to 30	111	32.2
	31 to 40	143	41.46
	41 to 50	67	19.63
	Above 50	23	6.71
<i>Education</i>	Diploma	23	6.8
	Bachelor	223	64.85
	Master	77	22.35
	PhD	21	6
<i>Position</i>	Employee	305	88.8
	Chief employee	30	8.7
	Management	9	2.5
<i>Industry</i>	Telecoms/IT	66	19.2
	Banking	98	28.5
	Manufacturing	81	23.5
	Education	99	28.8
<i>Work experience</i>	1 to 2 years	98	28.5
	3 to 5 years	170	49.4
	Above 5 years	76	22.1

4. Results

The effective factors in the research model are usually unobservable. Commitment, involvement, attachment, and personal norms are examples of the unobserved variables that need to be measured using several items. The Measurement Model (MM) and Structural Models (SM) are two components that are developed based on the observable and unobservable variables in the research model [41]. 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. Structural Equation Modelling (SEM) encompasses MM and SM and has been mentioned as a suitable statistical approach for this kind of research [42].

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 minus 2 and plus 2, which indicate the normal distribution of data [43]. The research model was developed based on SBP and TPB and previous studies. In this case, confirmatory factor analysis (CFA) is acknowledged to be an appropriate approach to test whether the constructs or factors are consistent with the items that measure them [44].

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. [41]. Therefore, the items with a factor loading of less than the threshold were dropped from the model.

The correlations between all two factors were tested in order to investigate the discriminant validity of the model. The results showed that the correlations between all two factors were less than the 0.9 threshold which indicates the discriminant validity of the model [45].

4.2. Testing the Structural model

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 2: Statistical indices

Fit indices	Model value	Acceptable standard
χ^2	988.89	-
χ^2/Df	1.98	<2
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 shows the results of the hypotheses testing.

Table 3: Hypotheses tests

Path	Standardized estimate	S.E.	p-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

5. Contribution and implementation

ISC has been identified as an important approach that decreases the risk of information security breaches 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 that explores whether ISC formation in organisations constitutes an effective and efficient approach that decreases the risk of information security incidents.

The important aspect of this study originates from the application 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 [18]; the output of his study also showed that attachment does not influence the attitude of employees towards complying with OISPs. Casper and Harris [15] 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 for management in organizations to mitigate 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, Parkin [46] 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 personalized 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 respondees’ IP address; in this way, participants with two or more responses can be detected.

References

1. Roumani, Y., J.K. Nwankpa, and Y.F. Roumani: *Examining the relationship between firm's financial records and security vulnerabilities*. International Journal of Information Management, 2016. **36**(6, Part A): p. 987-994. doi: <http://dx.doi.org/10.1016/j.ijinfomgt.2016.05.016>
2. Siponen, M., M. Adam Mahmood, and S. Pahnla: *Employees' adherence to information security policies: An exploratory field study*. Information & Management, 2014. **51**(2): p. 217-224. doi: <http://dx.doi.org/10.1016/j.im.2013.08.006>
3. Safa, N.S., et al.: *Information security conscious care behaviour formation in organizations*. Computers & Security, 2015. **53**(0): p. 65-78. doi: <http://dx.doi.org/10.1016/j.cose.2015.05.012>
4. Hassan, N.H., Z. Ismail, and N. Maarop. *A conceptual model for knowledge sharing towards information security culture in healthcare organization*. in *Research and Innovation in Information Systems (ICRIIS), 2013 International Conference on*. 2013.
5. Feledi, D., S. Fenz, and L. Lechner: *Toward web-based information security knowledge sharing*. Information Security Technical Report, 2013. **17**(4): p. 199-209. doi: <http://dx.doi.org/10.1016/j.istr.2013.03.004>
6. Tøndel, I.A., M.B. Line, and M.G. Jaatun: *Information security incident management: Current practice as reported in the literature*. Computers & Security, 2014. **45**(0): p. 42-57. doi: <http://dx.doi.org/10.1016/j.cose.2014.05.003>
7. Imperial, M.T.: *Using Collaboration as a Governance Strategy: Lessons From Six Watershed Management Programs*. Administration & Society, 2005. **37**(3): p. 281-320. doi: 10.1177/0095399705276111
8. Chen, Y.-H., T.-P. Lin, and D.C. Yen: *How to facilitate inter-organizational knowledge sharing: The impact of trust*. Information & Management, 2014: p. 568-578. doi: 10.1016/j.im.2014.03.007
9. Safa, N.S. and R. Von Solms: *An information security knowledge sharing model in organizations*. Computers in Human Behavior, 2016. **57**: p. 442-451. doi: <http://dx.doi.org/10.1016/j.chb.2015.12.037>
10. Austin, J.E. and M.M. Seitanidi: *Collaborative Value Creation: A Review of Partnering Between Nonprofits and Businesses: Part I. Value Creation Spectrum and Collaboration Stages*. Nonprofit and Voluntary Sector Quarterly, 2012. **41**(5): p. 726-758. doi: 10.1177/0899764012450777
11. Ahmad, A., S.B. Maynard, and G. Shanks: *A case analysis of information systems and security incident responses*. International Journal of Information Management, 2015. **35**(6): p. 717-723. doi: <http://dx.doi.org/10.1016/j.ijinfomgt.2015.08.001>
12. Hirschi, T.: *Causes of delinquency*. 1969: University of California Press.
13. Mesch, G.S.: *Social bonds and Internet pornographic exposure among adolescents*. Journal of Adolescence, 2009. **32**(3): p. 601-618. doi: <http://dx.doi.org/10.1016/j.adolescence.2008.06.004>
14. Reed, L.A., R.M. Tolman, and P. Safyer: *Too close for comfort: Attachment insecurity and electronic intrusion in college students' dating relationships*. Computers in Human Behavior, 2015. **50**(0): p. 431-438. doi: <http://dx.doi.org/10.1016/j.chb.2015.03.050>
15. Casper, W.J. and C.M. Harris: *Work-life benefits and organizational attachment: Self-interest utility and signaling theory models*. Journal of Vocational Behavior, 2008. **72**(1): p. 95-109. doi: <http://dx.doi.org/10.1016/j.jvb.2007.10.015>
16. Rocha Flores, W., E. Antonsen, and M. Ekstedt: *Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture*. Computers & Security, 2014. **43**(0): p. 90-110. doi: <http://dx.doi.org/10.1016/j.cose.2014.03.004>

