Motivation and opportunity based model to reduce information security insider threats in organisations

Nader Sohrabi Safa[a], *Carsten Maple*[b], *Tim Watson*[c], Rossouw Von Solms[d]
Cyber Security Centre at WMG, University of Warwick, Coventry, United Kingdom[a,b,c]
Centre for Research in Information and Cyber Security, School of ICT, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa[a,d]
Email: n.sohrabisafa@gmail.com[a], cm@warwick.ac.uk [b], tw@warwick.ac.uk [c]
rossouw.vonsolms@nmmu.ac.za[d]

Abstract

Information technology has brought many advantages for organisations, but information security is still a major concern in this domain. Users, whether intentionally or through negligence, are a great potential of risk to information assets. The lack of awareness, ignorance, negligence, resistance, disobedience, apathy and mischievous are root of information security incidents in organisations. As such, insider threats have attracted a number of experts' attention in this domain. Two particularly important considerations when exploring insider threats are motivation and opportunity. The most significant aspect of this research is derived from two fundamental theories – Social Bond Theory (SBT), used to motivate misbehaviour avoidance, and Situational Crime Prevention Theory (SCPT), to reduce the opportunities for misbehaviour. The results of data analysis show that situational prevention factors such as increasing the effort and risk, reducing the rewards and removing excuses can have a significant effect on negative attitudes towards misbehaviour, though reducing provocations does not have any effect on attitudes. Further, social bond factors such as commitment to organisational policies and procedures, involvement in information security activities and personal norms have significant effects on negative attitude towards misbehaviour. However, the attachment does not have any significant effect on employees' attitude in order to avoid misbehaviour. The findings also show that negative attitudes towards misbehaviour influence employees' intention positively, and in turn intention to avoid misbehaviour reduces insider threat behaviour. The outputs of this study shed some light on factors to reduce misbehaviour in the domain of information security for academics and practitioners.

Keywords: Information security, insider threat, organisation, risk, human factors

1. Introduction

Modern society is highly dependent on information technology systems; air traffic, defence, telecommunication, water distribution systems are examples of critical infrastructures that rely on information and in which information security is extremely important. Experts have, for many years, focused on the technological aspects of information security to guarantee a secure environment for information. However, it is acknowledged that the human aspects of information security play a vital role in this domain and should be taken into consideration along with technological aspects (Krombholz et al., 2015; Safa et al., 2015). Effective information security management cannot be realised without considering the roles of users and organisations (Posey et al., 2011). Attacks originating from insiders can have serious consequences on the appropriate functioning of computer systems (Magklaras et al., 2005). There are many types of insider, such as an auditor, customer, permanent or temporary employee, ex-employee or vendor, who have the legitimate capability to access one or many systems; the person interacts with the systems through an authentication mechanism. An insider does not need to spend as much effort and time to access the information target in comparison to external attackers. Organisations often trust them and anonymity is a characteristic that can decrease the risk of identification for them (Padayachee, 2015).

The Verizon Data Breach Investigations Reports (DBIR) (Verizon, 2016) presents a view of the threats, vulnerabilities and actions that lead to security incidents and the resulting impact on organisations based on real security data. DBIR 2016 asserts that 60% of threats can comprise organisations within minutes.

In this report, 55% of the incidents were the result of internal actors in organisations. Forty per cent of the incidents were perpetrated because of financial motivations whether the insider either planned to monetize the stolen data by selling it to others or by directly competing with their former employer. Figure 1 shows the variety of internal misuse pattern in 125 organisations.

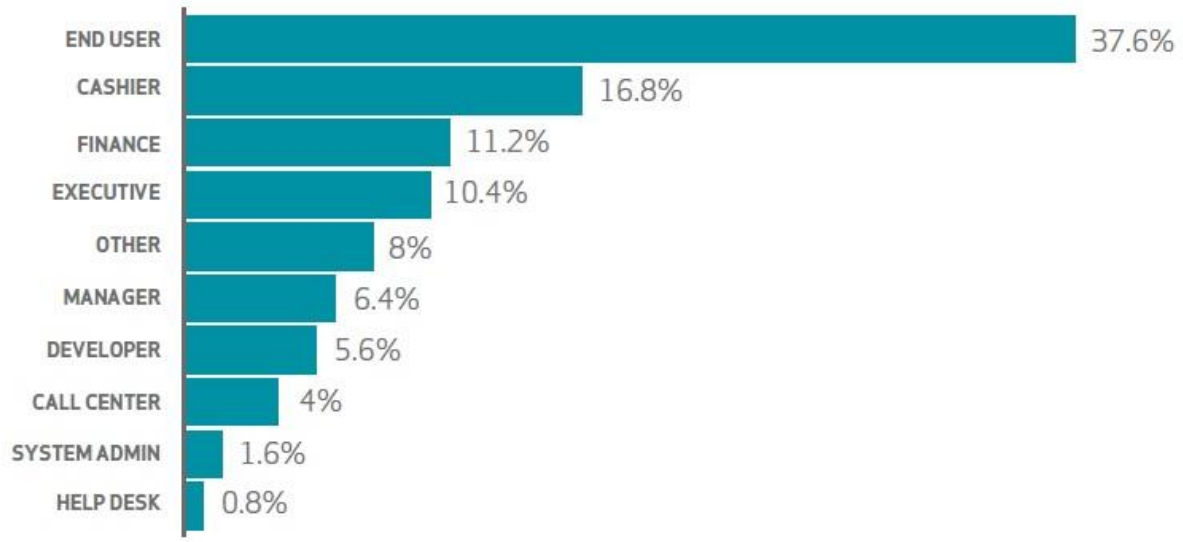

Figure 1: Internal Misuse Pattern (DBIR 2016)

Insider threats compromise information confidentiality, integrity and availability of information. Deletion, duplication, exfiltration and unauthorized extraction of critical information are examples of information security threats in this domain. The roots of these threats are apathy, bribery, corruption, espionage, embezzlement, extortion, ignorance and sabotage (Turkanović et al., 2013). It is acknowledged that both motivation and opportunity play crucial roles in the violation of information security rules and regulations (Padayachee, 2012).

Information security insider threats in organisations focuses on human (employees) as main subject in this domain. The convenience of conducting a crime and motivation for delinquency play important roles in the employees behaviour formation (Padayachee, 2013). In this research, a model has been presented to mitigate insider threats which is based on two important approaches – opportunity reduction for crime and motivation for avoiding misbehaviour. This study aims to investigate whether increasing the effort and risk for information security misbehaviour, reducing reward and provocations, and removing excuses for rationalisation of misbehaviour which originate from Situational Crime Prevention Theory mitigate insider threats in organisations. In addition, this research endeavours to examine whether employees' attachment and commitment to organisation, their involvement in information security activities and their belief about insider threats (personal norms) which come from Social Bond Theory influence their attitude and behaviour to avoid information security misbehaviour.

