End-User Perceptions on Information Security: Pragmatic Lessons on Social Engineering Attacks in the Workplace in Gauteng, South Africa

Shandre Jansen van Rensburg, University of South Africa, South Africa*

ABSTRACT

Information is a vital asset needed by many organizations to function effectively. However, this asset can easily be compromised; thus, its protection is crucial to the efficacy of an organization. A common information security breach used is social engineering. Social engineering is the use of manipulative and deceptive techniques against the inherent nature of human beings to access sensitive and confidential information to achieve an illicit action or omission of action. Through a qualitative inquiry, this article investigated the perceptions of employees concerning social engineering in the workplace to extract practical lessons from local businesses located in Gauteng Province, South Africa. The findings confirm that human beings should be at the forefront of defense against social engineering attacks and advocates for a multi-inter-trans-disciplinary social engineering protection model to practically assist organizations in developing a healthy and effective information security culture.

KEYWORDS

Cyber Security, Data Breaches, Information Security, Personal Information, Social Engineering

INTRODUCTION

Many information security breaches, which transpire in the workplace, are largely the result of noncompliance (intentional or unintentional) to information security policies (Kessler et al., 2020; Safa & Maple, 2016; Verizon Enterprise, 2018). In fact, organizations cite negligent employees as their greatest vulnerability to risk exposure (Ernst & Young, 2019). An International Business Machines (IBM, 2020) security study on the cost of information security breaches revealed that the global average cost of a data breach is \$3.86 million. The United States of America recorded the highest average total cost of data breaches at \$8.64 million, followed by the Middle East at \$6.52 million and Canada at \$4.5 million. Conversely, Latin American and Brazil had the lowest average total cost at \$1.68 million and \$1.12 million, respectively. In South Africa, the average cost of a data breach is estimated to be \$2.14 million and takes approximately 228 days to detect and contain (IBM, 2020). A global pandemic, brought about by COVID-19, has caused employers to allow their employees to work outside of the traditional office environment to increase social distancing defense mechanisms (World Health Organization, 2020; Blurke, 2020; Hunter, 2019; Kelly, 2020). This increase in remote

DOI: 10.4018/JGIM.293290

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

working and use of own device for work purposes makes it significantly more difficult and costly to identify and contain a data breach (Baillette & Barlette, 2020; IBM, 2020). Global and local findings show increased budget allocations for automated, physical and technological security systems (Chan et al., 2014; Herath & Rao, 2009; Mouton et al., 2014a). However, information security breaches are on the increase and are largely undeterred (Verizon Enterprise, 2018), particularly concerning mistakes and misdemeanors made by end-user employees (Chan et al., 2014). Within the South African context, scientific and pragmatic research on information security and the multi-inter-trans-disciplinary (MIT) nature of social engineering in the workplace is under-developed. There is a dearth of awareness and implementation of user-friendly resources to sustain a healthy level of security and protection.

Social engineering is a psychological strategy used to manipulate and exploit end-users for personal gain. It is the use of devious and deceptive techniques against the inherent nature of human beings to access sensitive and confidential information in order to achieve an illicit action or omission of action (Jansen van Rensburg, 2017). The root causes of data breaches are categorized as malicious attacks, system glitches and human error (IBM, 2020). Social engineering attacks are the result of one or a combination of these categories. Information security breaches manifest in different ways that include the hacking of Twitter as well as the Zoom and Marriott data breaches (Dutta, 2020). The Marriott data breach involved the theft of half a million global hotel guests' personal information through credential stuffing and phishing attacks – notorious social engineering techniques (Marriott International, 2020).

The social information processing approach proposes that researchers should study the informational and social environment where the behavior under investigation occurs (Salancik & Pfeffer, 1977). Therefore, this study was rooted in the organizational and information security climate. The organizational climate refers to the values, attributes and procedures (formal and informal) embraced by an organization that influences employee behavior. Chan et al. (2014) indicate that organizations that uphold a safety climate are more likely to influence their employees to comply with information safety requirements. Through the descriptive perceptions of end-user employees working in South African organizations, this article provides a holistic exposé of social engineering and the pragmatic lessons they offer. Thus, this paper contributes to knowledge by establishing social engineering as a MIT attack that consequently requires a MIT social engineering protection model to empower organizations to develop healthy and effective information security cultures.

The paper is organized as follows: a global perspective of information security and contextualization of social engineering in a (MIT) milieu, research methodology, findings and discussion. Additionally, the paper details and advocates for an MIT social engineering protection model.

GLOBAL PERSPECTIVE OF INFORMATION SECURITY IN THE WORKPLACE

The rapid development and transformation of information technologies and its use has resulted in a rise in security issues and breaches across the globe (Chmura, 2017). In the Global Information Security Survey conducted by Ernst & Young (EY), it was consistently found that the biggest security vulnerability is lack of awareness by employees (end-users) (EY, 2017). Exasperating the problem further is that the international standards and norms surrounding privacy, trust, disclosure of information online and healthy information security practices vary across cultures and nationalities (Benamati, Ozdemir & Smith, 2021; da Veiga & Martins, 2017). Insights drawn from this paper can assist managers, business owners and organizational decision makers with an example of a multi-inter-trans-disciplinary social engineering protection.

SOCIAL ENGINEERING CONTEXTUALISED IN A MULTI-INTER-TRANS-DISCIPLINARY MILIEU

Social engineering can be traced back to the existence of life intellectual enough to deceive (Ali-Kovero, 2020). The conceptual evolution of social engineering originates from the political science discipline found in the work of John Gray (1842), who referred to social engineers as people who portrayed themselves as having the solutions to political and societal problems. Seminal work on the subject matter delves into the conceptualization of the phenomenon, as well as the threats, attacks and defense strategies (Cialdini, 2001; Gragg, 2003; Hadnagy, 2011; Hatfield, 2018; Mann, 2008; Mitnick & Simon, 2002). Today, the disciplines that contribute to research on social engineering include psychology, law, criminology, security and computer science (Frangopoulos, 2007; Gragg, 2003; Nohlberg, 2008). In psychology, social engineering techniques are explained through “psychological triggers” (Gragg, 2003). Law highlights the influence of social engineering on the legality and social behavior in society (Nohlberg, 2008). Criminology and security sciences are particularly interested in social engineering and information security as these concepts cross the borders of criminality, legality and security (Hadnagy, 2018).

