Behaviour of Outsourced Employees as Sources of Information System Security Threats

Abstract

There is an increased need for information systems to be protected against unauthorized access and retrieval, particularly from legitimate 'insider' outsourced employees. While most studies have focused on organisations' employees as threats, only a few have focused on the role the outsourced employees' play as a potential threat. The study seeks to investigate the insider threat behaviour of an outsourced employee in developing countries as security threats to information systems by virtue of their privileged access. The study is quantitative and adopts social bond and involvement theories for this purpose. The research sample was chosen from organisations in Nigeria and South Africa which are the largest two national economies in Africa. Close-ended questionnaires were used and the data were analysed using factor analysis. The study found that outsourced employees exploit information systems vulnerabilities because they are not actively involved in the organisation and lack moral values and beliefs. The findings of this study will assist organisations in developing countries to mitigate the information security threats posed by outsourced employees.

Key Words: Digital Data, Insider threat, Outsourced employee

David Oyebisi and Kennedy Njenga, Behaviour of Outsourced Employees as Sources of Information System Security Threats: Proceedings of AsiaUSEC'20, Financial Cryptography and Data Security 2020 (FC). February 14, 2020 Kota Kinabalu, Sabah, Malaysia Springer, 2020.

1. Background

The advent of the internet and recent developments in electronic and mobile commerce have seen the increase of digital assets and digital data which can be shared among millions of users once it is created. Laws and regulations to protect organisations' digital assets are not uniformly defined, protected and regulated across boundaries. Considerable measures have been taken to prevent data breaches but most efforts have proven to be unsuccessful. A often under-appreciated vulnerability is when a trusted permanent and outsourced employee that have legitimate access to sensitive information of their organisation perpetrate cybercrime. Although malicious attacks can be initiated by both insiders and outsiders, disguised former or malicious employees can be potentially disastrous since they can use the knowledge and skills acquired legitimately during work process for illicit gain (Schaefer, Brown, Graessle, & Salzsieder, 2017).

Many organisations have taken measures to instil good cybersecurity protection, ideas, and perception into their employees. Despite all these measures, Aldawood and Skinner (2019) findings have shown that with state-of-the-art cybersecurity awareness and policies, a malicious employee can still steal sensitive information from their organisation. They suggest the need to profile at-risk employees and newly hired staff and tailored an adequate cybersecurity training program for them. However, newly employed workers may not necessarily be a malicious attacker.

Australia's largest bank (Commonwealth Bank of Australia) recently recorded a glitch in the banking app that was recently launched. The banking app erroneously activated multiple payments due to an error screen (Bajkowski, 2019). This error may have been averted if an effective penetration test has been conducted before the banking app is launched. Many Australian organisations are witnessing a decline in outsourcing penetration testing with contractual clauses where only Australian citizens are eligible employees to work on many projects. There is this untested assumption that there are more risks involved with outsourcing cybersecurity.

Researchers in the area of cybercrime and behaviour have traditionally emphasised permanent employees within the corporate structure as insider threats. Insider threat research has downplayed or ignored the role of outsourced employees. Since there is no national law and regulatory framework that specifically regulate outsourcing, there has been a considerable increase in outsourcing due to low operating costs abroad, and the abundance of highly skilled offshore workers (Borgese and Pascoe, 2019; Wallbank, 2019). Such an increase in outsourcing necessitates the importance of examining the cybercrime threats and risks posed by outsourced employees. This study seeks to fill the gap by focusing on the outsourced employees of organisations as a potential cybersecurity threat and their motive behind cybercrime.

2. Research Objective

The goal of this study is to explain the extent to which an outsourced employee could be a potential information security threat and how an organisation can discourage insider threats. To achieve this goal, the following objective is formulated:

To examine the major reasons why outsourced employees exploit the vulnerability of an organisation's secured information system.

