




A model to reduce insider cybersecurity threats in a South African telecommunications company

**Authors:**

Carol B. Silaule¹ 
Lean M. Makhubele¹ 
Stevens P. Mamorobela¹ 

Affiliations:

¹Department of Informatics,
Faculty of Information and
Communication Technology,
Tshwane University of
Technology, Pretoria,
South Africa

Corresponding author:

Carol Silaule,
csilaule@gmail.com

Dates:

Received: 10 May 2022
Accepted: 03 Aug. 2022
Published: 17 Oct. 2022

How to cite this article:

Silaule, C.B., Makhubele, L.M.
& Mamorobela, S.P., 2022, 'A
model to reduce insider
cybersecurity threats in a
South African
telecommunications
company', *South African
Journal of Information
Management* 24(1), a1573.
[https://doi.org/10.4102/
sajim.v24i1.1573](https://doi.org/10.4102/sajim.v24i1.1573)

Copyright:

© 2022. The Authors.
Licensee: AOSIS. This work
is licensed under the
Creative Commons
Attribution License.

Read online:

Scan this QR
code with your
smart phone or
mobile device
to read online.

Background: Cybersecurity breaches have become a growing challenge in today's digital economy. Organisations are faced with the responsibility of protecting their information resources from cybersecurity threats, and insider threats are one of them. Organisations have sophisticated technologies to protect themselves against these attacks, and their employees are often less guarded when it comes to protecting valuable company information systems.

Objectives: This research was aimed to develop and conceptualise a model to reduce cybersecurity insider threats in a South African telecommunication organisation.

Method: This study was conducted using a survey research approach, where close-ended questionnaires were utilised to collect data from respondents. The collected data was then analysed using IBM Statistical Package for Social Science (SPSS).

Results: The findings of the study indicated that personal norms in the domain of cybersecurity have a positive influence on individuals' attitude towards engaging in cybersecurity misbehaviour, and this has a significant relationship with their reduction of insider threats (RIT).

Conclusion: This study suggests that management should give close and thoughtful attention to factors that encourage their employees to engage in cybersecurity misbehaviour. As an efficient and effective approach to mitigate the risk of cybersecurity insider threats, identification and classification of these factors should be followed by proper planning with a goal of reducing their negative effect on employees' behaviour.

Keywords: cyberspace; cybersecurity; cyberthreats; insider threats; cybersecurity misbehaviour; information resources; telecommunications.

Introduction

Over the past 10 years, the internet and the broader concept of cyberspace has provided businesses with new opportunities for competitive advantage against their competitors and a direction for further economic growth (Sid 2017). These opportunities pose risks that arise because of the rapidly changing cyberthreat landscape and requires organisations to implement flexible and adoptable cybersecurity frameworks (Sid 2017). The emerging cybersecurity risks may arise from insider threats (Rodbert 2020). Insider threats can violate the organisation's security policy, either intentionally through malicious acts or through unintentional nonmalicious acts. Both actions can cause harm and significantly increase the probability of serious damage to the confidentiality, integrity or availability of the organisation's information systems or infrastructure and might result in compromising the security infrastructure of the organisation (Nurse et al. 2014).

Organisations are more focused on boosting the technology investment to protect themselves against external cyberattacks, and not enough emphasis is put on the insider threat aspects (Safa et al. 2019). Effective cybersecurity measures cannot be realised when the roles of users are not taken into consideration, as threats and attacks from employees may have a negative impact on the operation of the organisation's computer systems (Lamba et al. 2019). Furthermore, Clarke (2018) found that organisations are not putting enough effort towards reducing cybersecurity insider threats to improve their security posture and foster organisational culture change in security behaviour. Even though organisations consider cybersecurity insider threats as a risk to their business operations, there is a necessity to have a full view and interdisciplinary approach that considers the technological aspect of cybersecurity insider threats along with the human or insider element, which is difficult for organisations to detect, prevent or reduce. It is with this in mind that the study focused on the human or insider element by adopting the situational crime prevention (SCP) and social bond (SB) theories as a basis to develop a model to reduce cybersecurity

insider threats in a South African telecommunication company. The study addressed the following research questions:

1. What are the factors of SCP and social bond theories (SBT) that deter employees from engaging in cybersecurity insider threats?
2. What influence does employees' reduction of intention to misbehaviour (RIM) have on cybersecurity insider threat reduction?
3. Which factors of SCP and SBT best explain the reduction of insider threats (RIT)?

Figure 1 illustrates the research model of the study.

Literature review

Kemper (2017) defines cybersecurity as the 'preservation of the confidentiality, integrity and availability of information in cyberspace'. According to Von Solms and Van Niekerk (2018), cybersecurity deals with protecting digital assets such as hardware, network systems and processed information, which is stored by internetworked information systems in organisations, and it goes over and above the limitations of traditional information security to include the protection of the person who accesses the information on the cyberspace, as the person might be a potential target of cyberattacks or even unknowingly participating in cyberattacks.