The structure of the paper is as follow: The definition of the insider threats and why this subject is important with some evidence have been presented in introduction section. The effective factors that mitigate insider threats originate from two fundamental theories; These theories with their factors have been explained in section two. Research methodology with data collection and demography of participants exist in section three. The results of data analysis (measurement model and structural model) have been discussed in section four. The contribution and implementation of the finding have demonstrated in section five, and finally limitation and future research directions have been presented in section six.

2. Theoretical background and Research model

It has been acknowledged that social bond factors have significant effect on individuals' behaviour (Chapple et al., 2005). On the other hand, opportunity for crim can motivate offenders to conduct a crim or delinquent rules and regulations (Willison, 2006). That is why, this research investigates the effect of employees' attachment and commitment to organisations, involvement in information security activities and personal norms about information security delinquency that originate from Social Bond Theory on one hand, and the effect of increasing effort and risk, decreasing rewards and provocation and removing excuses for violating information security rules and regulations based on Situational Crim Prevention Theory. These two theories will be explained more in the next sections.

2.1. Situational Crime Prevention Theory

Reducing or stopping criminal activities is the main subject in the crime prevention. Situational Crime Prevention Theory discusses opportunity-reduction mechanism for different types of crime. This is a common approach to decrease the opportunities for many types of crime or delinquent behaviour that occurs in a variety of settings (Gianluigi et al., 2005). Situational Crime Prevention helps organisations to control or design the environment in order to reduce crime or threats from different perspectives. Situational Crime Prevention Theory is used in areas such as society, school, organisation, social network, e-commerce and so forth. Situational Crime Prevention makes crime more difficult and risky, lowers rewards as the consequences of crime as well as reducing excuses for conducting crime (Padayachee, 2013). Rationalisation and available opportunities for offending play vital roles in the formation of illegal activities. It is argued that if offending is difficult, consequently, propensity to offend will be reduced. For instance, if we do not use lock for the door of our house, our house will be more likely to be robbed by a thief, because they do not need to put a lot of effort to enter to the house. Easy access to a target and its benefit encourage them for robbery. Offenders estimate the benefits of their action, the risk of identification and associated costs of apprehension. The outcome of this process helps them to make decision about conducting the crime or delinquent behaviour (Levan et al., 2015). Consequently we used this model of opportunity reduction approaches to decrease misbehaviour and consequently insider threats in organisations.

2.1.1. Increase the Effort

Increasing the difficulty of carrying out a policy violation, such as access control and monitoring of facilities, strong enforcement of password and account policies and closing the doors of unauthorised data exfiltration, can impact on misbehaviours (Coles-Kemp et al., 2010). These approaches increase the difficulty of executing violations by employees in organisations. Authentication has been proposed to control access to facilities. Clearly, authentication must be supplemented by access control in order to be an effective means of controlling access to data and systems in organisations. However, traditional access control such as role-based access control (RBAC) is susceptible to the insider threat since the system grants access as long as the access is authorised. Hence, finger-grained authentication and access control may be an effective strategy to increase the effort expended for misbehaviour (Guido et al., 2013). We therefore hypothesised that:

H1: Increasing the effort for information security misbehaviour negatively influences employees' attitude towards reduce misbehaviour intention.

2.1.2. Increase the Risk

Increasing the risk refers the increased probability of detecting the crime and identifying the offender, resistance and apprehension associated with malfeasance (Li et al., 2010). Using a log correlation engine, security information and event management system, monitoring and auditing employees' actions, monitoring and controlling remote access and reducing anonymity are examples that increase the risk for violators (Yusop et al., 2014). All of these approaches increase the negative consequences

associated with malfeasance. The promotion of insider reporting is another approach that leads to information security controls for assisting natural surveillance. Internal information security incidents usually are predicted by pattern of previous incidents; identification of these patterns and prediction of similar future incidents also increase the risk for offenders and decrease the risk of insider threats (Safa et al., 2014). An insider incident response plan helps to decrease the risk of internal incidents and their serious consequences. Organisations can help employees to have a proper judgment about the consequence of their misbehaviour. Based on the above explanations, we considered this hypothesis:

H2: Increasing the risk for information security misbehaviour negatively influences employees' attitude towards reduce misbehaviour intention.

2.1.3. Reduce the Rewards

Reducing the rewards relates to the benefits of the crime. Beebe et al. (2005) showed that a perception of minimal benefit by offenders discourages them from perpetrating crimes. They argue that sanctions are insufficient and reduction of benefits should be taken in to consideration in order to dissuade offenders from committing crimes. Several technics have been proposed to reduce the benefit for employees' misbehaviour. Watermarking (identifying property), encryption (denying benefits), minimising reconnaissance information (concealing targets), information and hardware segregation (removing target) and disrupting markets are examples of the methods that reduce the rewards of criminal activity (Padayachee, 2013). Digital signatures can prove useful for non-reputation, but it is necessary to uses additional validation to decrease violation, such as time stamps (Brdiczka et al., 2012). Encryption, automatic data destruction mechanisms and incident continuity management are offered as effective approaches that deny benefits, particularly when offenders plan to sell stolen data (Li et al., 2010). Based on the aforementioned explanations, we postulated that reducing the rewards discourages employees from misconduct in organisations. Therefore, the below hypothesis is presented:

H3: Reducing the rewards for information security misbehaviour positively influences employees' attitude towards reduce misbehaviour intention.

2.1.4. Reduce Provocations

Reducing provocation aims to decrease the emotional triggers that may precipitate a motivated criminal to commit an offence. Avoiding disputes and managing negative issues in the work environment, reducing emotional arousal, frustrations and stress, avoiding disputes, neutralising peer pressure and discouraging imitation are examples of provocation reduction strategies in organisations (Cheng et al., 2013; Willison, 2006). Silowash et al. (2012) asserted that user participation would be beneficial, as the insider threat may be precipitated by security policies or controls that are misunderstood, poor communicated or inconsistently applied (Cpni, 2016). Hence, it may be useful to involve users in the entire information security life cycle from development to implementation. Security usability also could be a step towards reducing the insider's negative response towards information security control. Anger, fear, guilt, happiness and joy are other factors that affect employees' attitude toward misbehaviour in the domain of information security; management should reduce any provocations that threat information security in organisations (Kim et al., 2016). Hence, the following hypothesis is proposed in this research:

H4: Reducing provocations for information security misbehaviour positively influences employees' attitude towards reduce misbehaviour intention.