17. Rivkin, W., S. Diestel, and K.H. Schmidt: *Affective commitment as a moderator of the adverse relationships between day-specific self-control demands and psychological well-being*. Journal of Vocational Behavior, 2015. **88**(0): p. 185-194. doi: <http://dx.doi.org/10.1016/j.jvb.2015.03.005>
18. Ifinedo, P.: *Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition*. Information & Management, 2014. **51**(1): p. 69-79. doi: <http://dx.doi.org/10.1016/j.im.2013.10.001>
19. Costa, A.I.d.A.: *Conceptualization and measurement of personal norms regarding meal preparation*. International Journal of Consumer Studies, 2013. **37**(6): p. 596-604. doi: 10.1111/ijcs.12036
20. Fishbein, M. and I. Ajzen: *On construct validity: A critique of Miniard and Cohen's paper*. Journal of Experimental Social Psychology, 1981. **17**(3): p. 340-350. doi: [http://dx.doi.org/10.1016/0022-1031\(81\)90032-9](http://dx.doi.org/10.1016/0022-1031(81)90032-9)
21. Ajzen, I. and T.J. Madden: *Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control*. Journal of Experimental Social Psychology, 1986. **22**(5): p. 453-474. doi: [http://dx.doi.org/10.1016/0022-1031\(86\)90045-4](http://dx.doi.org/10.1016/0022-1031(86)90045-4)
22. Li, H., J. Zhang, and R. Sarathy: *Understanding compliance with internet use policy from the perspective of rational choice theory*. Decision Support Systems, 2010. **48**(4): p. 635-645. doi: <http://dx.doi.org/10.1016/j.dss.2009.12.005>
23. Ifinedo, P.: *Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory*. Computers & Security, 2012. **31**(1): p. 83-95. doi: <http://dx.doi.org/10.1016/j.cose.2011.10.007>
24. Cox, J.: *Information systems user security: A structured model of the knowing–doing gap*. Computers in Human Behavior, 2012. **28**(5): p. 1849-1858. doi: <http://dx.doi.org/10.1016/j.chb.2012.05.003>
25. Jeon, S., Y.G. Kim, and J. Koh: *An integrative model for knowledge sharing in communities-of-practice*. Journal of Knowledge Management, 2011. **15**(2): p. 251-269. doi: 10.1108/13673271111119682
26. Reitz, H.J. and L.N. Jewell: *Sex, Locus of Control, and Job Involvement*. H. Joseph Reitz, Faculty, University of Florida, and Linda N. Jewell, Faculty, University of California-Irvine. Abstract from *Academy of Management Journal*, March 1979, p. 72. The International Executive, 1979. **21**(2): p. 17-18. doi: 10.1002/tie.5060210210
27. Workman, M., W.H. Bommer, and D. Straub: *Security lapses and the omission of information security measures: A threat control model and empirical test*. Computers in Human Behavior, 2008. **24**(6): p. 2799-2816. doi: <http://dx.doi.org/10.1016/j.chb.2008.04.005>
28. Pi, S.-M., C.-H. Chou, and H.-L. Liao: *A study of Facebook Groups members' knowledge sharing*. Computers in Human Behavior, 2013. **29**(5): p. 1971-1979. doi: <http://dx.doi.org/10.1016/j.chb.2013.04.019>
29. Shibchurn, J. and X. Yan: *Information disclosure on social networking sites: An intrinsic–extrinsic motivation perspective*. Computers in Human Behavior, 2015. **44**(0): p. 103-117. doi: <http://dx.doi.org/10.1016/j.chb.2014.10.059>
30. Tamjidyamcholo, A., et al.: *Evaluation model for knowledge sharing in information security professional virtual community*. Computers & Security, 2014. **43**(0): p. 19-34. doi: <http://dx.doi.org/10.1016/j.cose.2014.02.010>
31. Lee, W.-K.: *The temporal relationships among habit, intention and IS uses*. Computers in Human Behavior, 2014. **32**(0): p. 54-60. doi: <http://dx.doi.org/10.1016/j.chb.2013.11.010>
32. Sohrabi Safa, N., R. Von Solms, and S. Furnell: *Information security policy compliance model in organizations*. Computers & Security, 2016. **56**: p. 70-82. doi: <http://dx.doi.org/10.1016/j.cose.2015.10.006>