Role of insiders in cybersecurity

Insider threats remain a significant problem within organisations, especially as industries' reliance on technology continues to grow (Dupuis 2016). Insiders pose a great threat to organisation security infrastructure because they have the knowledge on the organisation's security protocols and authorised access to the organisation resources (Al & Happa 2018). Insider threats can be posed either intentionally (malicious) or unintentionally (nonmalicious). An intentional or malicious insider is an employee with privileged access who intentionally seeks to perform a malicious act against the organisation which entrusted them with their valuable information assets, for example, revealing organisational secrets or deliberately causing sabotage to an organisation (Nurse et al. 2014). An unintentional or nonmalicious insider is described as an employee with access to an organisation's

network, system or data without any malicious intent associated with their action that causes harm or significantly increases the probability of serious damage to the organisation's information systems or infrastructure, for example, an employee misplacing their work device (Homoliak et al. 2017).

Situational crime prevention and social bond theories

Motivation and opportunity are key factors when exploring insider threats. Situational crime prevention theory explains how to decrease motivation and opportunity to reduce criminal activities or delinquent behaviour (Levan & Mackey 2015). The SCP theory therefore argues that motivation and opportunity may trigger an individual to commit a misconduct or delinquent behaviour (Padayachee 2016). The SCP theory focus is therefore different from that of other criminological theories because it seeks to reduce lawbreaking motivation and opportunities rather than punish or rehabilitate offenders. According to Clarke (2018), the SCP theory approaches crime reduction by making it impossible or difficult to commit the misconduct irrespective of the offender's motivation or intent, deterring the offender from committing the offence or by minimising stimuli that aggravate a person's motivation to commit a crime at any given time or event. Furthermore, a growing number of empirical studies and scientific evaluations have demonstrated that the SCP theory is an effective theory in reducing misconduct (Padayachee 2016).

On the other hand, the SBT states that everyone is capable of misbehaviour and that a 'bonding' or social bond to conventional society can prevent most people from getting involved in delinquency (Choi, Martins & Bernik 2018). According to Maalem et al. (2020), when an individual social bond is weak, the likelihood of that person to engage in criminal activities is increased. Furthermore, the SBT can be applied to establish the rationale of individuals engaging in criminal activities. The SBT is based on the premise that even when offenders are considering or leaning towards engaging in criminal activities, their strong social bonds can deter them away from committing the crime (Dupuis 2016). Furthermore, the author alluded that an insider may not engage in criminal activity for fear of losing social surroundings, reputation and involvement in conventional activities. However, if an insider has a weak belief system and maintains an antisocial background, the chances of an insider crime occurring increase exponentially.

Impact of insider threats to organisations

A survey conducted indicated that about 44% of all organisations experienced abuse of computer systems in 2008; 42% reported loss of laptops both in 2008 and 2009; and 17% reported theft of customer data (Richardson 2018). Homoliak et al. (2017) also conducted a survey which revealed that 25% of the respondents felt that 60% of the organisation financial losses was caused by insiders;

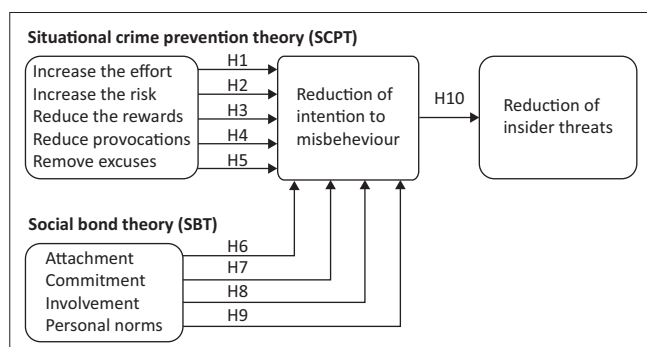


FIGURE 1: Research model on the reduction of cybersecurity insider threats.

unauthorised access or privileged access by insiders is 15%; and internet access and e-mail abuse by insiders are the fourth most widespread incident. Both the surveys indicate that insider threats are real and nearly rising to the level of an external threat (Homoliak et al. 2017).

Cyberthreats in the South African context

A study was conducted to analyse or review the findings of a research study which was undertaken with a goal of evaluating South Africa's cyberthreat landscape (Pieterse 2021). The study reviewed 74 cybersecurity incidents which were confirmed to have occurred between 2010 and 2020 in South Africa, affecting both government and private sectors. A few examples of organisations which were mentioned from the evaluating study include one of the government departments responsible for unemployment insurance payouts, where changes were implemented on their website to cater for temporary relief scheme during the coronavirus disease 2019 (COVID-19) pandemic; these changes unintentionally exposed confidential information of beneficiaries' employers. One of the private hospital service providers was a victim of a cyberattack in June 2020 whereby their admissions, business processing systems and e-mail servers were encrypted. Moreover, a data breach of great magnitude occurred in one of South Africa's credit bureau organisations, where one of their employers unintentionally exposed customers' personal information to a suspicious fraudster; this unfortunate incident is said to have affected 24 million South Africans and 800 000 business entities.