At the forefront of the most progressive advances in social engineering is the research founded on computerized automated defense mechanisms (Bay et al., 2006; Edwards et al., 2017; Gunawardena et al., 2013; Heartfield et al., 2016; Kaul & Sharma, 2013; Mouton et al., 2016; Rao & Ali, 2015). Recently, an experimental study on the prevention of social engineering attacks established that priming and warnings were effective as deterrents (Junger et al., 2017). The study, however, notes the crucial distinction between understanding social engineering attacks as opposed to merely priming and warning potential victims. Moreover, the prioritization of safety and security measures were not deemed essential in the experiment conducted (Junger et al., 2017). Consequently, social engineering protective measures should be clearly understood by end-users and safety and security should receive ongoing precedence.

The notion of social engineering is multi-faceted and needs to be explored in its entirety through an MIT approach. The concept of MIT has been originated to break down barriers between different disciplines. MIT research also seeks to contest “silo-isolation” and “compartmentalization” in order to make research more pertinent and practical (Stock & Burton, 2011). MIT studies integrate and incorporate research from various disciplines but remain within the boundaries of those disciplines (Okumus et al., 2018). The term “multidisciplinary” refers to the concurrent studying of a research topic across two or more disciplines (inclusive of sub-disciplines), while the term “interdisciplinarity” involves the transfer of methods from one discipline to another, sometimes resulting in the development of a new discipline. “Transdisciplinarity” is the term frequently used to describe research that sits above and beyond all disciplines (Stock & Burton, 2011). This type of research seeks consultation and insight across disciplinary boundaries. Moreover, it is invested in the collaboration of stakeholders (Okumus et al., 2018).

To date, research tends to contextualize its analysis from the author’s specific school of thought. Moreover, studies tend to examine social engineering in its general execution (Hadnagy, 2018; Junger et al., 2016; Mouton et al., 2016) as opposed to research in the workplace environment. Consequently, very little research has worked towards a holistic analysis of social engineering in the workplace. Although evidence of similar studies (Ali-Kovero, 2020; Gragg, 2003; Saleem & Hammoudeh, 2018) to the present one exists, it lacks the practicality of a holistic approach to social engineering within the context of a developing country. Thus, the present study makes an explorative contribution by advocating the need for a user-friendly MIT social engineering protection model in the workplace.

GOAL OF THE STUDY

This study sought to explore the perceptions of end-user employees concerning information security and social engineering in the workplace in order to extract practical lessons from local businesses in Gauteng Province, South Africa. Subsequently, the research sought to answer the following question: What social engineering vulnerabilities are responsible for security information breaches at local businesses in Gauteng, South Africa?

METHOD

Research Design and Procedures

The study applied a qualitative approach to explore information about security practices in the workplace in Tshwane, Gauteng Province. Furthermore, an interpretative instrumental case study design was used (Chen, Yen & Lin, 2015; Fouché & Schurink, 2011; Su, Xu, Li, Martínez-López, & Li, 2018). Interpretivism advocates that social problems in the real world can be uncovered when research is conducted systematically, interactively and methodologically. Instrumental case study designs endorse the development of new knowledge about a social issue and, subsequently, are used for theory building, testing and policy development (Creswell, 2014; Fouché & Schurink, 2011; Guba & Lincoln, 1994). Qualitative surveys were used in this study to gather data. Qualitative surveys are used in various disciplines as a tool to collect empirical data as they focus on a variety of meanings within a population, and not on the number of people surveyed. Therefore, their objective is not to establish frequencies but to unpack the topic under investigation within a specific population (Jansen, 2010). This data collection tool was appropriate in terms of application and facilitation in the working environment. Scientific research is founded on trust, acceptance, participation and mutual expectation (Strydom, 2011). The study adhered to the University of South Africa's (UNISA) ethics policy and ethical clearance from the College of Law Ethics Committee was obtained.

Sample

Purposive sampling was used to target local businesses. As endorsed by Campbell et al. (2020) purposive sampling was used to select participants who could yield appropriate and useful information and select cases that leverage limited research resources effectively. Criterion-I, homogeneity and theory-based purposeful sampling strategies were used in selecting the purposeful samples. The Criterion-I purposeful sampling strategy selects cases based on predetermined criteria. The main criteria for participation included willingness to participate and interest in improving information security awareness. Homogeneity was implemented to describe a small group, decrease disparity, and facilitate group interviewing. Theory-based purposeful sampling assisted in the construction of theoretical manifestations by examining the sample (Palinkas et al., 2015; Patton, 2002). Twenty businesses in Tshwane were approached to take part in the study. However, only three businesses responded favorably to this request. The potential reasons for the low response rate were allocated to the ambiguity concomitant with social engineering in developing countries as not many people are aware of what it entails, its significance and how it can impact them. Although confidentiality and anonymity were guaranteed, businesses did not want to take the risks inherent in their information being published. Additionally, businesses did not want to take part in the study to avoid "misusing" valuable time and resources. The author tried to alleviate these factors by introducing training as part of her research study to better equip local businesses.

Increasingly, research communities are calling for research methodology that is transformative and beneficial to their needs (Chiblow, 2020; Mertens, 2017). The sample groups from each organization varied. Organization A (nine participants) is an organization that specializes in tax, audit and advisory services. Organization B (eight participants) specializes in consulting and analysis services for managing security risks. Organization C (five participants) is an insurance company. The

line managers in each organization asked employees to take part in the study. As participation was voluntary, a total of 22 qualitative surveys were collected over a three-month period. The researcher engaged in an interactive process whereby additional information was requested from the research participants. Additionally, the author engaged in a rigorous study on the organizational policy for each sample group.