2.1.5. Remove Excuses

Excuse for violation refers to rationalisations that criminals may use to justify their behaviour. The delinquents try to justify their misconduct as a logical and rational manner in order to avoid the true explanation (Barlow et al., 2013). The rationalisation also plays an important role in violating of information security policies and procedures when employees calculate how costly it would be to follow

the recommended security practices (Jahyun et al., 2014). For instance, an employee shares a network password because he/she rationalizes that no one is being injured as a result of his/her behaviour. These rationalisations cause even non-malicious employees to knowingly violate security policies. By rationalising their motivations, they try to decrease their guilty or shame for intentionally violating IT policies. These rationalisations make their behaviour seem more normal or more necessary than is actually the case (Siponen et al., 2010). Clear documents and consistently enforced policies, controls and monitoring are approaches that can remove excuses from employees' rationales for misconduct. Setting and clarification of rules (information security policy), alerting conscience (code of ethics), cyber ethics training (even controlling drugs and alcohol) and assisting compliance with organisational policies and rules are examples of other methods to remove excuses for misconduct. having a proper mindset, thought and cognition about different aspects of information security can help to avoid mistakes in cognition and remove excuses from employees. Based on the aforementioned explanations, we conjectured that:

H5: Removing excuses for information security misbehaviour positively influences employees' attitude towards reduce misbehaviour intention.

2.2. Social Bond Theory

Social Bond Theory (SBT) is one of the most interesting social theories that has recently attracted the attention of experts in different domains. SBT focuses on peers and peer groups of individuals as developed by (Hirschi, 1969). SBT describes some of employees' activities in organisations focusing on four main factors- attachment to organisation, commitment to organisational goals, involvement in a particular activity and personal norms. SBT also illustrates why people commit crimes. SBT describes that individuals who have stronger social ties, engage less in deviant behaviour. Deviance manifests when the social bond is broken or weak. These findings encouraged us to use this particular theory in this study.

SBT also clearly describes the delinquency of adolescents clearly. Their attachment to conventional significant other, commitment to achieve conventional goals, involvement to specific activities and their belief in the validity of common value systems influence their delinquent behaviour. In this state, they ignore law and their duty (Mesch, 2009). Lee et al. (2004) asserted that social bond factors significantly mitigate insider computer abuse in organisations. In another study, social bond factors were used to describe compliance with organisational information security policies and procedures in order to decrease the risk of information security threats (Ifinedo, 2014; Sohrabi Safa et al., 2016). In this research, social bond factors have been applied to reduce insider threats in organisations.

2.2.1. Attachment

Attachment refers to affection and respect that an individual considers for significant others, such as an organisation, job, supervisor and even co-workers (Sohrabi Safa et al., 2016). Employees with strong attachment are less likely to engage in deviant behaviour (Cheng et al., 2013). Staff need their supervisors or head of departments' support for promotion; they care about the recognition provided by these people (Ifinedo, 2014). Administrators evaluate their performance and following his/her advices will influence employees' behaviour to avoid misbehaviour in organisations and promote a safe environment for information assets. Hence, we consider the below hypothesis:

H6: Attachment to organisation positively influences employees' attitude towards reduce misbehaviour intention.

2.2.2. Commitment

Users are one of the main elements in the domain of information security. Their commitment and responsibility to safeguard information assets are crucial in ensuring the security of information (Alhogail, 2015). Commitment refers to their effort, promise and support to safeguard organisational information assets. Personal achievement and reputation are important to committed individuals (Cheng et al., 2013). They spend more time and energy in order to achieve success in their career. Committed persons would not take the risk of breaking rules that could thereby jeopardize or destroy their career aspirations (Pfleeger et al., 2012). Therefore, employees with more commitment to the organisation are less likely to deviate from the security policies or commit violations of information security. Hence, the following hypothesis is proposed:

H7: Commitment to organisational policies and procedures positively influences employees' attitude towards reduce misbehaviour intention.

2.2.3. Involvement

Involvement has attracted attention of experts in various domains such as advertising, education, marketing, social psychology and so forth, due to its effect on human behaviour. Involvement refers to the energy, participation and time that someone spends in a particular activity or subject (Chang et al., 2011). Involvement shows the relationship between individual and object. High level of involvement has more effect on the human behaviour based on cognitive, affect and behavioural model (Sun, 2008). Involvement has been studied in the domain of human aspects of information security recently. Ifinedo (2014) applied involvement in Social Bond Theory to show how compliance with organisational information security policies forms. Sohrabi Safa et al. (2016) continued this research and extended the concept of information security involvement to information security knowledge sharing, collaboration, learning and experience. In this research, involvement refers to energy, time and effort that an employee spends to protect information or improve information security in an organisation. That is why we postulated that employee's involvement in particular activities such as information security deters him/her from misconduct in the domain of information security:

H8: Involvement positively influences employees' attitude towards reduce misbehaviour intention.

2.2.4. Personal Norms

Personal norms refers to an individual's value and view on a particular subject, event or thing. For instance, violation of organisational information security policies and procedures is an unacceptable practice (Ifinedo, 2012). Personal norms influence individual's attitude, intention and consequently his/her actual behaviour. Li et al. (2010) described the effect of personal norms on employee's intention toward proper use of the Internet in organisations. Ifinedo (2014) and Sohrabi Safa et al. (2016) applied personal norms to explain its positive effect on complying with organisational information security policies and procedures. In this research, we assumed that an employee with the belief that information security misbehaviour is a negative and an unacceptable practice is less likely to violate information security rules in organisations. Therefore:

H9: Personal norms positively influence employees' attitude towards reduce misbehaviour intention.

2.3. Attitude, Intention and Behaviour

Evaluation by an individual forms their attitude about an object. Our attitude is an expression of favour or disfavour toward an activity, event, idea, person, place or thing from extremely negative to extremely positive (Hepler, 2015). Attitude also forms based on an individual's past and present experiences and therefore has a dynamic effect on human behaviour. Intention plays an important role between attitude and the formation of behaviour. Intention is a mental status that refers to a commitment to execute an action now or in the future. Intention has the concept of planning and achieving a goal (Safa et al.,

2016). Ajzen et al. (1986) asserted that behaviour is driven by behavioural intention where the behavioural intention is a function of an individual's attitude towards the behaviour. Ifinedo (2014) showed how social bond factors influence employees' attitude and consequently their intention towards complying with organisational information security policies and procedures. In the same way, Sohrabi Safa et al. (2016) described how information security knowledge sharing, information security collaboration, intervention and employees' information security experience besides the social bond factors positively influence employees' attitude and intention towards complying with information security policies. Siponen et al. (2014) study also revealed the relationship between employees' attitude, intention and finally behaviour in the domain of information security. In this research, we postulated that:

H10: Negative attitude towards information security misbehaviour reduces intention to misbehaviour.

H11: Lower intention to information security misbehaviour reduces insider threats in organisations.

Table 1 shows the definition of effective factors in a concise form.

Table 1: Definition of effective factors in the model

Theories	Constructs	Definitions
Situational Crime Prevention (opportunity reduction)	Increase the effort	Refers to the difficulty of executing the criminal opportunity which may discourage employees.
	Increase the risk	Refers to the consequences of crimes such as detection by management or termination.
	Reduce the rewards	Refers to the reducing benefits of committing a crime.
	Reduce provocations	Refers to removing or mitigating noxious stimuli such as unnecessary stress or competition, conflicts, and so forth from the environment.
	Remove excuses	Refers to the rationalisations of the crime.
Social Bond Factors	Attachment	Refers to the affection and respect that an individual has with others (identification of organisational values).
	Commitment	Refers to an individual's effort and energy expended to support their organisational goals (can be safeguard of information assets).
	Involvement	Refers to the amount of energy, participation and time one spends on conventional workplace activities.
	Personal norms	Refers to the individual's own values and views about an object (avoiding information security misbehaviour is a valuable behaviour).
Attitude, Intention and Behaviour Chain	Attitude	Refers to an expression of favour or disfavour toward an object (it can be information security misbehaviour).
	Intention	Refers to planning and forethought to carry out an action now or in the future.
	Insider threats	Information security threats that originate from inside an organisation.

