IT Security Trust Model — Securing the Human Perimeter

Ileen E. Van Vuuren

***Abstract*—There are numerous technical advances in the field of Information Security (IS). Despite the application of these IS technological controls, it is often not enough to address security issues due to the vulnerable human component. With a considerable amount of support in literature, there is no doubt that the human factor is a major weakness in preventing IS breaches. The true level of security in technology and process relies on the people involved in its use and implementation. Thus, human factors play an increasing role in securing computer information assets and therefore are detrimental to the security of an organization. One of the most prominent aspects of security, which is linked to humans, is trust. It is safe to presume that trust will play an important role in any IS environment and may influence security behavior significantly. In this paper the findings of a prior study, which focused on identifying human security elements, their relationship with, and consequently their influence on trust, are explored further. This paper builds upon the prior study of identified human security elements, which spawns IS trust factor elements of a previously proposed IT Security Trust (ITST) Model. Furthermore, the paper adapts and expands the original ITST Model, renamed to Information Security DNA Model, providing insight into and recommendations on how the trust factor elements may be utilized in an attempt to manipulate human behavior in such a manner to equip employees with the necessary behavioral attributes for combatting social engineering related attacks within organizations which choose to follow an IS model built on the foundation of trust.**

***Index Terms*—Information security, social engineering, human factor, trust factors, trust, smart trust, information security DNA model, IT security trust model.**

I. Introduction

Eggars, Hamill and Ali [1] argue that in today's competitive business environment, data has become the new currency of business. All IT organizations to an extent are data companies, custodians of large volumes of client, employee or personal information, which tends to be sensitive in nature. From a regulatory compliance perspective, the Protection of Personal Information – PoPI Act [2], has become ever so important within South African organizations.

Despite the advanced technological controls being implemented today by organizations, the human factor is still seen as a significant threat through channels of social engineering [3]. Hackers are constantly on the lookout for ways to gain access to valuable resources such as computer systems, corporate or personal information for personal or financial gain. Occasionally, information systems are breached due to genuine gaps in the security posture of the organization, but more than often, hackers succeed through exploiting human behavior, such as trust – being too trusting of others, or ignorance – being negligent or naive to the consequences of being careless with information. Most often, this is due to a lack of security awareness, misjudging the level of risk associated with certain human behavior. Social engineering relies on human error, the lack of security awareness, knowledge and understanding, and consequently security behavior to gain access to any system, despite the layers of defensive security controls implemented via software or hardware technology. It is argued that the implementation of IS policies, processes and procedures for guiding the implementation of IS controls are null and void if trust is not established. This is true because of the fact that trust is a human factor which influences the effectiveness of a human beings ability and willingness to comply with policies, processes and procedures in their work environment. The ultimate security perimeter is the human being, and if not protected, the gates are wide open for intruders to take advantage and gain unsolicited control.

Therefore it is valuable to further explore the ITST Model in an attempt to address the human factor of IS, as the human factor has a relationship with IS within organizations and trust factors have an influence on employee IS behavior.

According to Thomson and Von Solms [4], it is vital that human-social aspects of IS are addressed through security awareness training and education in order to change the mindset and behavior of employees in an organization. Leach [5] states that three key factors are necessary to improve employee behavior in IS. These factors are: 1) the behavior demonstrated by senior management and colleagues — role models demonstrating ability, integrity and benevolence, 2) the employees' security common sense and decision-making skills — knowledge, training and awareness, and 3) the strength of the employee's psychological contract with the company — trust, which together forms the foundation of the ITST Model.

The paper focusses on each of the trust factor elements of the ITST Model, expanding those elements and providing recommendations on how each trust factor can be implemented/addressed within an organization to derive value by allowing employees to naturally practice behavioral attributes that will enable them to fend against social engineering manipulation, hence securing the human perimeter of organizations against social engineering related attacks.

These trust factors were identified by means of an extensive literature study that was conducted together with themes derived from qualitative semi-formal interviews, and a quantitative online survey that was sent out to all IT

Manuscript received November 25, 2015; revised January 30, 2016. This work was made possible through a Masters by Dissertation Bursary Grant received from the University of South Africa.