Case Study Descriptions

Research using singular case studies is deemed as scientific and valuable as the focus of the study is to contribute to theoretical development (Yin, 2009). The strength of a case study is its ability to capture an aspect of reality (Schurink et al., 2021). The data are presented by the organizations under evaluation, namely, Organizations A, B and C. When citing a specific research participant from a specific organization, the individual is referred to by the organization and participant number allocated, for example, Organization A Participant 1 is referred to as OAP 1, Organization B Participant 7 is referred to as OBP 7 and Organization C Participant 9 is referred to as OCP 9).

Table 1. Research participants

Organization	Identification	Job Title	Employment Period
Organization A (Information security department within a financial company)	OAP 1	IT Consultant	< 1 year
	OAP 2	IT Analyst	< 1 year
	OAP 3	IT Analyst	< 1 year
	OAP 4	IT Consultant	< 10 years
	OAP 5	IT Auditor	< 1 year
	OAP 6	IT Analyst	< 1 year
	OAP 7	IT Consultant	< 1 year
	OAP 8	IT Auditor	< 2 years
	OAP 9	IT Auditor	< 2 years
Organization B (Enterprise risk solutions company)	OBP 1	Project leader	< 4 years
	OBP 2	Information Analyst	< 2 years
	OBP 3	Accounts Manager	< 2 years
	OBP 4	Information Analyst	< 2 years
	OBP 5	Crime Analyst	< 4 years
	OBP 6	Head of Department	< 6 years
	OBP 7	Head of Department	< 5 years
	OBP 8	Information Developer	< 3 years
Organization C (Insurance company)	OCP 1	Forensic Analyst	< 3 years
	OCP 2	Manager	< 10 years
	OCP 3	Information Security Specialist	< 10 years
	OCP 4	Manager	< 2 years
	OCP 5	IT Security Consultant	< 8 years

(Source: Author's own)

The presentation and analysis of data should take into consideration the occupations and operational functions of each research participant. Organization A comprised an information security department within a financial institution. All the research participants worked in the field of information technology (IT) and security. Organization B represented an enterprise risk solutions company. The Chief Executive Officer (CEO) requested that the sample include various role-players within the institution, so that these individuals could train other members in their respective departments. Thus, the sample was quite diverse. Organization C, an insurance company, consisted of employees who specialized in information security.

Data Collection and Analysis

The researcher requested and organized a 60-minute information security workshop with each of the three organizations. The session consisted of two parts: the distribution of a qualitative survey (30 minutes) and a presentation (30 minutes) on social engineering and information security awareness in the work environment. The qualitative survey was purposefully done before the presentation so as not to influence the research participants' answers. This method of conducting research was deemed innovative and beneficial to the three businesses as well as to the study. The information security workshop provided insight into social engineering attacks, human vulnerability and applicable South African legislation. The mainly qualitative raw data received were categorized into relevant themes and analyzed thematically. As each sample group was relatively small, organizational policies applicable to the businesses and literature were used to develop the findings.

FINDINGS AND DISCUSSION

Online communication is a significant part of modern society, particularly in most business settings, as online communication is an expedient and effective business tool (Wood & Smith, 2014). Balle (2016) agrees that the use of the internet can assist in advancing any business. Predictably, all the research participants shared that they used technological devices and the internet daily for work and personal use. In terms of accessing their personal information, most of the participants were aware that their personal information is publicly available. OAP 6 specifically mentioned that laws that protect privacy are not enforced. The Experian data breach resulted in the socially engineered loss of personal information belonging to 24 million South Africans as well as almost 800 000 businesses (South African Banking Risk Information Centre [SABRIC], 2020). On the 19 August 2020, Experian South Africa, a consumer, business and credit information services agency, announced that it had been subject to a data breach involving personal information that was shared with a social engineer. A fictitious company entered into a service agreement with Experian and, by impersonating its role and intentions, managed to illicit personal information ranging from contact details to residential and work addresses. Experian publicly maintained that no personal consumer credit, financial or banking information was shared (Experian, 2020). However, under the ambit of the South African legislation, Experian faces no recourse (Olenick, 2020). As a developing African country, legislation to address such information breaches was only enacted in 2013 and made effective in 2020 (Moyo, 2020; RSA, 2013). Prior to this, Kyobe (2009), identified cost as the main influencing factor affecting compliance with government regulation on IT in South Africa. The South African government has given companies until July 2021 to comply with the Act's specifications or face severe penalties (Moyo, 2020; RSA, 2013).

Currently, only 17 out of 54 African countries have data privacy laws (Moyo, 2020). This absence of protective legislation exposes African countries to increased risks to their information security thus warranting the need for healthy information security practices. In a study done by Makanda et al. (2017) on cyber security in underdeveloped and developing countries, it was found that the weaknesses in cyber security could be detrimental for the countries involved. Furthermore, OAP 7 and OAP 8 mentioned security defects on websites, while OAP 8 drew attention to the use of "cookies"

and their role in compromising information security. Cookies are small files that are stored on a user's technological device. They are created to hold a small quantity of data specific to a user and a website. They can be accessed by the web server (a system that distributes content or services to end-users over the internet) or through the user's technological device. In this way, information can be carried from one website to another. Although cookies are not malicious, they are able to store information given to a website such as credit card information or passwords. Thus, cookies can be a threat to privacy, but this can be prevented by turning off the cookie feature in the browser (Safa et al., 2016). Moreover, in a study conducted by Howah and Chugh (2019), it was found that end-users tend to trust potentially spyware-infected software when the risk is anticipated as less than the benefit of the software. Trust was found to be based on unawareness and over-confidence. In social engineering, trust is an imperative variable which is exploited.