Research method and design

This study was conducted using a survey research approach. The targeted population for the study was professionals (project managers, software developers, business analysts, software test analysts, network specialists, IT architects, executive managers) within a division of a telecommunications company with legitimate access to computer systems, networks, data and information resources. A sample of 100 was randomly drawn using an Excel (Microsoft Corporation, Redmond, Washington, United States) random number generator from a population of 218. This probability sampling method based on simple random sampling techniques was recommended as all the members in the population had an equal opportunity of being selected (Taherdoost 2016). The Cohen statistical power analysis was utilised to determine the sample size of 100 (Drigo et al. 2020). However, only 95 out of the 100 targeted respondents returned fully completed questionnaires.

The participants were asked all the items associated with the variables on the proposed conceptual model. A secure web-based survey was used in this study as an instrument for gathering data to perform statistical analysis on the factors deterring employees from cybersecurity insider threats and ultimately their intention to reduce insider threats in an organisation. Data were collected using a 7-point Likert scale through a closed-ended questionnaire.

Analysis of data collected from the main survey questionnaire was evaluated through a two-stage approach, that is, the measurement model and structural model. The analysis was performed to ensure that there was no discrepancy in the collected data and to test and conduct an estimation of quantitative relationship that exists interdependently between independent variables (Durdyev, Ismail & Kandymov 2018).

Presentation of results

Demographic data

The results indicated that out of 95 respondents, 38.9% ($n = 37$) were male respondents and 61.1% ($n = 58$) were female respondents. Most of the participants were between 36 and 45 years at 56.8% ($n = 54$), followed by 26–35 years at 30.5% ($n = 29$). One respondent was above 55 years. Younger people (below 30 years) are more familiar with cybersecurity threats, while the older people are more cautious about cybersecurity issues (Fatokun et al. 2019). The study further showed a distribution of participants with various educational levels, including matric ($n = 2$), certificates ($n = 3$), diploma ($n = 17$), bachelor's degrees ($n = 30$), honours ($n = 19$), Master's ($n = 22$) and PhD ($n = 1$). Only one participant did not disclose his or her level of education. According to Bostan and Akaman (2017), highly educated people are aware of various technologies, and they become early adopters of new technologies. As noted by Bostan and Akman (2017), people with higher levels of education are more aware of cybersecurity issues. In relation to this study, it can be noted that most of the participants had higher levels of education, implying that they are highly aware of cybersecurity insider threats.

Correlation analysis of the constructs

According to Isaac and Chikweru (2018), before evaluating the relationship between the model and constructs, the two variables must be measured at the interval or ratio scale, ensuring that there is a linear relationship between the two variables, significant outliers do not exist and the data should be approximately normally distributed. For this study, these checks were conducted to ensure that Pearson correlation is the suitable statistic. To evaluate the constructs' relationships, the results were therefore analysed by using the bivariate Pearson correlation. The constructs' correlation was tested at 0.01 and 0.05 confidence level. Likewise, cases were also excluded from the analysis to allow only cases with no missing data to be analysed. Therefore, from the total population of 95, five cases were identified to have missing data; as a result, these cases were therefore eliminated from the analysis. Figure 2 shows the correlation analysis results.

The results in Figure 2 show a positive significant correlation among various model constructs. The results imply that there is a strong relationship among the model constructs. However, the results showed no relation between the involvement (IN) construct and the remove excuses (RE) construct. Most importantly, the results show a strong correlation significance between RIM and all the measuring constructs, that is,