3. Literature Review

A significant level of access and trust are given to an employee to work effectively in the organisation (Bamforth, 2015). The privileged access that enables an employee to perform their legitimate functions also allows them to abuse the system which makes it necessary to find a middle ground where adequate privileges are granted while malevolent usage is mitigated (Dini & Lopriore, 2015; Kim, Park, & Baskerville, 2016). Analysing such middle ground may reduce insider abuse (Kim et al., 2016). All organisations should endeavour to track all their employee's access to confidential information, ensuring that adequate mechanisms are available to detect and prevent any unauthorized access to sensitive data and information. Even with adequate technology to monitor employees' access to computer systems, intruding into the privacy of employees through electronic monitoring technology is a growing concern (Eivazi, 2011).

Research has shown that it is very difficult to determine and predict the motives behind insider attacks although it is believed that employees often do so to perpetrate fraud and for financial gain or revenge (Breeden, 2017). And insider threat attacks may also be motivated by overzealousness on the part of employees to get the job done, because of stress, espionage and some exacerbated factors outside the work environment such as family issues (Roy Sarkar, 2010). Malice is often associated with acts of revenge while espionage may result from a request from competitors. Once an insider has been motivated by one or more of the above-mentioned factors, s/he will scan for any vulnerability in the organisation's system to exploit but then it can also be the case that such attacks are actually made possible by the vulnerability of organisation's system such as poor access control policies (Huang, Liu, Fang, and Zuo, 2016).

To profile insider threat attacks, Baracaldo and Joshi (2013) have suggested a framework that expands the role based access control (RBAC) model by integrating risk evaluation processes, and the trust that an information system has for its users. The framework helps to adapt doubtful changes in insiders' behaviour by deleting privileges when the trust of insiders' falls below predefined levels. In this way, insider threat attacks could be avoided if access control systems can automatically generate exemptions in real-time when a user is embarking on actions that are inappropriate for their roles and responsibilities.

Babu and Bhanu (2015) also suggest that insider threats may be reduced by proper management of privileges in the information system environment. They propose a privilege management mechanism that integrates risk and trust to develop an efficient prevention mechanism against any forms of insider threats. Their approach successfully identified the malicious behaviour of insiders and any unauthorized requests by splitting user behaviours based on keystroke contents. However, none of the models is yet to identify potential insider attackers in advance. To identify the likelihood of insider attacks and to avert any possible internal threats, Roy Sarkar (2010) recommends a three-pronged approach where technological behavioural and organisational assessments are taken into consideration.

Employees' attitude towards insider threats is influenced by their cultures and belief systems. According to Liu (2014), when individuals move from one location to another, their cultural beliefs and values move with them while their institutional and external economic is abandoned. The culture and value they portray will also influence people around them. The workplace is not an

exemption. Employees cultural beliefs and values also influence their attitudes and behaviours concerning information security. An organisation can cultivate an information security culture through effective policies that will enhance employees' information security awareness (Von Solms & Von Solms, 2004; AlHogail, 2015; Dhillon, Syed, & Pedron, 2016).

4. Theoretical Framework

This study adopts social bond theory and involvement theory on the relationship between two entities to explore the insider threat behaviour of an outsourced employee. According to Hirschi's (1969) social bonding opinion an individual is less likely to commit delinquent acts when such an individual has a considerable level of social bonding in a particular society. The theory describes a unbreakable link that exists between individuals within a group and is suitable to understand a social problem that exists among entities. In corporate settings, employees with a greater level of social bonding with his/her organisation are less likely to commit a malicious act (Thompson, 2014). Hirschi (1969) categorised social bond into four components – attachment, commitment, involvement and personal norms.

Involvement theory identifies the degree of contribution in terms of energy and time given to a specific activity (Lee, Lee, & Yoo, 2004). In other words, the degree of time and energy sacrificed for any task determines the level of commitment and involvement of the individual. As in the case of information security awareness program, Rocha Flores, Antonsen, and Ekstedt (2014) claim that lack of information security awareness and knowledge can be attributed to low levels of employee's involvement. There is no doubt that involvement influences the attitudes and behaviour of employees.

4.1 Conceptual model

Figure 1 represents the conceptual model adopted in this study. Involvement is the antecedent variable while social bond and insider threat behaviours are the independent variable and dependent variable respectively.