Most of the participants noted that access controls and the measures put in place to protect sensitive and personal information existed. Four research participants (OAP 5, 6 and OBP 7, 8) were uncertain of such procedures. Those who responded positively (OAP 2, 3, 7, 8, 9; OBP 1, 2, 3, 4, 5, 6; OCP 1, 2, 3, 4, 5) were asked to elaborate on their responses and listed the use of an IT security policy, IP authentication, password-protected documents, authorization in terms of access, and encryption as part of their organization's access control procedures. OAP 8 specifically mentioned that their organization uses BitLocker. BitLocker is included with select editions of Windows Vista. It is an encryption feature installed on computers that prevents the transferring of documents onto an external hard drive unless an administrative password is inserted. It protects data by providing encryption mechanisms for entire volumes (Microsoft, 2009). This shared insight reinforces the notion that the workplace is still reliant on automated processes. Colaner (2020) argues that, as much as automation enhances cybersecurity, safety is inherently rooted in human nature. Human beings are at the forefront of cybersecurity – be it the perpetrators, naïve targets or change agents who actively and consciously guard against risks and threats. Furthermore, Colaner (2020) suggests that the function and effectiveness of automation is grossly overestimated and cannot be wholly depended on. OBP 2 and OCP 3 provided detailed contributions regarding the privacy policy in their organization. Their responses revealed the protocols put into place to police private and sensitive information. The participants seemed confident about these processes; however, sensitive information is still at risk from social engineering attacks. In 2017, Ethereum Classic Wallet fell victim to a social engineering attack. The wallet system serves the Ethereum Classic cryptocurrency – a type of cryptocurrency that runs smart contracts (Brook, 2017). Cryptocurrency or virtual currency is a type of decentralized virtual currency that enables direct transactions in the absence of a financial institution. Globally, cryptocurrencies are not recognized as legal tender in any jurisdiction (Reddy & Lawack, 2019). Social engineers impersonated the owner of the wallet and gained access to the domain registry to redirect the domain to their personal server. Consequently, these social engineers were able to steal thousands of dollars' worth of cryptocurrency (Brook, 2017). This example highlights that, despite policy policing privacy, social engineering risks continue to exist and evolve.

All the research participants (from Organizations A, B and C) shared that password management and network security were compulsory in their organizations. From the current sample, it appears to be common practice to exercise password management. Users have unique usernames and passwords, and passwords are complex and alphanumeric. In addition, users are required to change passwords on a regular basis and the same password cannot be reused. Technology is also configured to allow only authorized users to change passwords when the need arises. Most of the research participants (OAP 1, 2, 3, 4, 5, 6, 8 and 9) used electronic signatures (e-signatures), while only one (OAP 7) specified that he did not use an e-signature. All the research participants in Organizations B and C indicated that they made use of e-signatures.

As remote working continues to increase, the use of e-signatures is prevalent in the workplace. In South Africa, as in many other countries, legislation makes provision for the acceptance of e-signatures. The accepted examples of e-signatures include a typed name at the end of an e-mail,

a scanned image of a handwritten signature as well as a digital signature (Republic of South Africa [RSA], 2002). Wood (2010) explains that a signature is pragmatic and valuable as it is an illustrative mark used as a method of assurance that an object has been generated, approved or validated and that e-signatures serve the same purpose. However, Wood (2010) believes that e-signatures can be exploited through social engineering techniques to defraud the target. E-signatures can be easily copied if pasted into a Word Document or through a converted Portable Document Format (PDF). Furthermore, an e-signature that is handwritten and scanned to an e-mail address can still be copied. Thus, vulnerability is increased due to legislation accepting the legality of e-signatures and the ease in which they can be obtained. However, businesses can take specific steps to mitigate these risks by making use of digital signatures. A digital signature is a sub-category of an e-signature. It is an electronic expression attached to or associated with a document that is carried out by an individual with the intent to sign the document thus agreeing to its content (Whitman & Mattord, 2012). A digital signature as a mathematically authenticated encrypted message. Digital signatures enhance security as they ensure signer authentication, data integrity and non-repudiation. Signer authentication provides evidence of who signed or approved a document. Thus, a digital signature links the user's signature to a detectable entity. A digital signature maintains data integrity as it cannot be re-attached to another document. Non-repudiation is affected as verification of the sender cannot be contested (Wang, Shan, Chen, Zheng, Wang, Mingwei & Haihua, 2020).

To test whether the participants understood the concept of social engineering, they were asked to provide definitions. Most of the research participants (OAP 1, 2, 4, 7, 8, 9; OBP 1, 3, 6, 7; OCP 1, 2, 3, 4, 5) indicated that they understood social engineering and were able to substantiate their understanding of it. However, OBP 3 and 7 provided responses that displayed confusion regarding their understanding of social engineering. Three research participants (OAP 3, 5 and 6) indicated that they did not know what social engineering was, even though they work as an IT analyst, IT auditor and IT analyst respectively. This reveals that, even in IT-related fields, knowledge and awareness of social engineering may be inadequate. Once fundamental knowledge was established, the participants were provided with a series of hypothetical social engineering scenarios, based on the fundamental perspectives of social engineering, where their understanding of the topic under study was further questioned. This was done not only to extract hypothetical responses, but to also to create awareness of various types of social engineering attacks that can take place in a professional and personal capacity. Two hypothetical scenarios are highlighted below and are followed by the research participants' responses.

The Chief Financial Officer (CFO), of your company, whom you have never met before, is in another province. The CFO is known, by those who have had an encounter with him, for his high-pitched voice. One morning a man speaking in a high-pitched voice phone you, identifying himself as the CFO, and requests confidential financial information from you.