| Correlations† | | | | | | | | | | | | |
|---------------|-------------------------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---|
| | IE | IR | RR | RP | RE | AT | CO | IN | PN | RIM | RIT | |
| IE | Pearson Correlation Sig. (2-tailed) | 1 | | | | | | | | | | |
| IR | Pearson Correlation Sig. (2-tailed) | * 0.605 0.000 | 1 | | | | | | | | | |
| RR | Pearson Correlation Sig. (2-tailed) | * 0.426 0.000 | * 0.526 0.000 | 1 | | | | | | | | |
| RP | Pearson Correlation Sig. (2-tailed) | * 0.336 0.001 | * 0.325 0.002 | * 0.410 0.000 | 1 | | | | | | | |
| RE | Pearson Correlation Sig. (2-tailed) | * 0.494 0.000 | * 0.480 0.000 | * 0.529 0.000 | * 0.475 0.000 | 1 | | | | | | |
| AT | Pearson Correlation Sig. (2-tailed) | * 0.425 0.000 | * 0.297 0.005 | * 0.444 0.000 | * 0.354 0.001 | * 0.578 0.000 | 1 | | | | | |
| CO | Pearson Correlation Sig. (2-tailed) | * 0.454 0.000 | * 0.426 0.000 | * 0.534 0.000 | * 0.279 0.008 | * 0.619 0.000 | * 0.792 0.000 | 1 | | | | |
| IN | Pearson Correlation Sig. (2-tailed) | * 0.377 0.000 | * 0.456 0.000 | * 0.411 0.000 | * 0.165 0.121 | * 0.495 0.000 | * 0.517 0.000 | * 0.699 0.000 | 1 | | | |
| PN | Pearson Correlation Sig. (2-tailed) | * 0.390 0.000 | * 0.334 0.001 | * 0.458 0.000 | * 0.271 0.010 | * 0.581 0.000 | * 0.784 0.000 | * 0.824 0.000 | * 0.563 0.000 | 1 | | |
| RIM | Pearson Correlation Sig. (2-tailed) | * 0.422 0.000 | * 0.382 0.000 | * 0.514 0.000 | * 0.356 0.001 | * 0.614 0.000 | * 0.777 0.000 | * 0.820 0.000 | * 0.550 0.000 | * 0.806 0.000 | 1 | |
| RIT | Pearson Correlation Sig. (2-tailed) | * 0.358 0.000 | * 0.375 0.000 | * 0.499 0.000 | * 0.280 0.008 | * 0.573 0.000 | * 0.758 0.000 | * 0.837 0.000 | * 0.589 0.000 | * 0.820 0.000 | * 0.855 0.000 | 1 |

IE, increase the effort; IR, increase the risk; RR, reduce the rewards; RP, reduce provocations; RE, remove excuses; AT, attachment; CO, commitment; IN, involvement; PN, personal norms; RIM, reduction of intention to misbehaviour; RIT, reduction of insider threats.

*. Correlation is significant at the 0.01 level (2-tailed).

†, Listwise $n = 90$

FIGURE 2: The correlation analysis results.

increase the effort (IE), increase the risk (IR), reduce the rewards (RR), reduce provocations (RP), RE, attachment (AT), commitment (CO), IN and personal norms (PN). A strong correlation significance was also noted between RIT and all the measuring constructs, including the RIT construct.

Measurement model

This study applied structural equation modelling (SEM) to validate or check the measurement model, and the correlations of the independent and dependent variables were also explored using SEM. The measurement model executes the relationship between the measured to the latent variables. The ovals represented the latent variables when drawing the measurement model in AMOS v. 26.0 (IBM Corporation, Armonk, New York, United States), that is, IE, IR, RR, RP, RE, AT, CO, IN, PN, RIM and RIT. The indicators or attributes for each construct are represented by the rectangles. Construct indicators were coded based on the abbreviation of each construct. Arbitrary names with a term 'e' and a numerical value were the error terms. Nonidentification of the model is one of the known common errors of SEM. However, this was minimised by assigning a fixed value of one to at least one

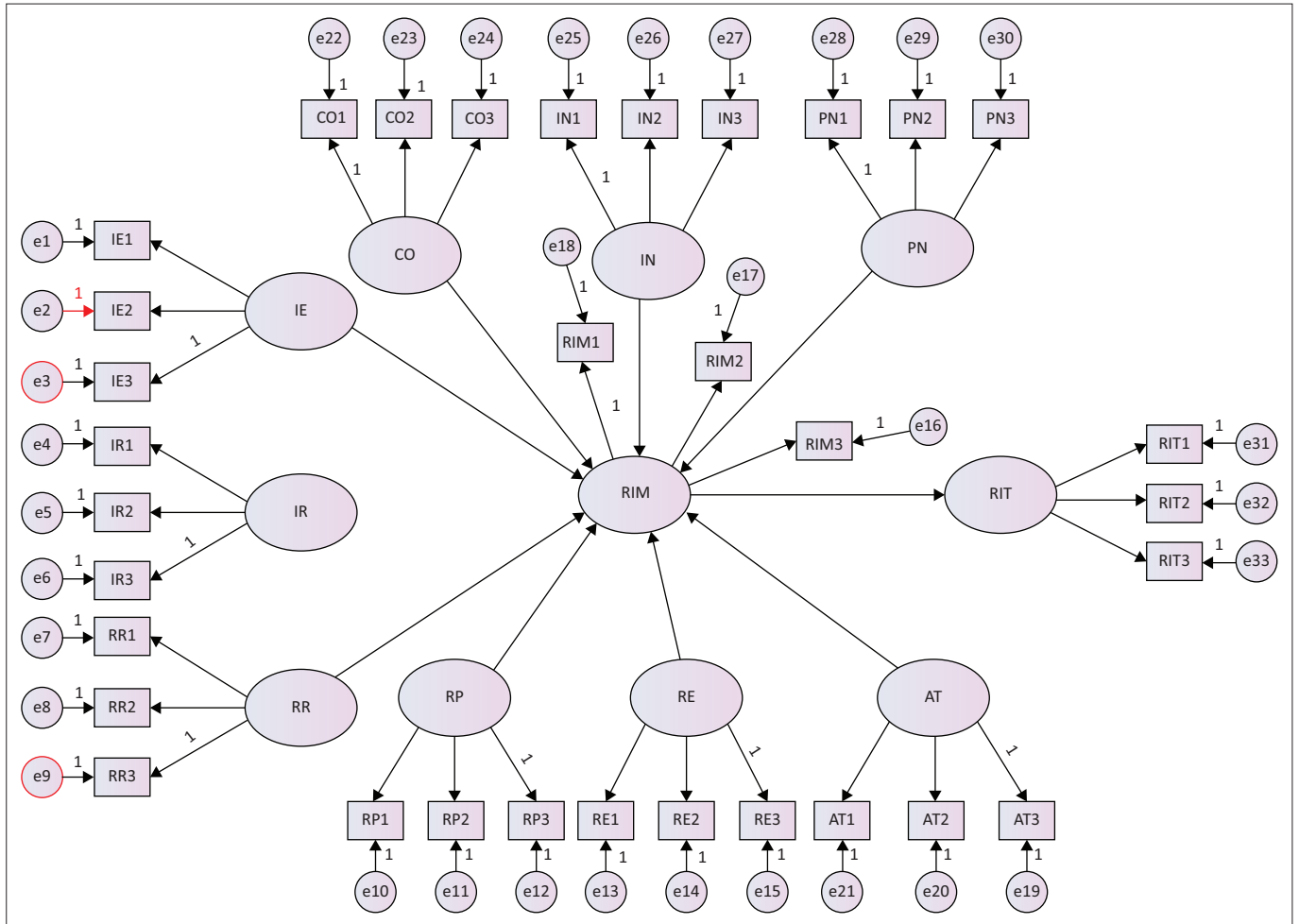
construct indicator. Figure 3 characterises the measurement model for this study.