Figure 2 shows research conceptual framework with more details.

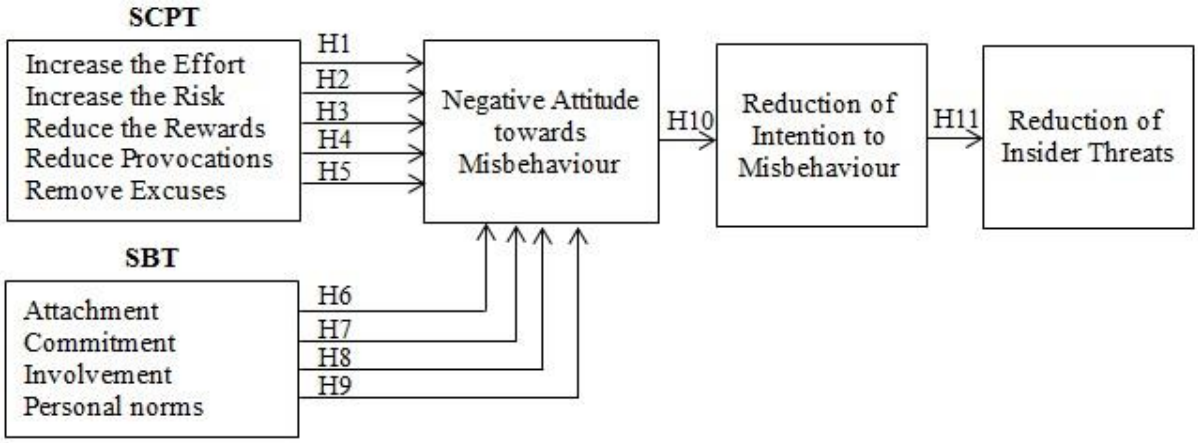

Figure 2:Conceptual model and hypotheses

3. Research Methodology

This research aims to conceptualise information security insider threats in organisations. A review of literature revealed that opportunity and motivation play important roles in the formation of insider threats. Five opportunity reduction strategies in order to decrease the chance of insider threats beside social bond factors in order to motivate employees to avoid information security misbehaviour formed the research model. We asked experts in this domain review the research model and inform us whether the conceptual model is in line with their experience and knowledge. The conceptual framework was approved by experts in this realm. Quantitative and qualitative approaches were applied in the course of the framework development. A questionnaire by means of five Likert scale was developed based on the concept of main factors and with respect to the previous studies. In order to expedite the process of data collection, data were collected by electronic questionnaire and paper-based questionnaire. The research model was developed based on two basic theories – the Situational Crime Prevention and Social Bond Theory – and a review of literature; that is why we considered Confirmatory Factor Analysis (CFA) approach in this research. Structural Equation Modelling (SEM) was used to test the reliability and validity of the model. Measurement model and structural model are two important parts of SEM. More explanation about these two important parts with their results will be presented in the next sections.

3.1. Data Collection

Data were collected from staff of several organisation that they are active in the field of e-Commerce, banking and insurance in South Africa. The employees were familiar with the importance of information security. These companies established organisational information security policies and procedures to safeguard their information assets. All staff should follow these rules and regulations. Data gathering was conducted from the first of September 2015 to end of December 2015. The questionnaire was developed based on the concept of factors and previous studies in this domain. The responses of questions were based on five Likert scale from strongly disagree to strongly agree. The aim of this study was described for participants and then we invited them to answer the questions based on their own knowledge and experiences. The consent of participants was important for us; after an indication of their consents to participate in this research, we requested to answer to questionnaire. We expressed for them that data would be kept confidential and only used for academic purposes in this research. The questionnaire was pilot-tested with 46 participants in order to be sure about applicability, comprehension and the unique interpretation of the questions. We observed their emotions, descriptions that the participants requested about questions and their hesitations. We revised and changed some words or sentences based on their feedbacks in order to increase the comprehension of the questions. It is important for us to be sure that they can understand questions easily and interpret them similar to

each other. The final version of the questionnaire was included 51 questions that every several questions (items) measure a main factor. Table 3 shows measurement model with its statistics in a concise form.

3.2. Demography

Two approaches were applied in order to speed up the process of data collection; data were collected by electronic questionnaire and paper-based questionnaire. Six hundred twelve participants answer the questionnaires, in which, two hundred and eleven were through the paper-based questionnaire and four hundred and one were through electronic questionnaire. We reviewed immediately the responses in order to decrease the number of incomplete questionnaires and kindly requested to reply the neglected questions. Nevertheless, twenty five (11.8%) paper-based questionnaires were discarded due to incomplete answers or because of the same responses were given to all items (questions).

The facilities in Google Forms efficiently helped us for data gathering; the electronic questionnaire was emailed to the email of some participants who we had their emails. Among four hundred and one questionnaires that we sent to the emails of participants, sixty nine questionnaires were rejected from the dataset due to incomplete responses or because of the same responses to all questions. Finally, five hundred eighteen questionnaires were collected for the data analysis. Table 2 shows the demography of respondents in a concise form.

Table 2: Participants' characteristics

Measure	Items	Frequency	Percent
Gender	Male	278	53.67
	Female	240	46.33
Age	21 to 30	142	27.41
	31 to 40	193	37.26
	41 to 50	105	20.27
	Above 50	78	15.06
Position	Employee	476	91.89
	Chief employee	31	5.98
	Management	11	2.13
Work experience	1 to 2 years	131	25.29
	3 to 5 years	276	53.28
	Above 5 years	111	21.43
Education	Diploma	42	8.11
	Bachelor	333	64.29
	Master	124	23.94
	PhD	19	3.66

4. Results

The variables that researchers usually measure are unobservable (latent) or unquantifiable such as effort, risk, attachment, commitment and so forth. These kinds of variables measure with several items (questions) that show the main factor. The measurement and structural models were developed based on the observed and latent variables in this research. The measurement model depicts the relationships between the measured variables with latent variables. The validity and reliability of the observed variables (indicators) were examined before the measurement model was fitted to the data. The relationships among the latent variables were tested in the structural model. Structural equation modelling has been acknowledge as the most appropriate approach for this kind of research (Hair et al., 2010).