Ileen E. Van Vuuren is with the Science, Engineering and Technology Department, School of Computing, University of South Africa, South Africa (e-mail: ileenvv@gmail.com).

employees of an IT retail service provider to 5 retailers situated in South Africa, with chain stores across Africa and in Asia. The survey focused on: 1) general security awareness, 2) awareness regarding security accountability, 3) existence/ absence of IS policy, process and procedure documentation, and most importantly, 4) perceived trust from an IS perspective. Results were consolidated and documented in a technical report that consisted of graphs, categorized according to research questions to be addressed, as well as themes that were identified. The research findings obtained served as input to identifying the elements of the ITST Model and are further utilized in this paper to assist with defining methodologies to follow for the practical implementation of each of the trust factor elements of the ITST Model by introducing an information security DNA (culture) to be adopted by organizations which choose to follow an IS model built on the foundation of trust, but within which security maturity and trust is considered to be relatively low.

The paper begins by discussing how social engineering has an impact on the human factor of IS, providing an overview of human security elements and their relationships to trust, which in turn spawn IS trust factor elements. Next, the paper defines trust from an IS perspective and provides a summary of related work in this field of study for setting the context. The paper proceeds by presenting the adapted and extended version of the ITST Model (IS DNA Model), providing recommendations on how each of the trust factor elements can be practically implemented to secure the human perimeter of IT organizations. Finally, the paper concludes by providing limitations of the IS DNA Model, as well as recommendations on how the research can be extended to further contribute and add to the existing body of knowledge.

II. Background and Related Work

A. Social Engineering and Its Relationship to the Human Factor of Information Security

Social engineering has become a popular channel for hackers to exploit the vulnerable human perimeter. Using a combination of social and technical trust relationships, the attacker can manipulate the trusted source to gain access to well-guarded applications and systems [6]. It should be noted that a vast amount of literature suggest technical controls to work more effectively than attempting to manage the human aspects of IS [7]. However, it is important to acknowledge that technology is not the only answer in addressing IS vulnerabilities and risks, but that the people aspect – employee behavior, attitudes and perception based on ability, integrity, knowledge, skills, benevolence; organizational aspects – culture of trust together with process play a vital role in protecting valuable company information assets from exploitation [8]. It is becoming more and more apparent that security failures are often due to issues other than the lack of suitable technical protection mechanisms. One of the most popular social engineering related techniques utilized to obtain private or confidential information from humans is phishing. For example, RSA Security [9], a well-established security company's network was breached in 2012 by an advanced attack which combined social engineering – falsely gaining the confidence of employees, with phishing, malware infected emails and privilege escalation, during which the attacker, posing as one of the targeted personnel, was able to use the network privileges obtained to gain access indirectly to highly secure parts of the network.

With the increased popularity of Bring Your Own Device and widespread use of smart devices in combination with its vulnerable internet, email and cloud storage capabilities, employees can unsuspectingly compromise both personal and organizational information stored and transmitted on these devices. Therefore, IS trust is no longer just an organizational and technological concept, but also a social and cultural aspect that extends beyond the boundaries of the traditional work environment and needs to be considered from an at home context within families, between spouse, between parent and child, as well as between individuals and social media platforms such as Twitter, Facebook and LinkedIn. The Internet and the Internet of Things (IoT) has become an integral part of every individuals work and personal life. Considering the billions of personal and work related e-mail messages that are transmitted annually worldwide, it is clear that phishing attacks form a significant part of day-to-day electronic communication activities and successful attacks may have a devastating effect on both enterprises and individuals [10]. With this in mind, it is safe to assume that social engineering techniques performed by educated hackers, exploit three main elements namely: 1) human factors, 2) organizational aspects, and 3) technological controls [11], together known as IS implementation elements.

B. Human Security Elements and their Relationship to Trust (Trust Factors)

In each of the IS implementation elements, human intervention is inevitable. Since humans are classified as the weakest link in IS, human-security elements spawn, such as accountability, leadership/employee behavior, visibility and transparency, knowledge and training, communication and collaboration, understanding and acceptance and most importantly, awareness, education and trust.