Testing the structural model

The reliability and validity of this study's model was tested using SEM, as it has the capability of simultaneously testing the model and its validity (Drigo et al. 2020). Furthermore, SEM is a confirmatory factor analysis which can be applied to test and estimate the casual or fundamental relationships using both underlying qualitative assumptions and statistical data. Based on the analysis of the structural measurement model results, the new values obtained for all the model fit indices were within the acceptable threshold. Therefore, it can be concluded that the structural model is fit to measure the reduction of cybersecurity insider threats in South African telecommunication organisation. Based on the structural model results, this study's theoretical hypotheses were also evaluated.

Hypothesis testing

After the completion of the construct's validity and reliability tests, the reduction of constructs to their composite scores was performed in order to allow for the correlation and



IE, increase the effort; IR, increase the risk; RR, reduce the rewards; RP, reduce provocations; RE, remove excuses; AT, attachment; CO, commitment; IN, involvement; PN, personal norms; RIM, reduction of intention to misbehaviour; RIT, reduction of insider threats.

FIGURE 3: The measurement model.

regression analysis, which was crucial to test the strength of the relationship between the constructs, which are the dependent, independent, moderator and mediating variables. Bivariate correlation coefficient analysis was used to test the strength of the relationship that exists between constructs of this study. Table 1 illustrates the results of the hypothesis testing as extracted from the statistical data analysis. The table shows motivation and opportunities that influence employees’ attitudes towards reducing their intention to participate in cybersecurity misbehaviour.

The outcome of testing H1 to H8 shows that these hypotheses were proven to not have any significance towards the employees’ reduction of their intention to engage in misbehaviour. Therefore, H1 to H8 are not supported. On the contrary, the results show that H9 and H10 are supported. This implies that employees who hold personal values and beliefs that are against misbehaviour in an organisation are most likely to reduce their intention to engage in misbehaviour, consequently reducing cybersecurity insider threats.

Discussions

The research questions which grounded this study provided the framework for the discussion.

Key findings

In the context of this study, PN refer to individual positive or negative beliefs, values and views towards engaging in specific behaviour in the domain of cybersecurity (Padayachee 2016). According to Schoenherr and Thomson (2021), cybersecurity behaviours are determined by individual PN, and their personality traits are likely to be associated with behaviours that both prevent and promote cybersecurity insider threats. Despite a person’s natural feeling towards misbehaviour, their strong will to avoid misbehaviour deters them from committing criminal acts. On the contrary, the possibility of an employee being involved in cybersecurity insider threats increases when they have negative views towards complying with organisation cybersecurity policies (Bell, Rodgers & Pearce 2019). Furthermore, the authors alluded that individuals who possess commendable PN and values have an attitude which is of a good outcome concerning adhering to cybersecurity policies, consequently reducing insider threats in their respective organisations.