4.1. Measurement Model

It is acknowledged that SEM is the most appropriate approach to explore relationship among variables and the data fit to the hypotheses. SEM isolate the error when measures the unobservable variables with observable variables (items). SEM also estimates regression among the unobservable variables. The

standard skewness and kurtosis were applied to test normal distribution of data. The results of these tests were between -2 and +2, which shows a normal distribution of data (Habibpor et al., 2008). The research model was formed based on a review of literature and two fundamental theories. That is why, Confirmatory Factor Analysis (CFA) has been applied to investigate whether the measured variables are consist with our understanding of the nature of the constructs or factors (Ho, 2006).

Factor loading of the measurement variables shows the convergent validity. Factor loading greater than 0.5 shows an acceptable convergent validity (Hair et al., 2010). Hence, we omitted items with factor loading less than 0.5 from the model. IE5 in the Increase Effort, RE4 in the Remove Excuses, AT3 in the Attachment, and PN2 in the Personal Norms were dropped from the model due to their lower factor loading on the related constructs. Internal consistency relates to the correlation among the items that can measure a factor. Cronbach's Alpha shows the internal consistency. The measure of Cronbach's Alpha for all constructs exceeded the threshold of 0.7, which indicates the composite reliability of the constructs (Arbuckle, 2007). Table 3 shows the results of statistical tests in a concise form.

Table 3: The constructs, the items, and their descriptive statistics

Constructs		Items	Mean	Std Dev	CFA Loading	Composite reliability
Increase the Effort	IE1	Control on information affects my attitude to be careful about my manner.	4.02	.82	.624	.802
	IE2	Surveillance on employee's access to information influences my attitude to be careful about my manner.	3.98	.78	.706	
	IE3	My effort to pass from access control affects my attitude towards avoiding misbehaviour.	4.24	.86	.596	
	IE4	Authentication systems influence my attitude to avoid misbehaviour.	4.18	.94	.692	
	IE5	Isolation of sensitive systems prompts me to avoid any misbehaviour.	3.86	.102	Dropped	
Increase the Risk	IR1	Probability of identification affects my attitude to be careful about my behaviour.	4.12	.94	.712	.742
	IR2	Tracking my access to information on the systems influences my attitude to be careful about my manner.	4.36	.68	.744	
	IR3	Reducing anonymity influence my attitude to avoid misbehaviour in organisation.	3.99	.74	.603	
	IR4	Monitoring and controlling remote access influence on my attitude to be careful about my behaviour.	4.16	.86	.728	
	IR5	Apprehension associated with misbehaviour affect my attitude to be careful about my manner.	4.26	.92	.782	
Reduce the Rewards	RR1	Encryption of data prevents suitability of data for selling and discourages employees to misbehaviour.	4.22	.68	.732	.782
	RR2	Automatic data destruction prevents to achieve data for abuse that discourage employees for misbehaviour.	3.88	.82	.806	
	RR3	Identification of property with watermarking decreases the benefit and affects employees' attitude to avoid misbehaviour.	4.32	.96	.704	
	RR4	Elimination of benefits influences employees' attitude to avoid information security misbehaviour in organisations.	4.08	.88	.746	
Reduce Provocations	RP1	Reducing employees' frustration and stress decrease provocation for information security misbehaviour.	4.18	.78	.662	.714

	RP2	Avoiding disputes reduce provocation and positively influences employees' attitude to avoid misbehaviour.	3.94	.82	.728	
	RP3	Reducing emotional arousal decrease provocation and positively influences employees' attitude to avoid misbehaviour.	4.08	.98	.698	
	RP4	I believe reducing provocations in organisations positively influences employees' attitude to avoid misbehaviour.	4.02	1.04	.738	
Remove Excuses	RE1	Clarification of information security policies positively influences employees' attitude to avoid misbehaviour.	4.14	1.06	.754	.798
	RE2	Assisting compliance with organisational information security policies positively influences employees' attitude to avoid misbehaviour.	4.06	.96	.749	
	RE3	Alerting employees' conscience positively influences employees' attitude to avoid misbehaviour.	4.22	.91	.736	
	RE4	Cyber ethics training positively influences employees' attitude to avoid misbehaviour.	3.88	.87	Dropped	
	RE5	Removing excuses from organisational environment positively affect employees' attitude to avoid misbehaviour.	4.06	.89	.704	
Attachment	AT1	My organisation's concerns about information security breaches are important for me.	4.26	.68	.762	.806
	AT2	I like to put my effort to safeguard organisational information assets.	4.32	.93	.748	
	AT3	I think the organisational problems are my problem.	4.04	1.09	Dropped	
	AT4	My interest to my organisation prevents me to think about misbehaviour.	3.94	.85	.801	
Commitment	CO1	I am committed to safeguard organisational information security assets.	4.26	.97	.764	.718
	CO2	I am committed to avoid any misbehaviour that jeopardizes information security.	4.16	.84	.742	
	CO3	I invest my energy and effort to make organisational environment secure for information assets.	3.88	.89	.814	
	CO4	I am committed to follow organisational information security policies in order to avoid any misbehaviour.	4.24	.82	.766	
Involvement	IN1	I actively involve myself in information security activities in order to avoid misbehaviour.	4.08	.96	.728	.788
	IN2	I attend information security training course in order to avoid misbehaviour.	4.14	.88	.708	
	IN3	I follow information security policies in order to avoid misbehaviour.	4.36	.87	.732	
	IN4	I value to participate in any information security activity.	4.18	.93	.788	
Personal Norms	PN1	Information security misbehaviour is a serious matter for me.	4.24	.89	.736	.742
	PN2	Information security misbehaviour is unacceptable for me.	3.84	.95	Dropped	
	PN3	I believe that avoiding information security misbehaviour affect organisational success.	4.26	1.05	.586	
	PN4	I believe that we should avoid any risky behaviour that threats information security.	4.08	.97	.668	
Attitude	ATT1	Information security misbehaviour is unacceptable for me.	4.22	.91	.589	.798

	ATT2	I esteem my organisational plan in order to decrease insider threats.	4.16	1.07	.726	
	ATT3	Organisational information security plans are important for me.	4.32	.86	.664	
	ATT4	I respect my organisational concern about insider threats.	3.88	.98	.678	
Intention	INT1	I plan to improve my information security behaviour.	4.20	.95	.718	.768
	INT2	I intend to care about my information security behaviour.	4.32	.89	.598	
	INT3	It is my intention to avoid any information security misbehaviour.	4.24	.96	.652	
	INT4	My intention to avoid misbehaviour positively influences my future behaviour.	3.82	.82	.738	
Actual Misbehaviour	BE1	I avoid any risky behaviour to safeguard information assets.	4.28	1.04	.716	.728
	BE2	I think about the consequence of my behaviour to avoid any information security misbehaviour.	3.88	.98	.676	
	BE3	I consult with information security experts to avoid any information security misbehaviour.	4.02	.86	.584	
	BE4	I never jeopardize information security with my behaviour.	4.22	.94	.648	

Although the unidimensional grouping shows discriminant and convergent validity, as the constructs are independent and unique, in order to explore the convergent and the discriminant validity of the instruments, we linked constructs to one another. Convergent validity was tested to indicate whether it is evident in the relationships between two related constructs, based on the research model. Correlations between theoretically different measures should be low. Discriminant validity shows the absence of any relationships between those constructs that should not relate to each other, based on the conceptual framework (Hair et al., 2010).

