A Behavioural Model for Assessing Employees Susceptibility to Social Engineering Attack

Ajah, E.O. & Longe, O.B.
Information Systems Programme
School of IT & Computing
American University of Nigeria
Yola, Nigeria
E-mail: emmanuel.ajah@aun.edu.ng, olumide.longe@aun.edu.ng
Phone: +2348160900893, +2347064499269

ABSTRACT

The protection of information systems infrastructure in organizations are paramount because the security of information confidentiality, integrity, availability, and accountability is a major concern to the public and private sectors. Organizations continue to lose money by the day and this challenges have led organizations' to implemented both technical and non-technical (policy development and implementation) measures to mitigate security breaches. Technical and non-technical measures have not effectively solved the information security problem facing organizations because employees continuously engage in activities that undermines information security policy in the work environment. This is clearly illustrated by the continuous increase in the number of attack cases recorded in recent times. Employees' behavior plays a huge role in the failure to mitigate information security risks. They are the weakest link in the information security architecture of any organization. Therefore, without effective and well-guided interaction between human and computer systems, even the best technical measure implemented to mitigate information security breach will not be successful. To model employee behavior that have continuously exposed them to social engineering attack, will require the guidance of some theories. These theories act as lens to model how employees' behavior facilitate the persistent susceptibility to social engineering attack. For the purpose of this paper, we will consider four theories; they include Neutralization Theory, Interpersonal Deception Theory, Information Manipulation Theory, and Rational Choice Theory. Using quantitative technique and a set of hypothesis, we developed a model that can be used to asses employee susceptibility to social engineering attacks. However, to achieve generalization, future work will test the efficacy of the model proposed in a larger empirical situation.

Keywords: Behavioural Model, Assesment, Employees Susceptibility, Social Engineering Attacks

23rd iSTEAMS Conference Proceedings Reference Format
Ajah, E.O. & Longe, O.B. (2020): A Behavioural Model for Assessing Employees Susceptibility to Social Engineering Attack
Proceedings of the 23rd iSTEAMS Conference, American University of Nigeria, Yola. April, 2020. Pp 47-58 www.isteams.net/yola2020..

1. INTRODUCTION

The emergence of knowledge-based economy today have influenced many organizations to solely depend on information systems for their day-to-day operation. Creating organizational fleaxibility in operation through interconnecting computer systems to the internet across the globe. Malicious group of people exploits these processes. Consequently, creating information security breach through the activities of activated virus, hackers, malicious and non-malicious insiders whose activities directly or indirectly prevent the organization from

achieving their goals and objectives (Krombholz, Hobel, Huber, & Weippl, 2015; Safa et al., 2015; Stanton, Stam, Mastrangelo, & Jolton, 2006; Williams, Hinds, & Joinson, 2018; Workman, 2007). The ubiquitous nature of Internet connectivity makes it possible for cybercrimes to be committed at any location in the world by exploiting human vulnerability. Therefore, cybercrime are increasingly committed because users are easily exploited and it is often difficult to trace and prosecute the offenders (Warkentin & Mutchler, 2014).

Accenture and the Ponemon Institute, (2019) published an outcome of a study carried out by interviewing 2,647 experts from 355 companies within 16 industries across 11 countries of the world, on the cost of cybercrime on this companies. The outcome clearly shows that American firms suffers the most lose with an average cost per company at US$27.4 million, which is twice the loss of any other country involved in the survey. The other countries who also lost high amount include Japan (US$13.6 million), Germany (US$13.1 million), The UK (US$ 11.5million) and the lowest of all loses were in Brazil and Australia whose lost are US$ 7.2million and US$6.8 million, respectively.

The protection of information systems infrastructure to ensure Information Confidentiality, Integrity, Availability, and Accountability is a major concern in the public and private sectors today. The risk of losing data through information security breach is both internally and externally motivated and organizations' have implemented both technical and non-technical (Policy Development and Implementation) measures to mitigate information security breaches encountered (Sikolia, Mason, Biros, & Weiser, 2014).