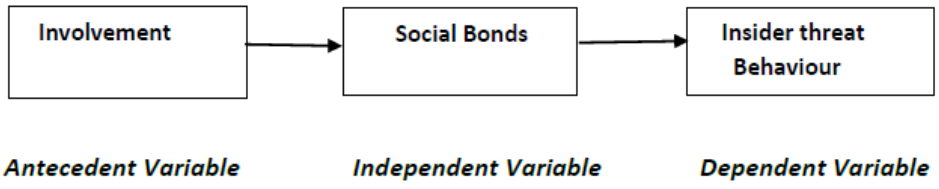

Fig 1: General Conceptual Model

Involvement (perception) of employees has a direct impact on their social bonds to the organisation. Attachment, commitment, involvement, and belief as collective components of the social bond, in turn, shape the insider threat behaviour of employees. The interdependence of these research constructs is illustrated in the model below.

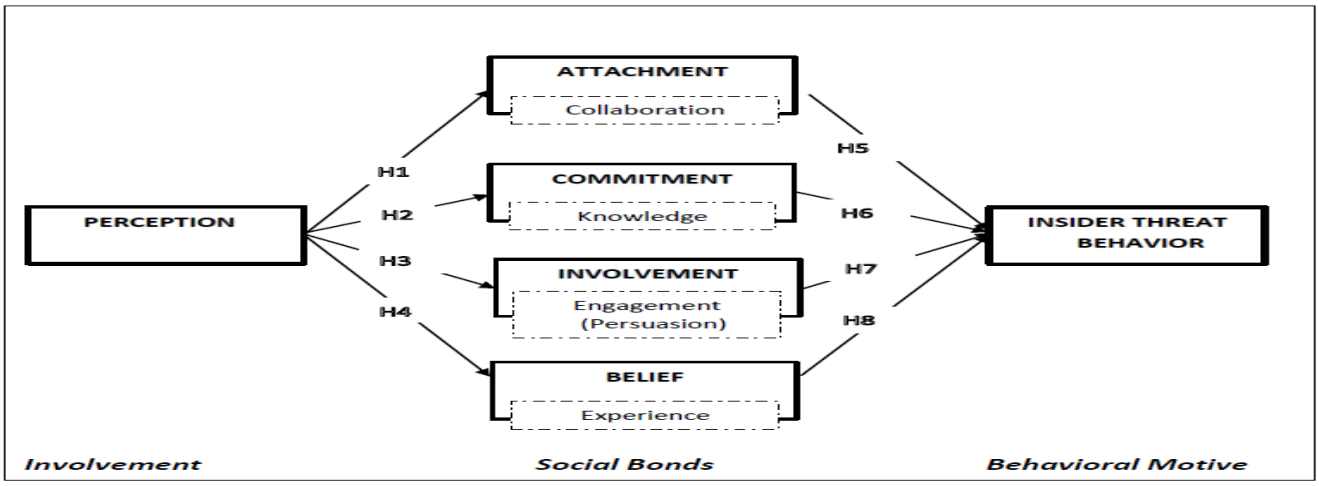

Figure 3.3: Research model

4.2 Hypotheses

Research has shown that collaboration and teamwork in the workplace have a positive impact on the productivity of an organisation (Flores-Fillol, Iranzo, & Mane, 2017). According to Hamilton, Coates, and Heffernan (2003) collaboration and teamwork result in between 6 and 18 per cent higher productivity. Not only will collaboration and teamwork ensure effective communication between employees management, but they also improve the attachment of employees to the organisation (Velez & Neves, 2017). Based on the above claims the following hypothesis is proposed:

H1: There is a positive relationship between employees' perception and attachment

Employees' commitment can be understood as psychological attachment to the organisation and it is crucial in determining whether an employee will remain with the organisation for a foreseeable future and at the same time work with other employees to achieve the organization's goals (Devece, Palacios-Marqués, & Pilar Alguacil, 2016; Wombacher & Felfe, 2017). Based on the perceived commitment of the employee to the organisation, the following hypothesis is proposed:

H2: There is a positive relationship between employees' perception and commitment

Employees' involvement is the opportunity given to employees to participate in the decisions that affect their organisation. This may be based on employees' task discretion and/or organizational participation (Markey & Townsend, 2013). It enhances productivity and job satisfaction, encourages employees to provide private information to further the interest of their organisation, generates trust and a sense of control among the employees, and minimizes the resources required to monitor and implement policy compliance among employees. Based on these benefits, the following hypothesis is proposed:

H3: There is a positive relationship between employees' perception and involvement

Many factors shape an employee perception of belief. According to Javanmard (2013), religiosity is associated with unconcealed behaviours that employees may exercise and it is formally linked to institutions such as churches and temples. It is important also to note that employee beliefs and value systems are reflections of their different cultures (Buchtel, 2014). Based on the above, the following hypothesis is proposed:

H4: There is a positive relationship between employees' perception and Belief

The attachment of employees to their organisations result in loyalty and loyal employees do their best to safeguard the interests of the organisation ((Esmaeilpour, & Ranjbar, 2017). Given that employee that is attached to her supervisor, job, and organisation is less likely to display inside threat behaviours, the following hypothesis is proposed:

H5: There is a negative relationship between employees' level of attachment and insider threat behaviour

Committed employees are most likely to dedicate their energy and time to their career development and advancement and are unlikely to break rules and regulations that will ridicule and jeopardize their status. Therefore, employees that are more committed to their organisation are unlikely to commit insider threat attacks. Based on this, the following hypothesis is proposed:

H6: There is a negative relationship between employees' level of commitment and the insider threat behaviour

According to Hirschi (1969), an engaged employee that spent considerable energy and time in conventional activities will be occupied and have fewer times to spend on deviant acts. Thus, an individual that is actively involved in the organisation is less likely to commit insider threat attack. Therefore:

H7: There is a negative relationship between employees' level of involvement and the insider threat behaviour

Employees' beliefs, values and norms shape the way they perceive organisational issues and have a direct influence on their behaviour in the organisation including how they will comply with information security policies (Van der Werff & Science Steg, 2016). According to Lee et al. (2004), employees with reasonable personal norms tend to conform to organisational information security behaviour. Therefore, the following hypothesis is proposed:

H8: There is a negative relationship between employees' level of belief and the insider threat behaviour

5. Research Methodology

Quantitative research method was identified as a suitable approach to collect data and to test hypotheses. A structured questionnaire was used and was considered as the ideal instrument that enabled a large amount of data to be collected from respondents' within a short period (Saris and Gallhofer, 2014). Respondents were identified from the corporate sector through judgmental, non-probability sampling technique. Only outsourced employees were considered. This technique

provides a reliable representative sample that presents an accurate result. This study follows Daniel's (2012) steps in selecting a sample. Firstly, a target population was identified. Secondly, the inclusion and exclusion criteria were used to select the sample. Thirdly, a plan was created to recruit and select the population elements. Fourthly, sample size was determined. Based on the recommendations of Daniel, (2012), this study adopts a fixed approach where 155 questionnaires were administered. The questionnaire was designed to have an introduction section where respondents were made to understand the purpose and benefits of the study. The approximate time of completion, ethical and privacy issues were also addressed in this section. The questionnaire consists of two major parts. The first part represented the biological information of respondents while the other part consisted of the main questions.

5.1 Data collection

Data was collected from identified outsourced employees mostly in the field of banking, e-commerce, audit, and insurance. An appointment was booked with those employees that are interested to partake in the survey. To minimise the numbers of incomplete questionnaires, responses from each participant were reviewed as soon as a questionnaire is completed. Respondents were asked to respond to any omitted questions.

5.2 Demography

Demographic information of respondents as shown by Table 1 and shows that male participants account for 53% while female participants account for 47%. Over half the respondents were aged between 30 to 39 years with most having a bachelor or masters degree. A majority has less than 3 years' work experience. This suggested that their level of commitment was not strongly nurtured.