Table 4: Correlation between different constructs

		Mean	SD	1	2	3	4	5	6	7	8	9	10	11	12
1	**IE**	4.11	0.98	0.838											
2	**IR**	4.18	0.75	0.402	0.826										
3	**RR**	4.13	0.83	0.301	0.402	0.769									
4	**RP**	4.01	1.01	0.519	0.386	0.402	0.798								
5	**RE**	4.12	1.12	0.498	0.414	0.417	0.275	0.891							
6	**AT**	4.17	0.94	0.542	0.255	0.278	0.276	0.218	0.827						
7	**CO**	4.14	0.88	0.244	0.512	0.332	0.276	0.429	0.498	0.818					
8	**IN**	4.19	1.06	0.312	0.422	0.421	0.316	0.495	0.346	0.535	0.858				
9	**PN**	4.18	1.23	0.198	0.230	0.196	0.267	0.203	0.295	0.375	0.402	.719			
10	**ATT**	4.15	0.89	0.638	0.552	0.603	0.638	0.256	0.503	0.498	0.358	0.579	.849		
11	**INT**	4.19	1.32	0.346	0.361	0.276	0.186	0.199	0.248	0.264	0.613	0.343	0.566	0.836	
12	**BE**	4.10	0.96	0.104	0.216	0.201	0.328	0.241	0.194	0.306	0.328	0.331	0.398	0.484	0.706

4.2. Testing the Structural Model

Structural equation modelling (SEM) encompasses a family of statistical methods to test a conceptual or theoretical model. SEM is widely applied in the different research areas, due to its ability to isolate observational errors from the measurement of latent variables. SEM explores the relationships among the dependent, independent, mediating and moderating variables. SEM considers reliable measurements, when it estimates the relationships among the variables and examines the overall data fit to the conceptual model. IBM Amos version 20 was used to calculate the models' parameters.

Confirmatory and exploratory factor analyses are two approaches in this domain. In this research, the conceptual framework stems from a review of the literature and two fundamental theories. This is why we applied confirmatory factor analysis (CFA). Comparative fit measures and global fit measures are two methods that were applied to explore the fit indices. The Chi-square test (χ^2) with degrees of freedom is commonly used as the global fit criterion. Chi-square / df also indicates the extent to which the data are compatible with the hypotheses. A model with better fit with the data would indicate a small Chi-square measure, and a Chi-square / df ratio of 2 or less (Arbuckle, 2007).

The hypotheses of the research may be rejected due to inappropriate sample size. The Chi-square is sensitive to sample size. Fortunately, the results show an adequate sample size for this test. The fit between the actual or observed data and the predicted values from the proposed model were examined by the Goodness of Fit Index (GFI). The Adjusted Goodness of Fit Index (AGFI) is another measure that is GFI when considering the degree of freedom. To test the data against the null model, the Comparative Fit Index (CFI) was calculated. A GFI, AGFI, CFI with measures greater than 0.9 is recommended by the experts (Byrne, 1994). To evaluate the model on the basis of the discrepancy and the degree of freedom, the Incremental Fit Index (IFI) is a useful complementary measure. IFI measures close to 1 show a very good Fit. To investigate the minimum discrepancy of the baseline model with the data, the Normed Fit Index (NFI) was computed (Bagozzi et al., 2011). If the data fit with the model perfectly, the measure of the NFI would be equal to 1. To answer the question of "how well does the model fit the population covariance matrix?" the Root Mean Square Error of Approximation (RMSEA) is another method that can be applied in the data analysis. An RMSEA measure with a value of less than 0.08 is considered good (Schumacker et al., 2010). Table 5 shows the model fit indices in a concise format.

Table 5: Model fit indices

Fit indices	Model value	Acceptable standard
χ^2	1118.89	-
χ^2/Df	1.92	<2
GFI	0.942	>0.9
AGFI	0.924	>0.9
CFI	0.912	>0.9
IFI	0.924	>0.9
NFI	0.936	>0.9
RMSEA	0.078	<0.08

The results of the data analysis are presented in Table 6. The outcomes showed that the path from increase the effort (β=0.712, p=0.012), increase the risk (β=0.689, p=0.008), reduce the rewards (β=0.622, p=0.012) and remove excuse (β=0.502, p=0.001) towards negative attitude about misbehaviour were significant. However, the effect of reduce provocation towards attitude was not significant. Therefore, H4 is rejected. The findings also revealed that, commitment to organisational plan and policies (β=0.742, p=0.004), involvement in information security activities (β=0.689, p=0.016) and personal norms (β=0.516, p=0.014) towards negative attitude about misbehaviour were significant; but attachment does not influence attitude significantly. Finally, the results showed that negative attitude about misbehaviour (β=0.718, p=0.001) significantly reduce intention to misbehaviour and reduction of intention to misbehaviour (β=0.698, p=0.001) reduces insider threats significantly.

Table 6: The results of the hypotheses testing

Path			Standardized estimate	*p*-Value	Results
IE	→	ATT	0.712	0.012	Support
IR	→	ATT	0.689	0.008	Support
RR	→	ATT	0.622	0.012	Support
RP	→	ATT	0.403	0.061	Not-Supported
RE	→	ATT	0.502	0.001	Support
AT	→	ATT	0.395	0.058	Not-Supported
CO	→	ATT	0.742	0.004	Support
IN	→	ATT	0.689	0.016	Support
PN	→	ATT	0.516	0.014	Support
ATT	→	INT	0.718	0.001	Support
INT	→	BE	0.698	0.001	Support

5. Contribution and Implementations

We unfold the Situational Crime Theory in order to describe how opportunity reduction strategies can mitigate the risk of insider threats in organisations. In addition, Social Bond Factors were used to increase the motivation of employees in order to avoid misbehaviour. To the best of our knowledge, this is among the first studies that conceptualize insider threats based on opportunity and motivation to avoid information security misbehaviour in organisations. This integrative conceptualization offers a new perspective to better understand insider threats formation. We believe, this supplements the previous researches that were published in this domain.

The results of data analysis showed that increase the effort and risk, reduce the rewards and remove excuses significantly reduced misbehaviour and consequently insider threats. However, reduce provocations does not significantly reduce insider threats. Based on Social Exchange Theory, individuals' behaviour is function of their intention that attitude toward the subject play an important role to form the intention (Ajzen et al., 1986). Increase the risk and effort and reduce the benefits or rewards are factors that affect employees' attitude and decision to avoid misbehaviour. Remove the excuse also negatively effect on employees' decision to engage to information security misbehaviour. One plausible explanation for this finding can originate from the Motivation Theory. Based on this theory, satisfying a need, desire, curiosity, anger, revenge and so forth are the reason and motivation for many actions (Ryan et al., 2010). Removing such excuses from organisational environment can decrease many of misbehaviour. Unlike to our expectation, reduce the provocation has not significant effect on employees' misbehaviour. One conceivable explanation for this finding might relate to the culture of people in this environment.