Technical measures have not effectively solved the information security problem facing organizations because employees continuously engage in activities that undermines information security policy in the work environment. Employees' behavior plays a huge role in the failure to mitigate information security risk. Employees are the weakest link in information security architecture of an organization. Therefore, without effective and well-guided interaction between human and computer systems, even the best technical measures implemented to mitigate information security breach will not be successful. (Stanton et al., 2006; Warkentin & Mutchler, 2014; Willison & Warkentin, 2013).

The remaining sections of this paper are structured as follows; section two contains the definition of social engineering and the various attack vectors used by social engineers. The theoretical background and the proposed conceptual framework we adapted is contained in section three of this paper. Section four discusses the validation methodology, proposed data collection method and the proposed approach adopted in the analysis of the collected data. The fifth section discusses the implications of the research study, practices in the industry and direction for future works.

2. SOCIAL ENGINEERING

Social engineering is an attack technique applied by people with malicious intent to deceive authorized users of information system (Algarni, Xu, & Chan, 2017; Mouton, Leenen, Malan, & Venter, 2014; Williams et al., 2018). The process involves exploiting human weakness, gullibility, and ignorance to gain access to organizations' network. Attacks persuade employees to obtain information that will grant them access to carry out malicious intent. Social engineers often depend on techniques that help to influence and persuade victims to divulge information that will enable them breach a secured network or system (Smith, Papadaki, & Furnell, 2013). The attack vectors are useful tools that aid the activities of a social engineer towards breaching an information system security.

This is illustrated in the figure1 below:

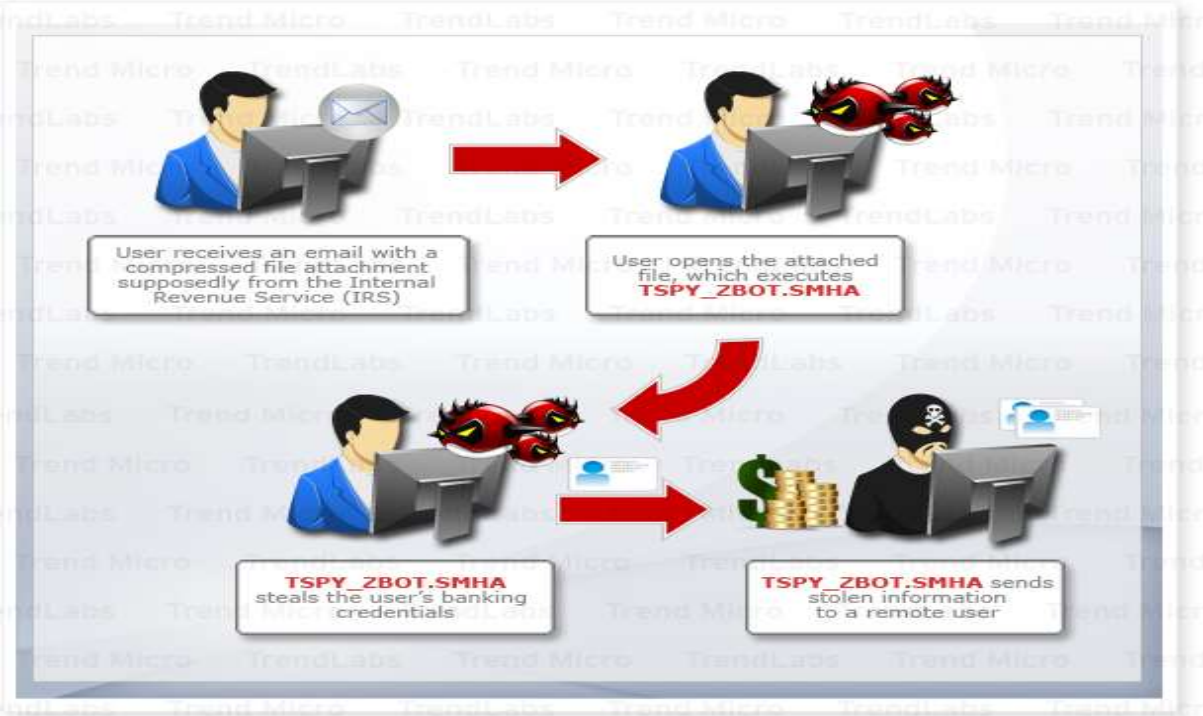

Figure 1: Social Engineering Facilitates Tax Season Malware Attacks - Threat
Source: Adopted from Ryan Angelo Certeza. (2011), Trendmicro.com

2.1 Social Engineering Attack Vectors

Social engineering attack on information systems completely operate by exploiting human component of information security architecture to achieve malicious intent. The following are various attack vectors used by social engineers, they include phishing, spear phishing, shoulder surfing, reverse engineering, water holing, baiting, dumpster diving and advanced persistent threat (Bullée, Montoya, Pieters, Junger, & Hartel, 2018; Krombholz, Hobel, Huber, & Weippl, 2015; Safa & Maple, 2016; Workman, 2008).

- **Phishing Attack:** This attack approach involves constructing a well-manipulated message, which are been sent via electronic mailing system to a target victim. The aim is to persuade and deceive victims to open an attachment or a hyperlink contained in the electronic message received. They often achieve this deceptive act by masquerading as a trusted person. The attacker usually targets a group of people or a specific victim in the case of a spear phishing attack (Applegate, 2009; Krombholz et al., 2015). However, spear phishing attack requires the attackers to first obtain detailed information about the identified victim before engaging the victim.
- **Shoulder Surfing:** This is an attack technique used by attackers to obtain vital information such as passwords, personal identity number and confidential information from a target victim. This is achieved through an attacker observing the victim by looking over the target shoulder while they work on a computer system (Applegate, 2009).

- **Reverse Engineering:** In this approach, the attacker first build trust between him and the victim. The trust is achieved by creating a problem that affects the victim, and the victim has no idea about the source of the problem been experienced on the system. Then, the attacker presents a solution to the problem. This makes the victim consider the perpetrator(attacker) as a trusted friend thereby divulging sensitive information to them (Krombholz et al., 2015).
- **Dumpster Diving:** This method of attack involves an attacker attempting to take advantage of the ignorance of employees' attitude towards disposing official document without checking through the kind of document or items they discarded as trash. Hackers often search for sensitive information in the trash bin of private individuals or organizations to find discarded information that might be useful to them. This information includes employees account details or sensitive information of the organization (Applegate, 2009; Krombholz et al., 2015).
- **Baiting:** This is an effective attack technique used by attackers to gain access to a secured system. An attacker strategically abandons a malware infected storage device such as a flash drive in a location where the targeted victim will find it. The victim out of curiosity or greed attempts to use the device; Hence, he activates or injects malware into their network or system. (Airehrour, Nair, & Madanian, 2018).
- **Water Holing:** This is a type of attack technique, an act of compromising a specific website that a victim is expected to visit. The attackers infect a website with a malware, the malware is activated by the employees unknowingly by their actions as they navigate through the website (Airehrour et al., 2018).
- **Advance Persistent Threat:** This is an internet based espionage; it is a form of attack technique used by hackers who have technical ability to persistently compromise a system or network with or without the knowledge of the victim (Krombholz et al., 2015).

Therefore, employees' attitude towards engaging in malicious activities, negligence or ignorance to operational ethics is a major security problem. Social engineers often take advantage of the employees' refusal or inability to comply with the Security Policy of the organization. (Siponen & Vance, 2010).