Table 1: Participants' Demography

Participants' demography			
Measure	**Items**	**Frequency**	**Percent**
Gender Distribution	Male	79	53 %
	Female	71	47 %
Age Distribution	Younger than 20	1	1 %
	20-29	45	30 %
	30-39	78	52 %
	40-49	23	15 %
	50 and older	1	1 %
Highest Qualification level	Grade 12/O level or lower	10	7%
	Diploma or Certificate	24	16 %
	Bachelor Degree(s)	72	48 %
	Master's degree	42	28 %
	Doctorate degree	2	1 %

IT Certification	Yes	74	49 %
	No	76	51 %
Years of IT Experience	Less than 1 year	45	31 %
	1-2 years	23	16 %
	2-5 years	21	14 %
	5-10 years	38	26 %
	10-15 years	9	6 %
	More than 15 years	9	6 %

5.3 Analysis

Exploratory Factor analysis helps reduce measurable variables to a smaller latent variable that has a common variance (Pallant, 2016). Exploratory factor analysis was used to determine the relationship between the subset of the study variables. Tabachnick and Fidell (2014) suggest a minimum sample size of 150 cases provided that the dataset has a high factor loading score above .08. A reverse scoring was checked collectively for all questions (items) to ensure that similar questions were asked. All components in the Component Matrix table (table excluded) were positive. In addition to correlation matric, Bartlett's test of Sphericity and Kaisers-Meyer- Olkin (KMO) also confirm the factorability of a dataset. The results have shown a Significant of ($p < .05$) for Bartlett's test of Sphericity and KMO index of .6 for all items.

The internal consistency indicator adopted in this study was the Cronbach alpha coefficient. The decision to use the Cronbach alpha coefficient was because it is suitable for multiple Likert scale questions (questionnaire) which were the research instrument favoured in this study (Pallant, 2016). The researcher also ensures that Cronbach alpha coefficients is used to measure each construct. Pallant (2016) recommends a Cronbach alpha coefficient of .7 and above for a reliable scale. Cronbach alpha coefficients were calculated and reported for each construct separately. The Cronbach's Alpha values of .7 and above for each construct in this study suggest a good internal consistency of all the items that constitute the research instrument (questionnaire). Table 2 depicts the Cronbach Alpha coefficient of the study constructs.

Table 2: Reliability Test

Reliability Test		
Construct	**Number of Items**	**Cronbach's alpha**
Perception of Organisation (POO)	5	.835
Attachment to Organisation (ATO)	5	.791
Commitment to Organisation (CTO)	5	.673
Involvement In Organisation (IIO)	5	.809
Belief (B)	5	.714

Insider Threat Behaviour (ITB)	10	.822

6. Testing the Model

Standard multiple regression was used to test the research hypotheses. The Correlation between outsourced employees' perception and outsourced employees' attachment, commitment, involvement, and belief were accessed. In the same vein, the correlation between insider threat behaviour and outsourced employees' attachment, commitment, involvement, and belief were assessed simultaneously using Pearson Correlation. All the p-values are less than .05 and suggest a correlation among the variables. Employees' attachment, employees' commitment, employees' involvement, and belief are jointly significant and explained.

50.3% of the variance in the employees' attachment is explained by employees' perception. Employees' perception was statistically significant to predict employees' attachment (beta = 709, Sig Value < 0.5). Therefore, the higher the perception of an employee, the higher the attachment to the organisation and vice versa. Therefore, hypothesis 1 is accepted. The contribution of Employees' perception to the prediction of Employees' commitment was also assessed. The beta coefficient of .453 and a sig value (less than .05) indicate that employees' perception makes a significant contribution to the prediction of employees' commitment. Based on the regression analysis test result for hypothesis 2, a positive perception of employees will result in reasonable commitment to the organisation. Therefore, hypothesis 2 is accepted.

The beta coefficient (.409) and the sig value (<.05) indicates that the employees' perception makes a significant contribution to the prediction of employees' involvement. The regression analysis for hypothesis 3 confirms a positive relationship between employees' perception and employees' involvement. Employees' are more involved in the organisation when their perception of the organisation is positive. Therefore, hypothesis 3 is accepted. The Pearson coefficient of .177 explains the weak correlation between employees' perception and employees' belief. Additionally, the r-square value (.031) indicates that 3% of the variance in the employees' belief is explained by the employees' perception while the p-value (sig. = .031). Henceforth hypothesis 4 is rejected. A positive or negative perception of employees' does not have any significant influence on their belief.