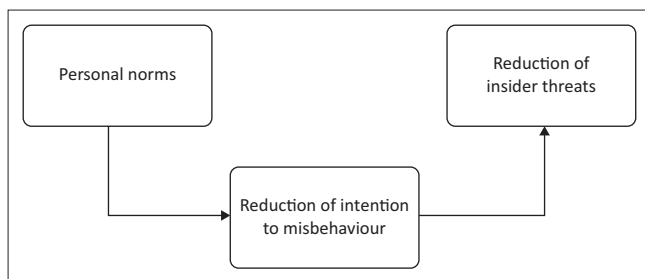
When employees in an organisation decide against the violation of cybersecurity policies, they are likely to comply or follow the prescribed policies and intend to reduce misbehaviour in the domain of cybersecurity, thereby

TABLE 1: Hypothesis test results.

| Hypotheses | Path | Hypothesis description | Estimate | <i>p</i> | Results |
|---|-------------|--|----------|----------|-----------|
| SCP theory: Attitudes that employees have towards reduction of intention to engage in cybersecurity violations may be influenced by: | | | | | |
| H1 | RIM <--- IE | Increasing the effort required to engage in cybersecurity misbehaviour | -0.065 | 0.48 | Rejected |
| H2 | RIM <---IR | Increasing the risk attached to engaging in cybersecurity misbehaviour. | 0.044 | 0.635 | Rejected |
| H3 | RIM <---RR | Reducing the rewards associated with engaging in cybersecurity misbehaviour. | 0.077 | 0.387 | Rejected |
| H4 | RIM <---RP | Reducing provocations for cybersecurity misbehaviour. | 0.013 | 0.805 | Rejected |
| H5 | RIM <---RE | Removing excuses for cybersecurity misbehaviour. | 0.045 | 0.628 | Rejected |
| SB theory: Factors that influence employees' attitudes towards reducing the intention to engage in cybersecurity violations: | | | | | |
| H6 | RIM <---RE | Attachment to an organisation | 0.241 | 0.369 | Rejected |
| H7 | RIM <---CO | Commitment to an organisation | -0.051 | 0.904 | Rejected |
| H8 | RIM <---IN | Involvement in cybersecurity | -0.009 | 0.935 | Rejected |
| H9 | RIM <---PN | Personal norms | 0.696 | 0.04 | Supported |
| Cybersecurity misbehaviour may be reduced by the: | | | | | |
| H10 | RIT <---RIM | low strength of an intent to participate in cybersecurity misbehaviour. | 0.942 | *** | Supported |

***, *p*-value of 0.05.

RIM, reduction of intention to misbehaviour; RE, remove excuses; IE, increase the effort; IR, increase the risk; RR, reduce the rewards; RP, reduce provocations; PN, personal norms; CO, commitment; IN, involvement; RIT, reduction of insider threats.

**FIGURE 4:** Model on the reduction of cybersecurity insider threats.

reducing insider threats (Chattopadhyay, Wang & Tan 2018). In this study, review of the literature revealed that PN affect individuals' attitudes towards engaging in organisational cybersecurity misbehaviour, and this has a significant relationship with their RIM (Rodbert 2020). According to the empirical evidence gathered in this study, PN were found to have a positive relationship with the reduction of intention to misbehave. This means that employees' PN influence their reduction of intention to misbehave, thus reducing insider threats in their organisation.

The findings of this study substantiate the main goal of this study, which was to develop and conceptualise a model to reduce cybersecurity insider threats in a South African telecommunication organisation. The model can be utilised as a mitigation strategy to reduce insider threats and attacks. From the suggested research model, the hypothesised relationships were tested. Some hypotheses were accepted, whereas others were rejected. From the accepted hypotheses, a new validated model was obtained; the model only shows those constructs where the hypothesised relationships were supported during the structural modelling. Figure 4 demonstrates the model developed from the findings of this study.

Strengths and limitations

Even though confirmation of the study's results is based on statistical instruments and methods that have been validated by previous research, the approaches will always have some

limitations around internal validity and generalisability (Saunders, Lewis & Thornhill 2019). This is because of statistical methods allowing for some measure of error, as well as the context in which the study was performed and how the research data was collected, which can cause problems with regard to validity and generalisability (Cohen 2019). Because of the nature of this study, it was expected that there could be some inherent bias with how individuals would answer the survey questionnaire, as it asks probing questions around the cybersecurity behaviours in cyberspace, which they might not be willing to share truthfully (Cohen 2019). Because of the challenges of the COVID-19 pandemic, it was difficult to physically collect data from participants in the organisation; therefore, the study only relied on electronic responses other than the physical questionnaire.

A cross-sectional survey was used in this study, thus justifying the collection of data only once. The single collection of data might be a missed opportunity to understand insider behaviour in the near future as far as cybersecurity is concerned and also the opportunity to predict or understand how the respondents are planning to reduce their intention to engage in cybersecurity misbehaviour in the long run.

Implications or recommendations

Even though the insider threats challenges are on the rise, there has been scant research explaining how organisations can determine whether their cybersecurity measures and insider threats mitigation strategies are suitable or best fit in their operational environment. Along with the technical solutions to insider threats challenges, future research should consider that exploring the motivation and opportunity to engage in insider threats could be more important to the context of insider threat reduction in the domain of cybersecurity than it is currently known and understood.