3. THEORETICAL BACKGROUND AND RESEARCH MODEL

To model employee behavioral pattern towards engaging activities that exposes them to social engineering attack, requires the guidance of some theories. These theories will act as theoretical lens by which we model employees' behavior that makes them susceptible to social engineering attack. In this paper, we propose to consider four different theories. This include Neutralization Theory, Interpersonal Deception Theory, Information Manipulation Theory, and Rational Choice Theory. From previous studies, scholars have approached their studies using various theories such as Theory of planned behaviour, Cognitive response theory and other. However, for this study, the above selected theories are been considered most appropriate because they provide a clear description and higher explanatory power that explains the phenomenon of interest (the behavioural pattern of employees making them susceptible to social engineering attack) (Algarni, Xu, & Chan, 2017; Siponen & Vance, 2010)

3.1 Conceptual Framework for Assessing Employee Susceptibility to Social Engineering Attack

The figure2 below is a framework, conceptually developed from four theories adapted in these studies as a theoretical lens that explains the behavior of employee susceptibility. The conceptual framework is designed to help demonstrate and explain how employee's behaviour exposes them to possible attack from a social engineer.

It contains concept like Negligence/Ignorance from previous literature and concepts adapted from Information Manipulation Theory (IMT), Interpersonal Deception Theory (IDT), Neutralization Theory (NT), and Rational Choice Theory (RCT). Consequently, the proposed conceptual framework is representing constructs that explains employees possible behaviour in a given organization, which exposes them to social engineering attack. Therefore, we intend to test this conceptual framework with the proposed empirical situation as described in the next section.

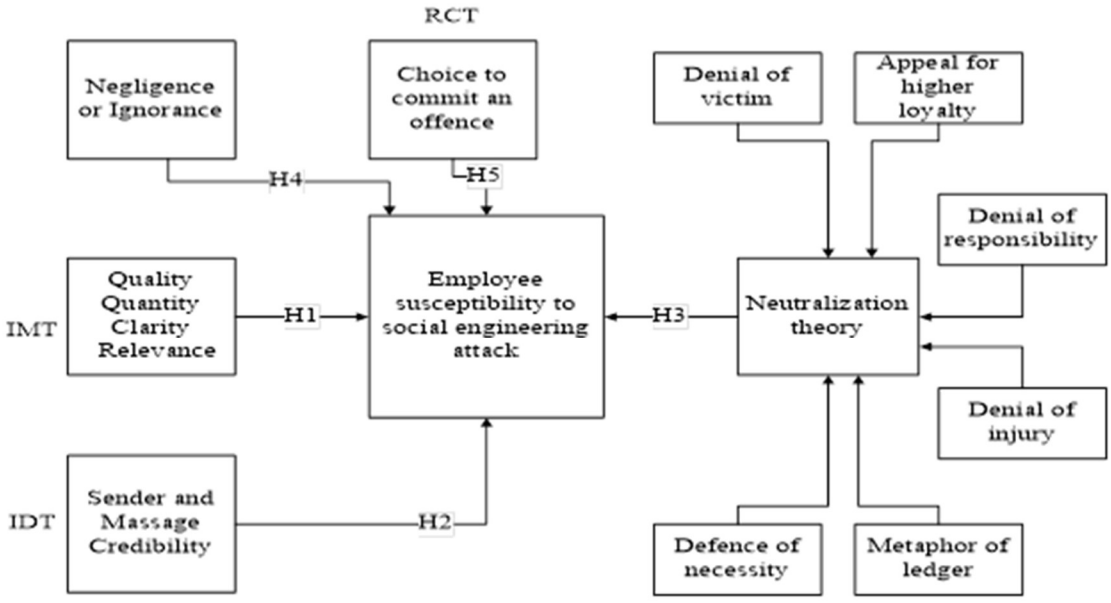

Fig1: Employee Susceptibility Model (ESM)
Source: Fieldwork Ajah and Lunge, 2019

Figure 2: Employee Susceptibility to Social Engineering Model
Source: Fieldwork Ajah and Longe, 2019