The contribution of attachment, commitment, involvement, and belief, individually to the prediction of insider threat behaviour suggests that belief makes the strongest contribution with a beta coefficient of .405. This was followed by employees' involvement with a beta coefficient of .182. However, employees' attachment and employees' commitment seemed to contribute insignificantly to explaining the threat behaviour with a Beta Coefficients of .136 and -.087 respectively. The significant value of belief and employees' involvement are less than .05 while the significant value of employees' attachment and commitment are greater than .05. Figure 2 below illustrates the result of the hypotheses test.

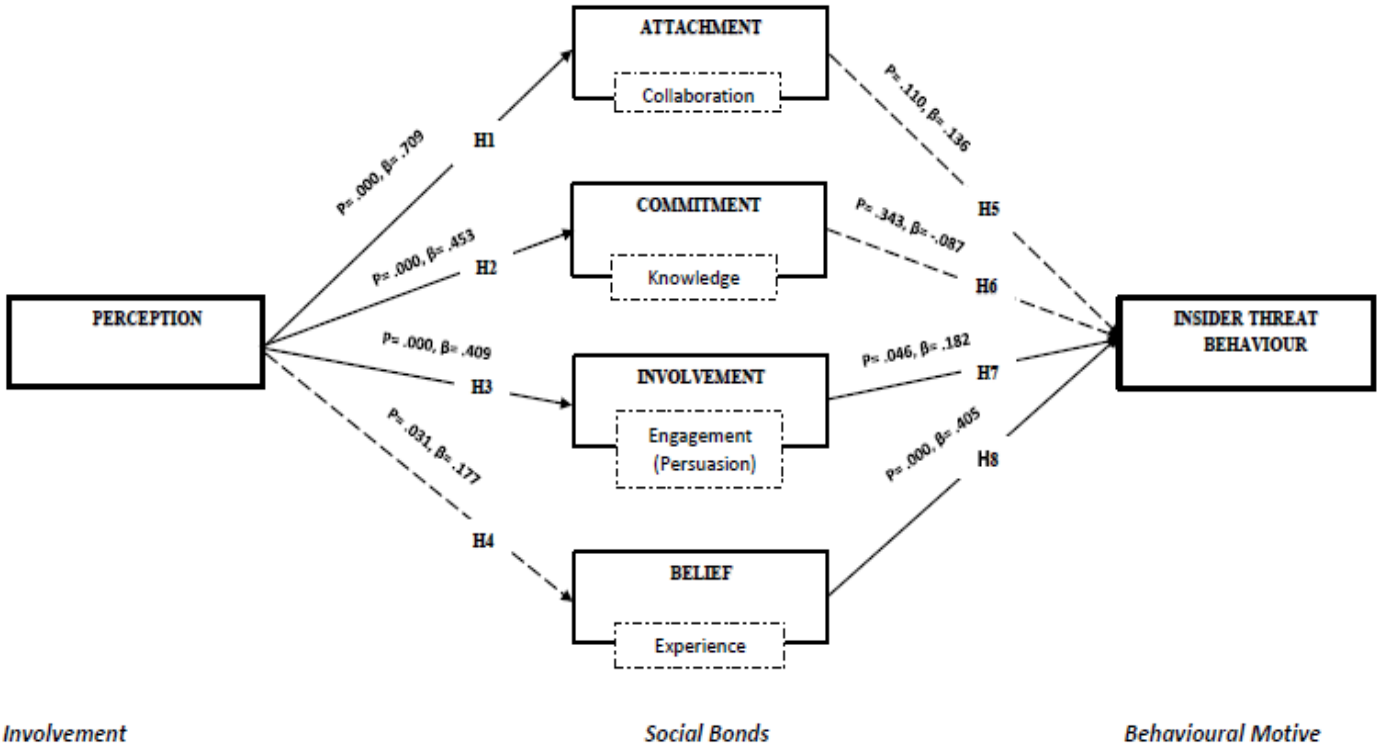

Fig 2: Revisited Model Based on Correlation and Regression Test and Hypothesis

If we have to make a prediction of threat behaviour and take into account employees' attachment, employees' commitment, employees' involvement and belief, employees' attachment and commitment are insignificant because they contribute little to the model. The most important factors of predicting threat behaviour are the level of employees' involvement in the organisation and their belief. Hypotheses 7 and 8 are accepted and hypotheses 5 and 6 are therefore rejected.