The hypothetical scenario posed above, illustrates a common social engineering technique – impersonation and ingratiation. Impersonation involves the conceptualization of a fictitious character who then plays out the role of this fabricated character with a victim (Ciampa, 2014). Provided with an advantageous prospect to gain favor with people of authority and power, a target might be willing to go out of their way to do something that they are not supposed to do. The target may fear that the fictitious person of authority will harbor ill feelings towards them and doubt their competency if they refuse (Frangopoulos, 2007). Most of the research participants (OAP 3, 5 and 6; OBP 1, 2, 3, 4, 5, 6, 7 and 8; OCP 1, 2, 3, 4 and 5) conveyed that they would seek authentication and permission before proceeding with the request. OAP 7 and 8 said that they would ask that the request be documented in e-mail. The responses showed that the organization have policies and procedures in place and that the staff members were aware of them. Although authentic and honest, OAP 2 and 9 revealed that they would give the information requested. OAP 9's elaborated that he would request the CFO to

confirm his identity fails to maintain adequate security. Although most of the participants reported that they would not adhere to the above request, when put in that situation, human nature is likely to comply with persuasive techniques.

Social psychology denotes that there are two routes to persuasion, namely, the “central” and “peripheral” route. Petty and Cacioppo (1986) outline this dual process model by advocating that communication is not always processed in the same way. The central route leans towards a systematic order and makes use of logical arguments to evoke a favorable response (Frangopoulos, 2007). This route allows the individual to think critically about the information received and to be swayed by the strength of its arguments (Petty & Cacioppo, 1986). The peripheral technique makes use of mental shortcuts, distraction techniques and peripheral cues to elicit favorable responses (Frangopoulos, 2007). Petty and Cacioppo (1986) argue that the peripheral route to persuasion is determined by superficial cues. Thus, rational objectives are misrepresented (Rusch, 1999).

You have been experiencing problems with your laptop and require urgent assistance. As such, you receive a phone call from a technician at desktop support who requests your login credentials to solve your problem.

Desktop support is a classic social engineering technique. Help desk and technical support personnel are trained to help end-users, which makes end-users good targets (Shaw, 2013). Although most of the research participants (OAP 1, 4 and 5; OBP 1, 2, 3, 4, 5, 6, 7 and 8; OCP 1, 2, 3, 4 and 5) declared that they would not share this information, OAP 2, 3, 7, 8 and 9 disclosed that they would provide their credentials to desktop support. Human logic often rests in the notion that complying with a successful request is dependent on providing a reason. In a seminal study done by social psychologist, Ellen Langer, this hypothesis was tested (Langer et al., 1978). Langer et al. (1978) conducted an experiment by trying to bypass the queue at a photocopy machine by phrasing the request in different ways. When a reason was provided, the request was granted 94 per cent of the time. Thus, it can be argued that it is logical to share the requested information when there is a need or a reason. Employees are often inundated with workloads and requests; thus, they easily fall victim to social engineering attacks.

From Practice to Theory: Towards A Multi-Inter-Trans-Disciplinary Social Engineering Protection Framework

Social engineering is multi-inter-transdisciplinary in nature, thus a protection framework guarding against social engineering attacks is needed. This framework is designed to be practically applicable and adaptable to businesses. The framework is based on the disciplines of criminology, security science, computer science, psychology and law, as well as literature and empirical data. In literature, frameworks regarding social engineering are mostly focused on the actual attacks involved and are thus not protective or multi-disciplinary in nature (cf. Mann, 2008; Mitnick & Simon, 2002; Mouton et al., 2014a; Mouton et al., 2014b; Nohlberg, 2008). Yaokumah, Walker and Kumah (2019) found that employee security training has positive effects on security behaviour. Consequently, this paper seeks to contribute to healthy and effective information security cultures by creating a protective and integrative MIT framework. The following figure illustrates the integrative MIT social engineering framework founded on the findings of a larger study conducted by Jansen van Rensburg (2017).

Figure 1. A Multi-inter-trans-disciplinary social engineering protection framework

(Jansen van Rensburg, 2017)

The MIT social engineering protection framework is categorized on three inter-reliant levels: fundamental, social and legislative controls. These levels are purposively designed to be user-friendly and easy to understand.

Fundamental Controls

The fundamental controls are based on the disciplines of criminology, security science and computer science. Social engineering is rooted in these disciplines and thus they form the most integral part of the framework. The fundamental controls are as follows:

- Evaluate a current information system

A current information system needs to be evaluated in terms of its effectiveness. Even if there is no formal system in place, this needs to be determined. The information security protection systems within the organization should be identified and assessed.

- Establish strengths and weaknesses

The security vulnerabilities should be established by determining the human and technical strengths that can be used to detect and deter social engineering attacks. Human strengths include the capacity of the personnel to detect, deter and withstand a social engineering attack. The capacity of an information system which can intercept a social engineering attack in the absence of human

involvement must be established and weaknesses should be identified in order to manage and minimize risk.

- Identify threats

The classification of threats allows the organization to determine the areas that present the greatest risks. Knowledge of social engineering attacks will enable the organization to adequately guard against them.

- Determine protection levels

An in-depth analysis of the organization's current measures to protect human and system vulnerabilities, while considering the potential threats, should be carried out. The protection levels should be evaluated in terms of the technology, identification and authentication processes, access control and the social engineering risks specifically relevant to the businesses.

- Conduct tests

Specialized and orchestrated testing of current systems should be done regularly to assess current levels of security accurately and an action plan, comprising improvement strategies must be designed to provide a return on the security investments identified.

Social Controls

The social controls are based on the psychological principles of social engineering and include the following:

- Monitor emotional well-being

As the human element involves psychological factors, such as desperation, fear, naivety and anxiety, which can play a key role in the success of a social engineering attack, it is important to monitor employees' well-being. These human vulnerabilities should be identified and taken into account when encountering any suspicious activity.

- *Mitigate social mechanisms*

Businesses should identify social mechanisms and develop countermeasures to guard against social engineering attacks. Psychological variables, such as trust, persuasion and compliance, should be examined and contextualized considering the businesses' circumstances.