3.1.1 Information Manipulation Theory (IMT)

This is a theory used in the field of communication and it is being adopted in information systems security studies to explain how employees in an organization are manipulated to divulge sensitive information to hackers for malicious intent. The theory states that in every conversation, individuals involved expect that information transmitted during conversation should possess quality, quantity, clarity, and relevance. IMT expresses that any or all the expectations can be easily exploited and manipulated by people with malicious intent to persuade and deceive the target employee to divulge sensitive information (Warkentin & Mutchler, 2014; Yeung, Levine, & Nishiyama, 1999). It is possible for employees to identify the level of deception a message or conversation contains through quantifying and measuring the level of quality, quantity, clarity, and relevance of the information communicated. However, this is often not the case because employees either have malicious intent, ignorant or neglect to evaluate the integrity of the message received.

3.1.1.1 Hypothesis

Based on the forgoing studies, we proposed the following hypothesis as derived from the IMT context.

H1: Employee inability to evaluate the integrity of received massage makes the employee susceptible to social engineering attack.

3.1.2 Interpersonal Deception Theory (IDT)

This is another theory used in the field of communication and information systems scholars for information security studies adopt it. This is a process where a sender (hacker) intentionally attempts to manipulate and deceive a receiver to divulge sensitive information that is capable of compromising the organization. However, it is expected that the receiver of the message judges the credibility of the sender and the message received. During the conversation, a hacker (sender) attempt to insert false information into the message sent, then observes to see the reaction of the receiver towards recognizing the false information sent.

If the receiver did not react to the false information, the sender will continue the conversation by inserting more false information and adjust his act in order to avoid being noticed or detected by the receiver (Burgoon & Buller, 2015; Hearn, 2006; Warkentin & Mutchler, 2014). This conversation will continue in this manner, thus increasing familiarity and trust between sender and receiver leading to a launch of an attack. This kind of conversation occurs in face-to-face communication and via telephone and through email. This trick helps to persuade an employee in revealing sensitive information like credit card information, password and other vital information (Kim, Yang, & Park, 2014; Vance & Siponen, 2012; Warkentin & Mutchler, 2014).

3.1.2.1 Hypothesis

The hypothesis that emanates from the foregoing is stated below

H2: Employee inability to determine the credibility of a sender during communication to avoid falsification of information positively increases employee susceptibility to social engineering attack.

3.1.3 Neutralization Theory

Employees' behavior has continuously violated measures put in place to mitigate information security breach in organizations. This is explained by the neutralization theory, this theory offers reasons why an employee will make existing security norms and policies inactive through justifying an act of non-compliant behavior that sabotages the security policy of the organization (Kim et al., 2014; Siponen & Vance, 2010; Warkentin & Mutchler, 2014). Therefore, neutralization theory has a great negative effect on deterrence theory because it justifies why an employee who has violated the security policy should not be sanctioned. Hence, sanctions lose potency in the face of neutralization techniques. "Neutralization theory states that regardless of the values and norms to which an individual prescribes a process to neutralize or justify, breaking a rule may be performed when the individual desires the outcome believed to be attainable by performing an action" (Warkentin & Mutchler, 2014).

Sykes and Matza (1957) proposed five techniques for neutralization theory, these include denial of responsibility; denial of injury; denial of the victim; condemnation of the condemners; and appeal to higher loyalties. Klockers, (1974) added metaphor of the ledger as a technique to the existing neutralization techniques and Minor (1981) also added another technique he called the defense of necessity.

For the purpose of this study, we will concentrate on the following neutralization techniques or constructs as illustrated in figure 1: denial of responsibility, denial of necessity, denial of injury, appeal for higher loyalties, the metaphor of the ledger and denial of the victim.