This study sampled its population from a telecommunication organisation; however, closely related to the augmentation of cybersecurity insider threats reduction measures, as well as the novelty of protecting valuable information resources in

South African telecommunications organisations, future researchers should consider increasing their sample population to cover the broader demographics of institutions other than the telecommunications industry, adopting other sampling and survey methods such as physical interviews which may help reach interested respondents who were thought of as previously unreachable. The adoption of a longitudinal timeline as well contextualising the privacy concept before participation should be considered by future researchers.

Lastly, this study can be further extended by exploring cybersecurity insider threats from different perspectives by exploring how organisational values, culture and employees' moral grounds discourage individuals from engaging in cybersecurity misbehaviour.

Conclusion

The study aimed at exploring and explaining the factors which deter employees from engaging in cybersecurity insider threats in a South African telecommunication company. The study examined factors of SCP and SB theories, which influence individual reduction of intentions to violate cybersecurity insider threats prevention policies and subsequently reduce insider threats in this context. On the basis of the empirical data derived from this study, a conceptual model has therefore been presented illustrating how to reduce insider threats in organisations.

A secure web survey was used to gather data from IT professionals who access company information resources, business applications, systems, networks and computing devices in the cyberspace. The survey was developed based on an extensive literature survey on cybersecurity insider threats. Situational crime prevention theory and SBT were used as theoretical lenses for this study. The analysis of the problem and context, the literature survey and the theoretical lenses informed the development of the research questions and research objectives and hypotheses. Based on the empirical evidence gathered in this study, the findings of the study confirmed some of the hypothesised relationships in the research model. Personal norms were found to have a positive influence on individual RIM, thus showing that individual norms and beliefs influence their RIM, which in turn reduces insider threats in their organisation.

Lastly, this study suggests that management should give close and thoughtful attention to factors that encourage their employees to engage in cybersecurity misbehaviour. As an efficient and effective approach to mitigate the risk of cybersecurity insider threats, identification and classification of these factors should be followed by proper planning with a goal of reducing their negative effect on employees' behaviour.

Acknowledgements

Dr L.M. Makhubele (DTech, Department of Informatics) was the research supervisor and Dr S.P. Mamorobela the cosupervisor (DTech, Department of Informatics). They

guided the researcher C.B. Silaule in designing the research questions, methodology, literature review, data collection, data analysis and discussion of findings.

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

Authors' contributions

C.B.S. was the research leader and involved in designing the research questions, methodology used, literature review, data collection, codification and analysis and writing of the manuscript. L.M.M. was the research supervisor and S.P.M. the cosupervisor. They guided the researcher C.B.S. in designing the research questions, methodology, literature review, data collection, data analysis and discussion of findings.

Ethical considerations

Ethical clearance to conduct this study was obtained from the Tshwane University of Technology Information and Communication Technology Faculty Committee for Research Ethics, before the survey was conducted (ref. no. FCRE/ICT/2020/09/005(1)). Ethical clearance was approved unconditionally on 27 October 2020. The ethical guidelines, as outlined in the approval protocol by the Ethics Committee, were followed throughout the data collection process.

Funding information

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability

No names will be provided in questionnaires and when reporting, the researcher will refer to participants as respondents. Feedback to participants will be given by providing a copy of the finished thesis to each section that was involved; moreover, another copy will be handed to the office of the Head of Department, which can be accessed by all employees within the Department. The copy of the thesis will also be made available electronically at Tshwane University of Technology library.

Disclaimer

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of any affiliated agency of the authors.

References

- Al, K. & Happa, J., 2018, 'Insider-threat detection using Gaussian', *Computers & Security* 77, 838–859. <https://doi.org/10.1016/j.cose.2018.03.006>
- Bell, C., Rogers, M. & Pearce, M., 2019, 'The insider threat : Behavioral indicators and factors influencing likelihood of intervention', *International Journal of Critical Infrastructure Protection* 24, 166–176. <https://doi.org/10.1016/j.ijcip.2018.12.001>