Legislative and Policy Controls

The legislative and policy controls should be modelled on the host country's legislation.

- Know their rights and responsibilities

Businesses should be aware of their rights and responsibilities regarding the protection of their information. These rights and responsibilities should be documented in an information security policy that will guide and govern the way employees protect the businesses' information. There is a distinction between employees knowing and understanding their rights and responsibilities regarding

the organization's information security mechanisms in place as opposed to being vaguely familiar with them.

- Understanding policy and legislation

Knowing, understanding and adhering to legislation and policy regarding information security are vital for the longevity of any business. Businesses cannot expect their employees to be experts in legislative matters. An intentional effort should be made so that all employees understand and comply with legislation.

CONCLUSION, LIMITATIONS AND FUTURE RESEARCH

The study analyzed three local businesses situated in Tshwane, Gauteng Province, South Africa, concerning information security. Through group-administered survey, continuous engagement, and an informative presentation on information security and social engineering, an interactive learning process was achieved. This was done through the mutual exchange of knowledge. The instructive data received from each business were analyzed, interpreted and presented. The paper establishes that the regular use of online communication and the accessibility of personal information, in the absence of security awareness and understanding, increases the risk of social engineering attacks and information security breaches. Additionally, it recommends that employees should be well-equipped to guard against social engineering attacks through the implementation of a social engineering protection model. This model is based on three inter-reliant levels and can be integrated in the information security policy of organizations invested in having a healthy information security culture. The paper notes limitations in terms of sample size, however, the author postulates that the empirical case study offered rich insights particularly for a global audience that is still developing its information security protocols. Furthermore, the responses received from the research participants indicate that there is a need for more awareness, as well as training workshops. Further research would be able to assist in equipping the workplace with the relevant knowledge and specific understanding of social engineering and how to implement the best information security practices.

FUNDING INFORMATION

This research was funded by the University of South Africa (College of Law).

ACKNOWLEDGMENT

The author would like to thank those who participated in the study.

REFERENCES

- Ali-Kovero, J. (2020). *Protecting against social engineering attacks in corporate environment* [Unpublished Master's dissertation]. University of Jyväskylä, Jyväskylä, Finland.
- Bailette, P., & Barlette, Y. (2020). Coping strategies and paradoxes related to BYOD information security threats in France. *Journal of Global Information Management*, 28(2), 1–28. doi:10.4018/JGIM.2020040101
- Balle, L. (2016). *How do businesses use the internet?* Retrieved 14 June, 2016, from <https://smallbusiness.chron.com/businesses-use-internet-752.html>
- Bay, H., Tuytelaars, T., & Van Gool, L. (2006). SURF: Speeded Up Robust Features. In A. Leonardis, H. Bischof, & A. Pinz (Eds.), *Lecture Notes in Computer Science: Vol. 3951. Computer Vision – ECCV 2006*. Springer. doi:10.1007/11744023_32
- Benamati, J. H., Ozdemir, Z., & Smith, H. J. (2021). Information privacy, cultural values, and regulatory preferences. *Journal of Global Information Management*, 29(3), 131–164. doi:10.4018/JGIM.2021050106
- Blurke, J. (2020). *As working from home becomes more widespread, many say they don't want to go back*. <https://www.cnn.com/2020/04/24/as-working-from-home-becomes-more-widespread-many-say-they-dont-want-to-go-back.html>
- Brook, C. (2010). *Classic Ether Wallet compromised via social engineering*. Retrieved 1 December, 2020, from <https://threatpost.com/classic-ether-wallet-compromised-via-social-engineering/126657/>
- Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: Complex or simple? Research case examples. *Journal of Research in Nursing*, 25(8), 652–661. doi:10.1177/1744987120927206 PMID:34394687
- Chan, M., Woon, I., & Kankanhalli, A. (2014). Perceptions of information security in the workplace: Linking information security climate to compliant behaviour. *Journal of Information Privacy and Security*, 1(3), 18–41. doi:10.1080/15536548.2005.10855772
- Chen, P. S., Yen, D. C., & Lin, S. (2015). The classification of information assets and risk assessment: An exploratory study using the case of C-Bank. *Journal of Global Information Management*, 23(4), 26–54. doi:10.4018/JGIM.2015100102
- Chiblow, S. (2020). An indigenous research methodology that employs Anishinaabek elders, language speakers and women's knowledge for sustainable water governance. *Water (Basel)*, 12(11), 1–13. doi:10.3390/w12113058
- Chmura, J. (2017). Forming the awareness of employees in the field of information security. *Journal of Positive Management*, 8(1), 78–85. doi:10.12775/JPM.2017.006
- Cialdini, R. B. (2001). *Influence: Science and practice* (4th ed.). Allyn & Bacon.
- Ciampa, M. (2014). *Security awareness: Applying practical security in your world* (4th ed.). Cengage Learning.
- Colaner, S. (2020). *The persistent humanity in AI and cybersecurity*. Retrieved 17 November, 2020, from <https://venturebeat.com/2020/02/11/the-persistent-humanity-in-ai-and-cybersecurity/>
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative and mixed methods approaches* (4th ed.). Sage.
- Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, 70, 72–94. doi:10.1016/j.cose.2017.05.002
- Dutta, P. (2020). *5 Biggest data breaches of 2020*. Retrieved 15 September, 2020, from <https://securityboulevard.com/2020/08/5-biggest-data-breaches-of-2020-so-far/>
- Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017). Panning for gold: Automatically analysing online social engineering attack surfaces. *Computers & Security*, 69(August), 18–34. doi:10.1016/j.cose.2016.12.013
- Ernst & Young. (2017). *Path to cyber resilience: Sense, resist, react. EY's 19th Global Information Security Survey 2016-17*. Retrieved 4 October, 2021, from <https://eyfinancialservicesthoughtgallery.ie/global-information-security-survey-2016/>

Ernst & Young. (2019). *Is cybersecurity about more than protection? EY Global information Security Survey 2018–19*. Retrieved 12 July, 2020, from https://assets.ey.com/content/dam/ey-sites/ey-com/en_ca/topics/advisory/ey-global-information-security-survey-2018-19.pdf

Experian. (2020). *Experian South Africa data incident*. Retrieved 29 October, 2020, from <https://www.experian.co.za/fraudulent-data-incident>

Fouché, C. B., & Schurink, W. (2011). Qualitative research designs. In A. S. de Vos, H. Strydom, C. B. Fouché, & C. S. L. Delpont (Eds.), *Research at grass roots: For the social sciences and human service professions* (4th ed.). Van Schaik.