- **Denial of Responsibility:** This is a technique where an employee violates security policy and expresses that they lack responsibility for the action, therefore, justifies their action by emphasizing that his action is beyond their control. They see themselves helpless of the situation leading to violation of the security policy (Warkentin & Mutchler, 2014).
- **Defense of Necessity:** This technique expresses a justification for breaking information security policy and why they should not fill guilty of violating any rule. Because the end justifies the means. (Warkentin & Mutchler, 2014). For example, an employee disclosing sensitive information without authorization because it is a matter of national security.
- **Denial of Injury:** This technique justifies breaking information security rule by minimizing the level of harm created (Warkentin & Mutchler, 2014). Employees' tries to minimize the level of damage their action have caused the organization by emphasising that their action did not cause any lasting damage to the system.
- **Appeal to Higher Loyalties:** This technique attempts to justify violating the rule by making excuses that the job could not have been done without violating the rule (Warkentin & Mutchler, 2014).
- **The Metaphor of the Ledger:** This technique illustrates how an exceptional employee attempts to rationalize his misdeed in violating information security policy by referring to some good deed done in the past (Warkentin & Mutchler, 2014).
- **Denial of Victim:** In this technique, an aggrieved employee attempts to justify an act of policy violation by emphasizing that the victim of his act deserves to be punished based on some offense the victim had committed earlier (Warkentin & Mutchler, 2014). . For example, an employee who is aggrieved with the employer's previous action towards them might choose to violate security policy in order to punish the employer.

3.1.3.1 Hypothesis

An applicable hypothesis is stated below.

H3: Continuous neutralization of sanctions as employees engage in activities that violates security policies in the organization, positively increases employee susceptibility to social engineering attack.

3.1.4 Negligence or Ignorance

In many occasion, employees violate information security policies because of negligence or ignorance (Siponen & Vance, 2010). Therefore, social engineers often take advantage of this group of employees to carry out their malicious intent against the organization through various attack vectors identified above.

3.1.4.1 Hypothesis

A relevant hypothesis is stated below.

H4: Negligence and ignorance positively enhances employee continuous susceptibility to social engineering attack.

3.1.5 Rational Choice Theory (RCT)

This theory proposes that an assessment of cost and benefits of one's decision to violate a law or policy is carried out before engaging in deviant behaviour. Therefore, individuals tend to be sensitive to the consequence of their action before engaging in them. Note that if an employee perceives that the benefit of his deviant behavior outweighs the cost, they engage in the act (Bulgurcu, Cavusoglu, & Benbasat, 2010; Kim et al., 2014; Sikolia et al., 2014; Warkentin & Mutchler, 2014).

3.1.5.1 Hypothesis

The justified hypothesis is stated below.

H5: Continuous engagement in deviant behaviour due to its benefits, increases employee susceptibility to social engineering attack.

The act of persuasion and manipulation are major tools applied by social engineers. Social engineers in an information security context effectively utilize these tools. This enables them bypass technical security measures in an organization, thereby gaining access to confidential information. Human dynamic behavior presents the desired opportunity to hackers who seek to exploit and attack an organization by taking advantage of employees susceptibility (Bullée et al., 2018; Workman, 2007). The ability for an information systems user in organization to guide their behavior, by ensuring that they comply to security policies of the organization, helps to protect the organization from been exploited by hackers (Safa, Maple, Watson, & Von Solms, 2018; Yeboah-Boateng, 2013).

This can only be achieved in an ideal situation where the employees maintain the right attitude. However, it is not often experienced in a work environment. The figure1 above illustrates the theoretical framework of the study as discussed above. It clearly shows the behavioral pattern of employees in a given organization and how their choice to violate security policies by indulging in unethical activities exposes the organization to social engineering attack. However, the protection of the information systems of an organization from social engineering attack depends on employees attitude towards compliance with information security policies in place (Airehrour et al., 2018; Applegate, 2009; Krombholz et al., 2015).