In order to promote trust between the human factor and technological controls, the elements of acceptance and understanding are required – TAM [12]. In order to promote trust between organizational aspects and technological controls, clearly defined roles and responsibilities and accountability for IS are required – employees in accountable roles need to practice certain leadership behavioral attributes in order to positively influence co-worker's and subordinate's perception of them, necessary to build strong trust relationships. The most prominent leadership behavioral attributes that need to be demonstrated by individuals in accountable roles include ability, integrity and benevolence [13]. Furthermore, in order to promote trust between the human factor and organizational aspects, self-trust and relationship trust together with IS awareness are required. Communication and collaboration, as well as visibility and transparency are necessary to promote awareness and relationship trust. In addition, communication and collaboration, together with knowledge and training are necessary to promote understanding and acceptance.

Furthermore, knowledge and training together with visibility and transparency are necessary to enable positive leadership behavior and perception, especially for employees in accountable roles.

Communication, collaboration, visibility and transparency together with knowledge sharing are dependent on trust and therefore the implementation of IS policies, processes and procedures for guiding the implementation of IS controls are null and void if trust is not established. As previously mentioned, this is due to the fact that trust is a human factor which influences the effectiveness of a human being's ability or willingness to comply with IS policies, processes and procedures in their work environment. Besides organizational trust, social trust also needs to be considered – humans are creatures of habit and if an IS culture of trust is not practiced at home in the same manner in which it is practiced in the work environment, it creates the opportunity for the manifestation of negligence and distrust.

As a result of the inter-trust relationships that exist between IS implementation and human security elements, it is safe to assume that trust will play a significant role in any IS environment as trust will probably improve IS and vice versa. Employees' perceived levels of IS and trust are closely related and therefore it is appropriate to consider human trust perceptions when dealing with social engineering and security awareness in the workplace and at home.

Fig. 1 below, presents the original ITST Model which depicts the human-security trust relationships that exist between the three IS implementation elements, each acting as both security control and vulnerability.

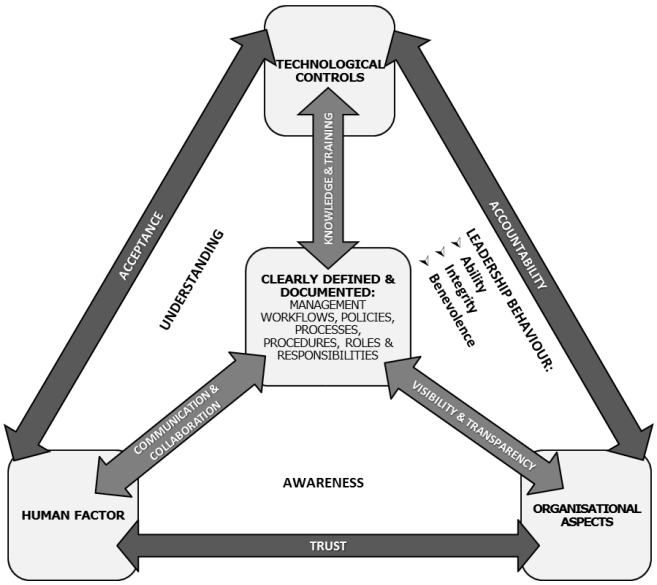

Fig. 1 Original proposed ITST model.