Frangopoulos, E. D. (2007). *Social engineering and the ISO/IEC 1799: 2005 Security Standard: A study on effectiveness* [Unpublished MA dissertation]. University of South Africa, Pretoria.

Gragg, D. (2003). *A multi-level defense against social engineering*. SANS Institute: As part of Information Security Reading Room. Retrieved 12 October, 2015, from https://www.sans.org/reading_room/whitepapers/engineering/

Gray, J. (1842). *An efficient remedy for the distress of nations*. Adam and Charles Black.

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 105–117). Sage.

Gunawardena, S., Kulkarni, D., & Gnanasekariyer, B. (2013). *A Steganography-based framework to prevent active attacks during user authentication* [Paper presentation]. 8th International Conference on Computer Science & Education, Colombo.

Hadnagy, C. (2011). *Social engineering: The art of human hacking*. Wiley.

Hadnagy, C. (2018). *Social engineering: The science of human hacking*. Wiley. doi:10.1002/9781119433729

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, 73, 102–113. doi:10.1016/j.cose.2017.10.008

Heartfield, R. L. G., & Gan, D. (2016). *An eye for deception: A case study in utilising the Human-As-A-Security-Sensor paradigm to detect zero-day semantic social engineering attacks* [Paper presentation]. 15th IEEE/ACIS International Conference on Software Engineering Research, Management and Applications, London, UK.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviours in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154–165. doi:10.1016/j.dss.2009.02.005

Howah, K., & Chugh, R. (2019). Do we trust the internet? Ignorance and overconfidence in downloading and installing potentially spyware-infected software. *Journal of Global Information Management*, 27(3), 87–100. doi:10.4018/JGIM.2019070105

Hunter, P. (2019). Remote working in research: An increase usage of flexible work arrangements can improve productivity and creativity. *EMBO Reports*, 20(1). Advance online publication. doi:10.15252/embr.201847435 PMID:30530631

International Business Machines (IBM). (2020). *Cost of data breach report 2020*. Retrieved 15 September, 2020, from <https://www.ibm.com/za-en/security/data-breach>

Jansen, H. (2010). The logic of qualitative survey research and its position in the field of social research methods. *Forum Qualitative Social Research*, 11(2), 11–32.

Jansen van Rensburg, S. K. (2017). *The human element in information security: An analysis of social engineering attacks in the greater Tshwane area of Gauteng, South Africa* (Unpublished PhD thesis). University of South Africa.

Junger, M., Montoya, L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, 66, 75–87. doi:10.1016/j.chb.2016.09.012

Kaul, P., & Sharma, D. (2013). Study of automated social engineering, its vulnerabilities, threats and suggested countermeasures. *International Journal of Computers and Applications*, 67(7), 13–16. doi:10.5120/11406-6726

Kelly, J. (2020). *Here are the companies leading the work-from-home revolution*. <https://www.forbes.com/sites/jackkelly/2020/05/24/the-work-from-home-revolution-is-quickly-gaining-momentum/#21925761848a>

- Kessler, S. R., Pindek, S., Kleinman, G., Anel, S. A., & Spector, P. E. (2020). Information security climate and the assessment of information security risk among healthcare employees. *Health Informatics Journal*, 26(1), 461–473. doi:10.1177/1460458219832048 PMID:30866704
- Kyobe, M. (2009). Factors influencing SME compliance with government regulation on use of IT: The case of South Africa. *Journal of Global Information Management*, 17(2), 30–59. doi:10.4018/jgim.2009040102
- Langer, E., Blank, A., & Chanowitz, B. (1978). The mindlessness of ostensibly thoughtful action: The role of “placebic” information in interpersonal interaction. *Journal of Personality and Social Psychology*, 36(6), 635–642. doi:10.1037/0022-3514.36.6.635
- Makanda, K., Vallent, T. F., & Kim, H. (2017). Remarks on National Cyber Security for underdeveloped and developing countries: Focused on Malawi. *American Journal of Engineering Research*, 6(7), 257–260.
- Mann, I. (2008). *Hacking the human: Social engineering techniques and security countermeasures*. Routledge.
- Marriott International. (2020). *Marriott International Notifies Guests of Property System Incident*. Retrieved 15 September, 2020, from <https://news.marriott.com/news/2020/03/31/marriott-international-notifies-guests-of-property-system-incident>
- Mertens, D. (2017). Transformative research: Personal and societal. *International Journal for Transformative Research*, 4(1), 18–24. doi:10.1515/ijtr-2017-0001
- Microsoft. (2009). *BitLocker drive encryption overview*. Retrieved 2 August, 2016, from [https://technet.microsoft.com/en-us/ITBPary/cc732774\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/ITBPary/cc732774(v=ws.11).aspx)
- Mitnick, K. D., & Simon, W. L. (2002). *The art of deception*. Wiley Publishing.
- Mouton, F., Leenen, L., Malan, M. M., & Venter, H. (2014a). Towards an ontological model defining the social engineering domain. In K. Kimpka, D. Whitehouse, T. Kuusela, & J. Phahlamohlaka (Eds.), *ICT and Society. HCC 2014. IFIP Advances in Information and Communication Technology* (Vol. 431). Springer. doi:10.1007/978-3-662-44208-1_22
- Mouton, F., Leenen, L., Malan, M. M., & Venter, H. S. (2014b). Social engineering attack framework. *Information Security for South Africa*, 1-9.
- Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, 59, 186–209. doi:10.1016/j.cose.2016.03.004
- Moyo, A. (2020). *Only 17 out of 54 African states have data privacy laws*. IT Web Business Technology Media Company. Retrieved 4 November, 2020, from <https://www.itweb.co.za/content/WnxEv4gon4qV8XL>
- Nohlberg, M. (2008). *Securing information assets: Understanding, measuring and protecting against social engineering attacks* [Unpublished DPhil Thesis]. Stockholm University, Stockholm, Sweden.
- Okumus, F., Van Niekerk, M., Koseoglu, M. A., & Bilgihan, A. (2018). Interdisciplinary research in tourism. *Tourism Management*, 69, 540–549. doi:10.1016/j.tourman.2018.05.016
- Olenick, D. (2020). *Experian breach in South Africa affects 24 million consumers*. Retrieved 29 October, 2020, from <https://www.bankinfosecurity.com/experian-breach-in-south-africa-affects-24-million-consumers-a-14862>
- Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health*, 42(5), 533–544. doi:10.1007/s10488-013-0528-y PMID:24193818
- Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Sage.
- Petty, R. E., & Cacioppo, J. T. (1986). *Communication and persuasion: Central and peripheral routes to attitude change*. Springer-Verlag. doi:10.1007/978-1-4612-4964-1
- Rao, R., & Ali, S. T. (2015). A desktop application to detect phishing webpages through heuristic approach. *Procedia Computer Science*, 54, 147–156. doi:10.1016/j.procs.2015.06.017
- Reddy, E., & Lawack, V. (2019). An overview of the Regulatory Developments in South Africa regarding the use of cryptocurrencies. *South Africa Mercantile Law Journal*, 31(1), 11–28.