4. VALIDATION METHODOLOGY

The main purpose of this study is to develop a model that assesses the behavioural pattern of employees in a work environment. The model aims to express how an employee become exposed to the activities of social engineers, whose main objective is to take advantage of vulnerable employees in the cyber space. This research study will adopt quantitative method of research. A questionnaire will be developed based on the phenomenon of interest and based on acquired knowledge from the previous literatures. An electronic and a paper questionnaire will be developed to enable us collect the required data from the chosen sample space. The expected questions contained in the questionnaire will be based on a five-point Likert scale that will range from strongly agree to strongly disagree.

4.1 Proposed Data Collection

A survey approach will be adopted to help us collect data required to test the validity of the hypothesis derived from the theoretical framework. The proposed audience for survey will cut across a population that will be carefully selected from a group of information systems users, consisting of four (4) organizations that have implemented information security policy within the organizations. The population sample will consist of two (2) public organization and two (2) private organization. A total number of 200 users, 50 users from each organization will be involved in the survey process. The data obtained from the survey will be analysed using a statistical tool called structural equation modelling tool.

4.2 Proposed data analysis approach

The research model as shown above was developed from four theories: This includes neutralization theory, interpersonal deception theory, information manipulation theory, and rational choice theory. The need to validate the observable and latent variables derived from the theories that guide our model is why we are proposing a confirmatory factor analysis approach, to enable us assess the measurement model and further assess structural model validity of the proposed theoretical framework. Structural equation modelling is adopted for this study because of its uniqueness in measurement analysis towards this kind of study that involves investigating behavioural pattern of information systems users.

It is a processing tool for testing hypothesized relationships between constructs of a theoretical framework. Testing developed theoretical models focuses on:

- The entire related model fit.
- The direction, significance and size of the entire structural parameters estimated, which are indicated with a single headed arrow on the path diagram.

There are some stages involved in structural equation modelling, this are illustrated below:

- Definition of individual construct.
- The development of the overall measurement model.
- Develop a study pattern to produce empirical results.
- Evaluating the measurement model validity of the theoretical framework.
- Specify the structural model.
- Evaluating structural model validity of the theoretical framework.

5. RESEARCH IMPLICATION AND FUTURE DIRECTION

5.1 Implication for Practice

The complexity in user behavior towards the use of information systems in organization, have continuously sabotaged organizational objectives. Employees' engagement in activities that make them susceptible or vulnerable to social engineering attack is alarming. Therefore, understanding the factors responsible for this persistent behavior cannot be overemphasized. The identification of the causalities responsible for this phenomenon will help to guide organizations towards mitigating security breach and improve employee behavior towards the use of information systems in work environment.

5.2 Implication for Policy

The outcome of this research will drive the development of policies that will help guide employee behaviour in work environment. Consequently, makes employees to be conscious of attacks from social engineers and enables them understand how to prevent been susceptible attack.

5.3 Direction for Future Research

Further research is needed to test the efficacy of the model proposed. In addition, to understand how best to mitigate employee susceptibility. It is also important to conduct a future research on a large empirical situation cutting across various organizations for better generalization of outcome.