- Bostan, A. & Akman, I., 2017, 'Impact of education on security practices in ICT', *MIS Quarterly: Management Information Systems* 13, 319–339.
- Chattopadhyay, P., Wang, L. & Tan, Y.P., 2018, 'Scenario-based insider threat detection from cyber activities', *IEEE Transactions on Computational Social Systems* 5(3), 660–675. <https://doi.org/10.1109/TCSS.2018.2857473>
- Choi, S., Martins, T. & Bernik, I., 2018, 'Information security: Listening to the perspective of organisational insiders', *Journal of Information Science* 44(6), 752–767. <https://doi.org/10.1177/0165551517748288>
- Clarke, R.V., 2018, 'The theory and practice of situational crime prevention', *Crime Prevention Studies* 1(1), 1–19. <https://doi.org/10.1093/acrefore/9780190264079.013.327>
- Cohen, J., 2019, *Information systems IBM SPSS workbook*, vol. 1, pp. 11–14, School of Economic and Business Sciences, Hillsdale, NJ.
- Drigo, E., Rodriguez, J., Embirucu, M. & Fihlo, S., 2020, 'Analysis of operational communication through structural equation modeling', *IEEE Access* 8, 121705–121723. <https://doi.org/10.1109/ACCESS.2020.3006421>
- Dupuis, M., 2016, 'Curiosity killed the organization: A psychological comparison between malicious and non-malicious insiders and the insider threat', *Cybersecurity Crime Prevention Studies* 5, 35–40. <https://doi.org/10.1145/2978178.2978185>
- Durdyev, S., Ismail, S. & Kandymov, N., 2018, 'Structural equation model of the factors affecting construction labor productivity', *Journal of Construction Engineering and Management* 144(4), 18–21. [https://doi.org/10.1061/\(ASCE\)CO.1943-7862.0001452](https://doi.org/10.1061/(ASCE)CO.1943-7862.0001452)
- Fatokun, F., Hamid, S., Norman, A. & Fatakun, J., 2019, 'The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: An empirical investigation on Malaysian Universities', *Journal of Physics: Conference Series* 1339, 19–21. <https://doi.org/10.1088/1742-6596/1339/1/012098>
- Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y. & Ocha, M., 2017, 'Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures', *Journal for Applied Mathematics and Computer Science* 52(2), 1–40.
- Isaac, E. & Chikweru E., 2018, 'Test for significance of pearson's correlation coefficient (r)', *International Journal of Innovative Mathematics, Statistics & Energy Policies* 1, 11–23.
- Kemper, G., 2017, 'Improving employees' cyber security awareness', *Computer Fraud & Security Bulletin* 2017(8), 11–14.
- Lamba, A., Singh, S., Singh, B., Dutta, N. & Muni, R., 2019, 'Analyzing and fixing cyber security threats for supply chain management', *SSRN Electronic Journal* 4(5), 5678–5681.
- Levan, K. & Mackey, A., 2015, 'Prevention of crime and delinquency', *International Encyclopedia of the Social & Behavioral Sciences* 18, 877–882. <https://doi.org/10.1016/B978-0-08-097086-8.45012-9>
- Maalem, A., Caulkins, B., Mohapatra, R. & Kumar, M., 2020, 'Review and insight on the behavioral aspects of cybersecurity', *Journal of Cybersecurity* 3, 1–18. <https://doi.org/10.1186/s42400-020-00050-w>
- Nurse, J., Buckley, O., Legg, P., Goldsmith, M., Creese, S., Wright, G. et al., 2014, 'Understanding insider threat: A framework for characterising attacks', *IEEE Security and Privacy Workshops* 10, 224–228. <https://doi.org/10.1109/SPW.2014.38>
- Padayachee, K., 2016, 'An assessment of opportunity-reducing techniques in information security: An insider threat perspective', *Decision Support Systems* 92, 47–56. <https://doi.org/10.1016/j.dss.2016.09.012>
- Pieterse, H., 2021, 'The cyber threat landscape in South Africa: A 10-year review', *The African Journal of Information and Communication* 28, 1–21. <https://doi.org/10.23962/10539/32213>
- Richardson, R., 2018, *CSI computer crime and security survey*, vol. 1, pp. 1–30, Computer Security Institute, San Francisco.
- Rodbert, M., 2020, 'Why organisational readiness is vital in the fight against insider threats', *Network Security* 2020(8), 7–9. [https://doi.org/10.1016/S1353-4858\(20\)30092-1](https://doi.org/10.1016/S1353-4858(20)30092-1)
- Safa, N., Maple, C., Watson, T. & Von Solms, R., 2019, 'Motivation and opportunity based model to reduce information security insider threats in organisations', *Total SS Private Sector* 12, 1–61.
- Saunders, M., Lewis, P. & Thornhill, A., 2019, *Research methods for business students*, 5th edn., vol. 5, pp. 14–134, Pearson Education Limited, Cape Town.
- Schoenherr, J.R. & Thomson, R., 2021, 'The cybersecurity (CSEC) questionnaire: Individual differences in unintentional insider threat behaviours', *Journal of Information Security and Applications* 4, 8–28. <https://doi.org/10.1109/CyberSA52016.2021.9478213>
- Sid, L., 2017, 'A novel model for cybersecurity economics and analysis', *17th IEEE International Conference on Computer and Information Technology*, Helsinki, Finland, Aug 22–23, 2017, vol. 17, pp. 274–279.
- Taherdoost, H., 2016, 'Sampling methods in research methodology; How to choose a sampling technique for research', *International Journal of Academic Research in Management (IJARM)* 5(2), 18–27.
- Von Solms, R. & Van Niekerk, J., 2018, 'From information security to cyber security', *Computers and Security* 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>