C. Trust

The concept of trust is widely used in many different research disciplines, such as marketing, psychology, information systems and strategic management [14]. As a result, even within the IS discipline, numerous research approaches are taken to study trust and trust relationships [15]-[19]. The variety of viewpoints on trust has also led to a plethora of definitions. Nevertheless, two critical components can be identified throughout the various definitions: 1) confident expectations and 2) a willingness to be vulnerable [20]. In addition, there are various similar definitions of trust. The Macquarie Online Dictionary [21] describes trust as "on whom or that on which one relies" whilst another online dictionary definition states it as "a confidence that something is safe, reliable, or effective" [22]. According to Kearney and Kruger [7], the key words revolve around confidence and reliability. If one is confident that something is safe, reliable and effective, there would be a higher level of trust in that matter. However, trust in this study refers to human nature of non-compliance and not the computational notion of trust. It also refers in this paper to the sense of security or security confidence employees have in their corporate environment, towards co-workers, subordinates and systems, i.e. the level of confidence an employee has in a co-worker or subordinate regarding IS, based on perception and as demonstrated through ability, integrity and benevolence, together with ability and skill demonstrated through the usage of various IS systems/ technological tools, which in turn requires knowledge and understanding. In the past, IS trust predominantly focused on compliance to IS standards, and controls as governed by well-known IS frameworks such as NIST SP800 and ISO 27001/2. Within this context trust was confined within the traditional work space. With the transformation of the organizational work environment, moving from the traditional work space to a virtual workspace based on the concept of anytime anywhere, enabled through the advanced technology of the digital era, IS trust is no longer confined to those traditional organizational boundaries, but also extends to the social and personal/home environment. IS trust in this paper therefore focusses on IS compliance from a social/cultural trust perspective, looking into the different dimensions of trust which extends beyond the organizational boundary. IS trust within this context refers to the sense of security confidence employees have in their interactions with social media platforms such as Twitter and Facebook at home and at work, but also the sense of security confidence or trust family members have towards each other, "giving their spouse or children the benefit of the doubt" for acting securely on the internet and smart devices, but with good judgement. It is argued, that if this culture of IS awareness, together with IS trust can be cultivated at home, especially in the early stages of children's development, it might significantly contribute to improving the default nature of IS behavior of future generation employees within organizations.

III. Adapted and Extended ITST Model: Proposed IS DNA Model

Fig. 2 below, depicts the newly adapted and extended ITST Model (IS DNA Model), which implements the IS trust factors, injecting it into the organization's culture by presenting a security DNA to be built into the organizations existing culture for driving the different dimensions of IS trust for compliance within the work environment, whilst encouraging similar behavior to be adopted at home. This model is applicable to organizations which choose to follow a security model built on the foundation of trust within which

the level of IS maturity and trust is considered to be relatively low.

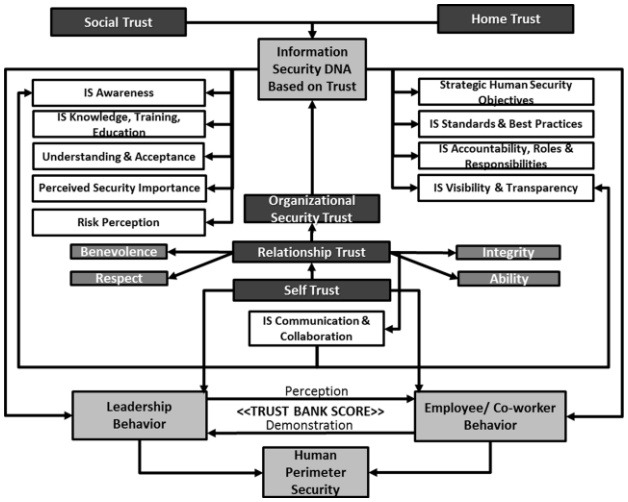

Fig. 2. Proposed IS DNA model — Adapted and extended from the ITST model.

A. Information Security DNA Based on Trust

According to Da Veiga and Elof [23], Information Security DNA, more commonly known as Information Security Culture, is defined as the "attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organization's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behavior evident in artefacts and creations that become part of the way things are done in the organizations to protect its information assets." According to Von Solms [24], the IS culture has to support the instructions and procedures of the organization so that IS will become a natural part of daily routines. Both Martins and Elof [25], and Von Solms state that IS culture can be consciously developed by directing employee behavior in the desired direction. The IS DNA Model is based on this concept and focusses specifically on trust factor elements, which is proven to have an influence on employee behavior, to direct that behavior into a favorable future state for IS within an organization to fend against social engineering and information system related attacks.

B. Information Security DNA Implementation

In order to implement an IS DNA within an organization, certain metrics need to be defined as a starting point, which entails understanding the current IS posture (as-is state) of the organization and then from there, document the target IS (to-be) state. Next, the to-be roadmap needs to be defined which explains what is required to move from the as-is state to the proposed to-be state for IS within the organization. To assist with planning the scope of each of the items on the to-be roadmap, it is recommended to make use of the SMART Goals Model [26] for preventing scope creep and staying focused. In addition, the Plan-Do-Check-Act (PDCA) ISO Model [27] may assist with following necessary procedures for the implementation of to-be items.