7. Contribution and Implication

The study findings show that the most important factors predicting threat behaviour would include employees, involvement in the organization are and their belief. This is important since involvement and belief as to be seen as a management and leadership philosophy and not necessarily a goal. Without enabling people, chances are that they will act contrary to the desired success of the organisation. Indeed some could act contrary to policy and to be deviant. In the discipline of Information Systems, this is crucial due to the need to protect these systems from threats of deviant acts. Organisations should try to engage outsourced employees by giving a sense of ownership and commitment for them to be positive co-contributors to organizational success.

8. Conclusion

This study considered the potential threat that an outsourced employee could be to an organisation. The study focused on deviant behaviour as a potential source of this threat. Involvement theory and four elements of Social Bond Theory were examined. I demonstrate how the perception of

employee shaped their attachment, commitment, involvement and belief to their organization. I further used these four elements to explain the bonds the employees would have with the organisation. I explained that the predisposition to be deviant will be determined by how strong these elements are present and how they shape the ties an outsourced employee has to an organisation. A theoretical model was developed to test this and the quantitative research methodology adopted. The work presents useful insights as to the outsourced employees' involvement and belief being strong determinants to predict deviance and therefore risk to information systems. I believe the work carried out would be useful in helping management foster an environment whereby properly motivated, involved, committed employees are they insourced or outsourced will help contribute to organisational goals.

9. Declaration of Replication Studies

The author declares that part of this paper has previously been published in a conference proceeding.

10. Acknowledgements

The author thanks Professor Alana Maurushat who provided valuable feedback during the preparation of this paper. Professor Alana Maurushat is Professor of Cybersecurity and Behaviour at Western Sydney University.

References

Aldawood, H. & Skinner, G. (2019). "Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues.", Future Internet, vol. 11, no. 3, pp. 73-73.

AlHogail, A. (2015). "Design and validation of information security culture framework". Computers in Human Behaviour, vol. 49, pp. 567-575.

Babu, B.M. & Bhanu, M.S. (2015). "Prevention of Insider Attacks by Integrating Behaviour Analysis with Risk based Access Control Model to Protect Cloud", Procedia Computer Science, vol. 54, pp. 157-166.

Bamforth, R. (2015). "How to free your business and staff with self-service", Computer Weekly, pp. 16-19.

Bajkowski, J. (2019). CBA Netbank app error causes mistaken multiple payments. [online] iTnews. Available at: https://www.itnews.com.au/news/cba-netbank-app-error-causes-mistaken-multiple-payments-530665 [Accessed 6 Sep. 2019].

Baracaldo, N. & Joshi, J. (2013). "An adaptive risk management and access control framework to mitigate insider threats", Computers & Security, vol. 39, no. Part B, pp. 237-254.

Borgese, A. and Pascoe, N. (2019). Outsourcing 2019 | Laws and Regulations | Australia | ICLG. [online] International Comparative Legal Guides International Business Reports. Available at:

https://iclg.com/practice-areas/outsourcing-laws-and-regulations/australia [Accessed 1 Sep. 2019].

Breeden, J. (2017). “Are Careless Insiders the Biggest Federal Cyber Threat?”, NextGov.com (USA).

Buchtel, E.E. (2014). “Cultural sensitivity or cultural stereotyping? Positive and negative effects of a cultural psychology class“, International Journal of Intercultural Relations, vol. 39, pp. 40-52.

Daniel, J. (2012). Sampling essentials: practical guidelines for making sampling choices, Sage, Los Angeles.

Devece, C., Palacios-Marqués, D. & Pilar Alguacil, M. (2016). "Organizational commitment and its effects on organizational citizenship behavior in a high-unemployment environment", Journal of Business Research, vol. 69, no. 5, pp. 1857-1861.

Dhillon, G., Syed, R. & Pedron, C. (2016). “Interpreting information security culture: An organizational transformation case study“, Computers & Security, vol. 56, pp. 63-69.

Dini, G. & Lopriore, L. (2015). “Password systems: Design and implementation“, Computers & Electrical Engineering, vol. 47, pp. 318-326.

Eivazi, K. (2011). “Computer use monitoring and privacy at work“, Computer Law & Security Review, vol. 27, no. 5, pp. 516-523.