REFERENCE

1. Airehrour, D., Nair, N. V., & Madanian, S. (2018). Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model. *Information*, *9*(5), 110. https://doi.org/10.3390/info9050110
2. Ajah, E.O. & Longe, O.B. (2019). Employee Susceptibility Model (ESM), PhD Fieldwork- American University of Nigeria, Yola, April 2019.
3. Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. *European Journal of Information Systems*, *26*(6), 661–687. https://doi.org/10.1057/s41303-017-0057-y
4. Applegate, S. D. (2009). Social Engineering: Hacking the Wetware! *Information Security Journal: A Global Perspective*, *18*(1), 40–46. https://doi.org/10.1080/19393550802623214
5. Bulgurcu, Cavusoglu, & Benbasat. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523. https://doi.org/10.2307/25750690
6. Bullée, J.-W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks-A literature-based dissection of successful attacks: On the anatomy of social engineering attacks. *Journal of Investigative Psychology and Offender Profiling*, *15*(1), 20–45. https://doi.org/10.1002/jip.1482
7. Burgoon, J. K., & Buller, D. B. (2015). Interpersonal Deception Theory. In C. R. Berger, M. E. Roloff, S. R. Wilson, J. P. Dillard, J. Caughlin, & D. Solomon (Eds.), *The International Encyclopedia of Interpersonal Communication* (pp. 1–6). https://doi.org/10.1002/9781118540190.wbeic170
8. Hearn, J. (2006). *Interpersonal Deception Theory: Ten Lessons for Negotiators*. 6.
9. Kim, S. H., Yang, K. H., & Park, S. (2014). An Integrative Behavioral Model of Information Security Policy Compliance. *The Scientific World Journal*, *2014*, 1–12. https://doi.org/10.1155/2014/463870
10. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005
11. Minor, W. W. (1981). *AND EMPIRICAL EXAMINATION*. 24.
12. Mouton, F., Leenen, L., Malan, M. M., & Venter, H. S. (2014). Towards an Ontological Model Defining the Social Engineering Domain. In K. Kimppa, D. Whitehouse, T. Kuusela, & J. Phahlamohlaka (Eds.), *ICT and Society* (Vol. 431, pp. 266–279). https://doi.org/10.1007/978-3-662-44208-1_22
13. Safa, N. S., & Maple, C. (2016). Human errors in the information security realm – and how to fix them. *Computer Fraud & Security*, *2016*(9), 17–20. https://doi.org/10.1016/S1361-3723(16)30073-2
14. Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications*, *40*, 247–257. https://doi.org/10.1016/j.jisa.2017.11.001
15. Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65–78. https://doi.org/10.1016/j.cose.2015.05.012
16. Sikolia, D., Mason, M., Biros, D., & Weiser, M. (2014). *A Theory of Employee Compliance with Information Security*. 7.
17. Siponen, & Vance. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, *34*(3), 487. https://doi.org/10.2307/25750688

18. Smith, A., Papadaki, M., & Furnell, S. M. (2013). Improving Awareness of Social Engineering Attacks. In R. C. Dodge & L. Futcher (Eds.), *Information Assurance and Security Education and Training* (Vol. 406, pp. 249–256). https://doi.org/10.1007/978-3-642-39377-8_29
19. Stanton, J. M., Stam, K. R., Mastrangelo, P. M., & Jolton, J. A. (2006). *BEHAVIORAL INFORMATION SECURITY*. 19.
20. Sykes, G. M., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, *22*(6), 664. https://doi.org/10.2307/2089195
21. Ryan Angelo Certeza. (2011). https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web- attack/82/social-engineering-facilitates-tax-season-malware-attacks
22. Vance, A., & Siponen, M. T. (2012). IS Security Policy Violations: A Rational Choice Perspective. *Journal of Organizational and End User Computing*, *24*(1), 21–41. https://doi.org/10.4018/joeuc.2012010102
23. Warkentin, M., & Mutchler, L. (2014). Behavioral Information Security Management. In H. Topi & A. Tucker (Eds.), *Computing Handbook, Third Edition* (pp. 54-1-54–20). https://doi.org/10.1201/b16768-62
24. Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, *120*, 1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004
25. Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly*, *37*(1), 1–20. https://doi.org/10.25300/MISQ/2013/37.1.01
26. Workman, M. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information Systems Security*, *16*(6), 315–331. https://doi.org/10.1080/10658980701788165
27. Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, *59*(4), 662–674. https://doi.org/10.1002/asi.20779
28. Yeboah-Boateng, E. O. (2013). *Of Social Engineers & Corporate Espionage Agents: How Prepare Are SMEs in Developing Economies?* 9.
29. Yeung, L. N. T., Levine, T. R., & Nishiyama, K. (1999). Information manipulation theory and perceptions of deception in Hong Kong. *Communication Reports*, *12*(1), 1–11. https://doi.org/10.1080/08934219909367703