C. Low IS Maturity & IS DNA Trust Factor Elements

In order to obtain buy-in from management for the implementation of an IS DNA within organizations with low levels of trust and IS maturity, the strategic objectives/intent of the IS DNA Model must be clearly communicated. This in turn may require IS awareness, education and training in order to obtain understanding and acceptance of the IS DNA Model. IS awareness in an organization is the cornerstone of a security culture [28]. Employees will make mistakes; forget to log off, passwords are not changed, and stand the chance of being manipulated by social engineers. These are the realities of working in the digital era of information technology. The recognition of failures in security and the assurance that it is okay to make mistakes but that it needs to be reported is vital in the protection of an information system. This, together with consciousness of both internal and external risks, is important to drive behavior and thus have an influence on the security culture of an organization. Whilst IS awareness includes IS education and training as necessary components for driving IS behavior, IS awareness also requires behavioral adaptation to create the appropriate response to the protection of information in accordance with its value to the organization. In addition clearly defined IS principles need to be defined and communicated to provide guidance on IS strategy of the organization after buy-in has been obtained. Clearly defined and documented IS policies, processes and procedures are necessary together with clearly defined, documented and communicated IS roles of accountability and responsibility create visibility and transparency, necessary to promote an IS culture of trust.

Other elements that comprise security DNA, include perceived security importance and risk perception. IS knowledge and training are necessary to promote IS understanding and acceptance. In addition, decisions materialized through behavior are based on knowledge and the perception of the risk (or lack of perception in most cases). Furthermore, the types of security issues themselves and the impact of these are fundamental to awareness. Another vital aspect of awareness is breach identification and its consequences. The awareness by employees of the detection of information breaches and its consequences will influence how seriously individuals take their responsibility. If there are no apparent consequences for not monitoring and reporting breaches and behaving securely, the phenomena results in the creation of a relaxed attitude to security. Whilst using stringent security controls as a security measure is not recommended to changing behavior and attitudes as it could jeopardize trust relationships [29-30] if not properly managed, it can also be effective and should be one part of a multi-layered approach to security. The perception of lower risk means staff will ignore certain procedures and are more likely to circumvent those policies, procedures and controls. Poor IS compliance behavior in this regard might not be due to malicious intent; but merely to circumvent the process in order to work faster or more efficiently as the vast implementation of security controls tend to complicate matters. It is also argued that this tendency to by-pass IS compliance controls might be due to the fact that a lack of IS trust exist because of the lack of trust factor elements which has an influence on that trust relationship. Trust is a human factor which influences the effectiveness of a human being's ability or willingness to comply to certain standards and best

practices, therefore an IS cultural mind shift is required to change the perception of IS within the workplace, which might also cultivate positive IS behavior at home, if implemented correctly.

D. Dimensions of Trust

Self-trust: Self-trust is derived from personal ability and capacity to set and achieve goals and keep commitments [31]. In order to promote self-trust in specific IS activities, IS education in the form of knowledge gathering and formal training on that specific IS topic are necessary, together with management recognition for IS achievements to build a level of IS confidence. That inner sense of IS competency established through confidence, contentment and consistency then makes it possible to be worthy of the trust of others and consequently has an influence on relationship trust. The IS DNA Model aims to promote self-trust through establishing facilitated IS focus groups to encourage informal knowledge sharing activities, establishing an IS training program for certifying individuals on IS topics relevant to their work environment, establishing an IS Awareness program for educating employees during induction training and ongoing awareness campaigns, establishing a IS performance recognition program based on a points system to display a token of appreciation from management.

Relationship Trust: Relationship trust from an IS perspective, refers to the level of confidence an employee has within a co-worker or subordinate to perform an IS activity or work task and vice versa. This trust relationship is predominantly based on the level of competence/ability demonstrated by both parties as well as perception of one another, influenced by various factors and cultural norms, such as integrity, benevolence and respect. Relationship trust is essentially managed through virtual trust accounts that exist between individuals [31]. The IS DNA Model aims to promote relationship trust through similar means as discussed above for self-trust when improving competency and ability, but in addition will focus on creating awareness regarding human characteristics in addition to traditional awareness program material for IS which communicates that, if not given attention to, might negatively influence perceptions of one another and ultimately decrease virtual trust account scores, resulting in a lack of communication and collaboration required between IS implementation stakeholder parties. The IS awareness program will incorporate techniques on how employees can mitigate such negative human characteristics through practicing certain high-trust leadership behaviors discussed further in Section E of this paper.