We postulated that employees' commitment influences their attitude towards reduce their intention to conduct misbehaviour based on a review of literature. Committed persons will not take the risk of jeopardise their role in organisations (Sohrabi Safa et al., 2016). Fortunately, the results of statistical analysis showed a significant relationship between commitment and individuals' attitude towards reduce intention to conduct misbehaviour. Involvement in information security activities and personal belief that information security misbehaviour is a negative and unacceptable manner, have significantly effect on employees' attitude towards reduce misbehaviour intention. But, attachment did not influence attitude towards reduce misbehaviour intention. This findings is in line with Ifinedo (2014) research output. One conceivable reason for this finding can be in individuals' self-interest for such discord (Casper et al., 2008). The review of literature, proofs and supports besides the results of statistical analysis show the soundness and effectiveness of the proposed approach.

6. Conclusion, Limitation and Future Works

The Internet has become a conduit for services, applications, information content and opportunities for individuals and organisations. However, anecdotal and empirical evidence implies that the number and severity of information security breaches is growing; information security breaches and privacy violations are main concern of both users and firms. Remarkable portion of these threats refers to insider of organisation. Reduction of information security insider threats should be taken into the consideration. In this regard, a conceptual model has been presented that shows how we can reduce insider threats in organisations. The significant aspect of this study is derived from inclusion of Situational Crime Theory and Social Bond Theory on one hand, and psychological effect of password, authentication, access control, monitoring system and surveillance, incident management and so forth on employees' behaviour, on the other hand. We adopted opportunity reduction strategies in the domain of information security and showed that increase the effort and risk, reduce reward and remove excuses decrease insider threats in organisations. In addition, this study describes how involvement in information security activities, commitment to organisational plan and policies and personal norms that information security misbehaviour is unacceptable, can mitigate insider threats in organisations.

This study suggests, managements should pay attention to the environmental factors that encourage employees towards information security misbehaviour. Identification and classification of these environmental factors and appropriate plan to decrease their negative effects on employees' behaviour can mitigate the risk of insider threats. This research shows the importance of human and psychological aspects of information security clearly. Proper information security training and psychological consultations can be a solution for insider threats particularly when rationalisation of misbehaviour plays an important role.

The finding also showed that information security involvement decrease insider threats. Staff involve in information security activities in the different shapes; information security knowledge sharing, information security collaboration and information security experience are different forms of involvement. Researchers can also investigate the effects of these activities on insider threats in the future.

This research can be extended further; we can look to the information security insider threats from different perspective. Motivations for misbehaviour play a vital role in the domain of information security insider threats. Identification of motivational factors and classification of them in two groups of intrinsic and extrinsic motivations can help management to control and decrease insider threats in organisations. Another clue for future research can be identification and classification of opportunities that have the potential of information security threats in organisation; removing these opportunities from inter-organisational environment can significantly improve security of information assets.

There were limitations to this study. The samples in this study were collected from companies that have established suitable information security policies in South Africa. One of the limitations is the paucity of organisations that have established information security policies in order to mitigate the risk of information breaches in their institutions. It is a hard task obtaining permission from organisations for survey and data collection in the domain of their information security; however, the generalization of findings can be improved with a bigger sample size and more companies for investigation. Data collection was conducted in South Africa. This can be extended to other countries as well. Another important limitation stems from the inability to control double responses by participants that fill out the electronic questionnaire through Google Drive. Such concerns can be addressed by controlling the responses' IP address. In this way, we can detect participants with two or more responses.

References

Ajzen, Icek, & Madden, Thomas J. (1986). Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of Experimental Social Psychology, 22*(5), 453-474. doi: http://dx.doi.org/10.1016/0022-1031(86)90045-4

AlHogail, Areej. (2015). Design and validation of information security culture framework. *Computers in Human Behavior, 49*, 567-575. doi: http://dx.doi.org/10.1016/j.chb.2015.03.054

Arbuckle, James L. (2007). *Amos 16.0 User's Guide*. Chicago, IL 60606-6307, U.S.A.: SPSS, Inc.

Bagozzi, Richard P., & Yi, Youjae. (2011). Specification, evaluation, and interpretation of structural equation models. *Academy of Marketing Science 40*, 8-34. doi: 10.1007/s11747-011-0278-x

Barlow, Jordan B., Warkentin, Merrill, Ormond, Dustin, & Dennis, Alan R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security, 39, Part B*, 145-159. doi: http://dx.doi.org/10.1016/j.cose.2013.05.006

Beebe, Nicole Lang, & Rao, V. Srinivasan. (2005). *Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security*. Paper presented at the SoftWars Conference LasVegas, NV.

Brdiczka, O., Juan, Liu, Price, B., Jianqiang, Shen, Patil, A., Chow, R., . . . Ducheneaut, N. (2012, 24-25 May 2012). *Proactive Insider Threat Detection through Graph Learning and Psychological Context.* Paper presented at the Security and Privacy Workshops (SPW), 2012 IEEE Symposium on.

Byrne, Barbara M. (1994). *Structural Equation Modeling with EQS and EQS-Windows: Basic Concepts, Applications, and Programming*: Sage Publications, Inc. Thousand Oaks, CA, USA.

Casper, Wendy J., & Harris, Christopher M. (2008). Work-life benefits and organizational attachment: Self-interest utility and signaling theory models. *Journal of Vocational Behavior, 72*(1), 95-109. doi: http://dx.doi.org/10.1016/j.jvb.2007.10.015

Chang, Hsin Hsin, & Chuang, Shuang-Shii. (2011). Social capital and individual motivations on knowledge sharing: Participant involvement as a moderator. *Information & Management, 48*(1), 9-18. doi: http://dx.doi.org/10.1016/j.im.2010.11.001

Chapple, Constance L., McQuillan, Julia A., & Berdahl, Terceira A. (2005). Gender, social bonds, and delinquency: a comparison of boys' and girls' models. *Social Science Research, 34*(2), 357-383. doi: http://dx.doi.org/10.1016/j.ssresearch.2004.04.003

Cheng, Lijiao, Li, Ying, Li, Wenli, Holm, Eric, & Zhai, Qingguo. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security, 39, Part B*(0), 447-459. doi: http://dx.doi.org/10.1016/j.cose.2013.09.009

Coles-Kemp, Lizzie, & Theoharidou, Marianthi. (2010). Insider Threat and Information Security Management. In C. W. Probst, J. Hunker, D. Gollmann & M. Bishop (Eds.), *Insider Threats in Cyber Security* (Vol. 49, pp. 45-71): Springer US.

CPNI. (2016). Centre for the Protection of National Infrastructure from http://www.cpni.gov.uk/about/context/

Gianluigi, Me, & Spagnoletti, P. (2005, 21-24 Nov. 2005). *Situational Crime Prevention and Cyber-crime investigation: the Online Pedo-pornography case study.* Paper presented at the Computer as a Tool, 2005. EUROCON 2005.The International Conference on.