33. Shropshire, J., M. Warkentin, and S. Sharma: *Personality, attitudes, and intentions: Predicting initial adoption of information security behavior*. Computers & Security, 2015. **49**(0): p. 177-191. doi: <http://dx.doi.org/10.1016/j.cose.2015.01.002>
34. Park, J.H., et al.: *An investigation of information sharing and seeking behaviors in online investment communities*. Computers in Human Behavior, 2014. **31**(0): p. 1-12. doi: <http://dx.doi.org/10.1016/j.chb.2013.10.002>
35. Jeon, S.-H., Y.-G. Kim, and J. Koh: *Individual, social, and organizational contexts for active knowledge sharing in communities of practice*. Expert Systems with Applications, 2011. **38**(10): p. 12423-12431. doi: <http://dx.doi.org/10.1016/j.eswa.2011.04.023>
36. Triandis, H. *Values, attitudes, and interpersonal behavior*. in *Nebraska symposium on motivation*. 1980. Nebraska: University of Nebraska Press.
37. Reid, M.F., et al.: *Information Technology Employees in State Government: A Study of Affective Organizational Commitment, Job Involvement, and Job Satisfaction*. The American Review of Public Administration, 2008. **38**(1): p. 41-61. doi: 10.1177/0275074007303136
38. Cheng, P.-Y., et al.: *Ethical contexts and employee job responses in the hotel industry: The roles of work values and perceived organizational support*. International Journal of Hospitality Management, 2013. **34**(0): p. 108-115. doi: <http://dx.doi.org/10.1016/j.ijhm.2013.03.007>
39. Safa, N.S. and M.A. Ismail: *A customer loyalty formation model in electronic commerce*. Economic Modelling, 2013. **35**(0): p. 559-564. doi: <http://dx.doi.org/10.1016/j.econmod.2013.08.011>
40. Bryce, J. and J. Fraser: *The role of disclosure of personal information in the evaluation of risk and trust in young peoples' online interactions*. Computers in Human Behavior, 2014. **30**: p. 299-306. doi: 10.1016/j.chb.2013.09.012
41. Hair, J.F., et al.: *Multivariate Data Analysis*. Seventh Edition ed. 2010.
42. Arbuckle, J.L.: *Amos 16.0 User's Guide*. 2007, Chicago, IL 60606-6307, U.S.A.: SPSS, Inc.
43. Habibpor, K. and R. Safari: *Comprehensive guide for using SPSS software and data analysis*. 2008.
44. Ho, R.: *Handbook of Univariate and Multivariate Data Analysis and Interpretation with SPSS*. 2006, Boca Raton: Taylor & Francis Group.
45. Schumacker, R.E. and R.G. Lomax: *A Beginner's Guide to Structural Equation Modeling*. Third Edition ed. 2010, New York: Taylor & Francis Group.
46. Mace, J.C., S. Parkin, and A.v. Moorsel: *A Collaborative Ontology Development Tool for Information Security Managers* Proceedings of the 4th Symposium on Computer Human Interaction for the Management of Information Technology, 2010.