Esmaeilpour, M. & Ranjbar, M. (2017). “Investigating the impact of commitment, satisfaction, and loyalty of employees on providing high-quality service to customer“, Romanian Economic and Business Review, vol. 12, no. 1, pp. 82-98.

Flores-Fillol, R., Iranzo, S. & Mane, F. (2017). “Teamwork and delegation of decisions within the firm“, International Journal of Industrial Organization, vol. 52, pp. 1-29.

Hamilton, C., Coates, R. & Heffernan, T. (2003). "What develops in visuo-spatial working memory development?", European Journal of Cognitive Psychology, vol. 15, no. 1, pp. 43-69.

HirschI, T. (1969), Causes of Delinquency, Berkeley: University of California Press.

Huang, C., Liu, J., Fang, Y. & Zuo, Z. (2016). “A study on Web security incidents in China by analyzing vulnerability disclosure platforms“, Computers & Security, vol. 58, pp. 47-62.

Javanmard, H. (2012). “The impact of spirituality on work performance“, Psychology of Religion and Spirituality, Vol. 6, No. 3, 175-187.

Kim, J., Park, E.H. & Baskerville, R.L. (2016). “A model of emotion and computer abuse“, Information & Management, vol. 53, no. 1, pp. 91-108.

Lee, S.M., Lee, S. & Yoo, S. (2004). “An integrative model of computer abuse based on social control and general deterrence theories“, Information & Management, vol. 41, no. 6, pp. 707-718.

Liu, C. (2014). “Feature: The enemy within: the inherent security risks of temporary staff”, Computer Fraud & Security, vol. 2014, no. 5, pp. 5-7.

Markey, R. & Townsend, K. (2013). “Contemporary trends in employee involvement and participation“, Journal of Industrial Relations, vol. 55, no. 4, pp. 475-487.

Pallant, J. (2016). SPSS survival manual: a step by step guide to data analysis using IBM SPSS, Sixth edn, Allen & Unwin, Sydney.

Rocha Flores, W., Antonsen, E. & Ekstedt, M. (2014). “Information security knowledge sharing in organizations: Investigating the effect of behavioural information security governance and national culture“, Computers & Security, vol. 43, pp. 90-110.

Roy Sarkar, K. (2010). “Assessing insider threats to information security using technical, behavioural and organisational measures“, Information Security Technical Report, vol. 15, no. 3, pp. 112-133.

Saris, W.E. & Gallhofer, I.N. (2014). Design, evaluation, and analysis of questionnaires for survey research, Second edn, Wiley, Hoboken.

Schaefer, T., Brown, B., Graessle, F. & Salzsieder, L. (2017). “Cybersecurity: Common Risks: A dynamic set of internal and external threats includes loss of data and revenue, sabotage at the hands of current or former employees, and a PR nightmare“, Strategic Finance, vol. 99, no. 5, pp. 54-61.

Tabachnick, B.G. & Fidell, L.S. (2014). Using multivariate statistics, 6th , internat edn, Pearson Education, Harlow.

Thompson, N. (2014). What is Travis Hirschi’s Social Control Theory? Enotes. Available at: http://www.enotes.com/homework-help/what-travis-hirschis-social-control-theory-196501. [Accessed 16 June 2016].

Van der werff, E. & Science Steg, L. (2016). “The psychology of participation and interest in smart energy systems: Comparing the value-belief-norm theory and the value-identity-personal norm model“, Energy Research & Social, vol. 22, pp.107-114.

Velez, M.J. & Neves, P. (2017). “The relationship between abusive supervision, distributive justice and job satisfaction: A substitutes for leadership approach“, Revue Europeenne de Psychologie Appliquee, vol. 67, no. 4, pp. 187

Von solms, R. and Von solms, B. (2004). “From policies to culture”, Computers & Security, vol. 23, no 4, pp. 275-279.

Wallbank, P. (2019). The future of outsourcing. [online] Theaustralian.com.au. Available at: https://www.theaustralian.com.au/business/business-spectator/news-story/the-future-of-outsourcing/22a80aea41b2700fc209173dbc6d20d4 [Accessed 1 Sep. 2019].