Guido, Mark D., & Brooks, Marc W. (2013, 7-10 Jan. 2013). *Insider Threat Program Best Practices.* Paper presented at the System Sciences (HICSS), 2013 46th Hawaii International Conference on.

Habibpor, Karim, & Safari, Reza. (2008). *Comprehensive guide for using SPSS software and data analysis*.

Hair, Joseph F., Black, William C., Babin, Barry J., & Anderson, Rolph E. (2010). *Multivariate Data Analysis* (Seventh Edition ed.).

Hepler, Justin. (2015). A good thing isn't always a good thing: Dispositional attitudes predict non-normative judgments. *Personality and Individual Differences, 75*(0), 59-63. doi: http://dx.doi.org/10.1016/j.paid.2014.11.016

Hirschi, Travis. (1969). *Causes of delinquency*: University of California Press.

Ho, Robert. (2006). *Handbook of Univariate and Multivariate Data Analysis and Interpretation with SPSS*. Boca Raton: Taylor & Francis Group.

Ifinedo, Princely. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95. doi: http://dx.doi.org/10.1016/j.cose.2011.10.007

Ifinedo, Princely. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79. doi: http://dx.doi.org/10.1016/j.im.2013.10.001

Jahyun, Goo, Myung-Seong, Yim, & Kim, D. J. (2014). A Path to Successful Management of Employee Security Compliance: An Empirical Study of Information Security Climate. *Professional Communication, IEEE Transactions on, 57*(4), 286-308. doi: 10.1109/TPC.2014.2374011

Kim, Jongwoo, Park, Eun Hee, & Baskerville, Richard L. (2016). A model of emotion and computer abuse. *Information & Management*. doi: http://dx.doi.org/10.1016/j.im.2015.09.003

Krombholz, Katharina, Hobel, Heidelinde, Huber, Markus, & Weippl, Edgar. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113-122. doi: http://dx.doi.org/10.1016/j.jisa.2014.09.005

Lee, Sang M., Lee, Sang-Gun, & Yoo, Sangjin. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41*(6), 707-718. doi: http://dx.doi.org/10.1016/j.im.2003.08.008

Levan, Kristine, & Mackey, David A. (2015). Prevention of Crime and Delinquency. In J. D. Wright (Ed.), *International Encyclopedia of the Social & Behavioral Sciences (Second Edition)* (pp. 877-882). Oxford: Elsevier.

Li, Han, Zhang, Jie, & Sarathy, Rathindra. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*(4), 635-645. doi: http://dx.doi.org/10.1016/j.dss.2009.12.005

Magklaras, G. B., & Furnell, S. M. (2005). A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computers & Security, 24*(5), 371-380. doi: http://dx.doi.org/10.1016/j.cose.2004.10.003

Mesch, Gustavo S. (2009). Social bonds and Internet pornographic exposure among adolescents. *Journal of Adolescence, 32*(3), 601-618. doi: http://dx.doi.org/10.1016/j.adolescence.2008.06.004

Padayachee, K. (2013, 14-16 Aug. 2013). *A conceptual opportunity-based framework to mitigate the insider threat.* Paper presented at the Information Security for South Africa, 2013.

Padayachee, K. (2015). Aspectising honeytokens to contain the insider threat. *Information Security, IET, 9*(4), 240-247. doi: 10.1049/iet-ifs.2014.0063

Padayachee, Keshnee. (2012). Taxonomy of compliant information security behavior. *Computers & Security, 31*(5), 673-680. doi: http://dx.doi.org/10.1016/j.cose.2012.04.004

Pfleeger, Shari Lawrence, & Caputo, Deanna D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*(4), 597-611. doi: http://dx.doi.org/10.1016/j.cose.2011.12.010

Posey, Clay, Bennett, Rebecca J., & Roberts, Tom L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security, 30*(6–7), 486-497. doi: http://dx.doi.org/10.1016/j.cose.2011.05.002

Ryan, Richard M., Lynch, Martin F., Vansteenkiste, Maarten, & Deci, Edward L. (2010). Motivation and Autonomy in Counseling, Psychotherapy, and Behavior Change: A Look at Theory and Practice. *The Counseling Psychologist*. doi: 10.1177/0011000009359313

Safa, Nader Sohrabi, Ghani, Norjihan Abdul, & Ismail, Maizatul Akmar. (2014). An artificial neural network classification approach for improving accuracy of customer identification in e-Commerce. *Malaysian Journal of Computer Science, 27*(3), 171-185.

Safa, Nader Sohrabi, Sookhak, Mehdi, Von Solms, Rossouw, Furnell, Steven, Ghani, Norjihan Abdul, & Herawan, Tutut. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*(0), 65-78. doi: http://dx.doi.org/10.1016/j.cose.2015.05.012

Safa, Nader Sohrabi, & Von Solms, Rossouw. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442-451. doi: http://dx.doi.org/10.1016/j.chb.2015.12.037

Schumacker, Randall E., & Lomax, Richard G. (2010). *A Beginner's Guide to Structural Equation Modeling* (Third Edition ed.). New York: Taylor & Francis Group.

Silowash, George, Cappelli, Dawn, Moore, Andrew P., Trzeciak, Randall F., Shimeall, Timothy J., & Flynn, Lori. (2012). Common Sense Guide to Mitigating Insider Threats (4th Edition ed.).

Siponen, Mikko, Adam Mahmood, M., & Pahnila, Seppo. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224. doi: http://dx.doi.org/10.1016/j.im.2013.08.006

Siponen, Mikko, & Vance, Anthony. (2010). Neutralization: new insights into the problem of employee systems security policy violations. *MIS Quarterly, 34*(3), 487-502.

Sohrabi Safa, Nader, Von Solms, Rossouw, & Furnell, Steven. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82. doi: http://dx.doi.org/10.1016/j.cose.2015.10.006

Sun, Shaojing. (2008). An examination of disposition, motivation, and involvement in the new technology context computers in human behavior. *Computers in Human Behavior, 24*(6), 2723-2740. doi: http://dx.doi.org/10.1016/j.chb.2008.03.016

Turkanović, Muhamed, & Polančič, Gregor. (2013). On the security of certain e-communication types: Risks, user awareness and recommendations. *Journal of Information Security and Applications, 18*(4), 193-205. doi: https://doi.org/10.1016/j.jisa.2013.07.003

Verizon. (2016). Data Breach Investigations Report (DBIR 2016) (Vol. 1, pp. 1-70). United States: Verizon.

Willison, Robert. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization, 16*(4), 304-324. doi: http://dx.doi.org/10.1016/j.infoandorg.2006.08.001

Yusop, Zulkefli Mohd, & Abawajy, Jemal H. (2014). Analysis of Insiders Attack Mitigation Strategies. *Procedia - Social and Behavioral Sciences, 129*, 611-618. doi: http://dx.doi.org/10.1016/j.sbspro.2014.06.002