Republic of South Africa (RSA). (2002). *Department of Justice. Electronic Communications and Transactions Act 25 of 2002. Published in the Government Gazette (23708)*. Government Printer.

Republic of South Africa (RSA). (2013). *Department of Justice. Protection of Personal Information Act 4 of 2013. Published in the Government Gazette (37067)*. Government Printer.

Rusch, J. J. (1999). *The “social engineering” of internet fraud*. Retrieved 9 January, 2016, from https://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm

Safa, N., & Maple, C. (2016). Human errors in the information security realm and how to fix them. *Computer Fraud & Security*, 16(9), 17–20. doi:10.1016/S1361-3723(16)30073-2

Safa, N. S., Von Solms, R., & Fitcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security*, 2016(2), 15–18. doi:10.1016/S1361-3723(16)30017-3

Salancik, G. R., & Pfeffer, J. (1977). An examination of need-satisfaction models of job attitudes. *Administrative Science Quarterly*, 22(3), 427–456. doi:10.2307/2392182

Saleem, J., & Hammoudeh, M. (2018). Defense Methods against social engineering attacks. In K. Daimi (Ed.), *Computer and Network Security Essentials* (pp. 603–618). Springer. doi:10.1007/978-3-319-58424-9_35

Schurink, W. J., Schurink, C. B., & Fouché, C. B. (2021). Thematic inquiry in qualitative research. In C. B. Fouché, H. Strydom, & W. J. H. Roestenburg (Eds.), *Research at grass roots: For the social sciences and human service professions* (5th ed.). Van Schaik.

Shaw, R. (2013). *Social engineering: A hacking story*. InfoSec Institute. Retrieved 11 May, 2020, from <http://resources.infosecinstitute.com/social-engineering-a-hacking-story>

South African Banking Risk Information Centre (SABRIC). (2020). *Experian Data Breach*. Retrieved 29 October, 2020, from <https://www.sabric.co.za/media-and-news/press-releases/experian-data-breach/>

Stock, P., & Burton, R. J. F. (2011). Human aspects of information security in organisations. *Sustainability*, 3, 1090–1113. doi:10.3390/su3081090

Strydom, H. (2011). Sampling in the qualitative paradigm. In A. S. de Vos, H. Strydom, C. B. Fouché, & C. S. L. Delpont (Eds.), *Research at grass roots: For the social sciences and human service professions* (4th ed.). Van Schaik.

Su, W., Xu, X., Li, Y., Martínez-López, F. J., & Li, L. (2018). Technological innovation: A case study of mobile internet Information Technology applications in community management. *Journal of Global Information Management*, 26(2), 193–203. doi:10.4018/JGIM.2018040109

Verizon Enterprise. (2018). *Data Breach Investigations Report*. Retrieved 18 August, 2018, from https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

Wang, F., Shan, G. B., Chen, Y., Zheng, X., Wang, H., Mingwei, S., & Haihua, L. (2020). Identity Authentication Security Management in Mobile Payment Systems. *Journal of Global Information Management*, 28(1), 189–203. doi:10.4018/JGIM.2020010110

Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security* (4th ed.). Cengage Learning.

Wood, A. F., & Smith, M. J. (2014). *Online communication: Linking technology, identity and culture* (2nd ed.). Psychology Press.

Wood, M. (2010). *Want my autograph? The use and abuse of digital signatures by malware*. Retrieved 7 April, 2018, from https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/digital_signature_abuse.pdf?la=en.pdf?dl=true

World Health Organization. (2020). *Coronavirus disease (COVID-19) pandemic*. Retrieved 9 September, 2020, from <https://www.who.int/emergencies/diseases/novel-coronavirus-2019>

Yaokumah, W., Walker, D. O., & Kumah, P. (2019). SETA and security behaviour: Mediating role of employee relations, monitoring and accountability. *Journal of Global Information Management*, 27(2), 102–121. doi:10.4018/JGIM.2019040106

Yin, R. K. (2009). *Case Study Research, Design and Methods* (4th ed.). Sage.