Organizational Trust: When working with trusted employees, more can get done. Organizational trust is derived from alignment – having the organizations information systems, structures and rewards aligned with one consistent objective. When all these elements are aligned correctly, IS trust and trust in general grows [31]. When various elements are misaligned, trust is reduced. Therefore, it is imperative that the IS DNA is aligned with organizational culture, to promote organizational trust with IS in mind. The IS DNA Model aims to achieve this alignment through introducing three main enterprise IS principles, which requires buy-in and commitment from management for providing guidance and awareness on the strategic direction of IS within organizations which choose to follow an IS model built on the foundation of trust. The three principles are:

- Information Security is every employee's responsibility
- Information Security is a way of working and thinking
- Information Security is at all times to the best interest of the company and its employees

From the three principles, IS policies, standards, best practices and processes spawn to provide visibility and guidance required for promoting positive IS practices and behavior. The IS principles, policies, standards, best practices and processes, together with clearly defined roles, accountability and responsibilities will be communicated as part of the IS awareness and induction programs to create transparency of the IS DNA movement throughout the organization.

Social Trust and Trust at Home: Due to the merging of the traditional office space and home space as a result of technological advances such as the "Bring Your Own Device" initiative and "virtual office environments", IS trust is becoming a new important topic from a social platform and home interaction perspective. The ability to practice smart trust in this regard is vital to the IS well-being of individuals and organizations. Smart trust is based on the concept of finding the sweet spot between trusting everyone/everything blindly and being highly selective about who/what you trust [31]. Smart trust requires an individual to moderate and manage the amount of trust they extend to social platforms or to other individuals on a daily basis. The IS DNA Model aims to promote social trust and home trust by means of focusing on awareness and education of smart trust characteristics in the work environment, enabling employees to exercise sound judgment in a low-trust world by minimizing risk and maximizing possibilities. To exercise smart trust, the IS DNA Model will combine a high propensity to trust with equally high analysis [32]. Analysis in this context refers to an employee's ability to assess, evaluate, and consider implications and consequences, including risk. Smart Trust analysis involves the assessment of three vital variables: 1) opportunity — the situation within which trust is extended to someone/something, 2) Risk — the level of risk involved and lastly, 3) Credibility—the character and competence of the individual/ platform involved. The IS DNA Model will address the three variables for growing high-trust relationships by creating awareness among employees on 3 core beliefs during induction and training programs: 1) Every employee is worthy of being trusted, 2) Most people can be trusted – it plays out in organizational design, affecting systems, processes, structures and strategies and 3) Extending trust is a better way to lead – trust inspires employees to perform and ultimately leads to greater propensity to trust. The IS DNA Model approach is not built on the assumption that the organization requires more rules, more regulations, and more referees; it's built on the evidence that extending trust and creating a high-trust culture in which top performance is expected to bring significantly greater dividends for employees on every level within an organization.

E. Leadership Behavior, Co-worker/Subordinate Behavior and Trust

Little attention has been given to leadership behavior from a trust perspective and the influence it can have on co-worker/subordinate behavioral outcomes. Trust is the building block of social exchange and therefore influences relationship trust [33]. Leader-co-worker and leader-subordinate relationships require trust. Employees in leadership roles are considered trustworthy based on leadership behavior demonstrated through characteristics of conduct, integrity, ability to express interest/empathy for subordinate employees. [34].

Research indicates that trust, most specifically leadership trust, is a vital and viable component of organizational success [35]-[38]. Effective leadership trust is also based in exchange theory, which proposes that leaders and members create a mutual reciprocal relationship [39]. When subordinates trust a leader, they are willing to be vulnerable to the leader's action and vice versa—confident that their rights and interests will not be abused [40]. Leaders have a significant responsibility to increase co-worker and subordinate involvement to breed relationship trust. Honesty, for example, consistently ranks at the top of most individual's list of characteristics they admire in their leaders/co-workers/subordinates. From an IS DNA perspective, it is also important that leadership trust only exists if leadership is aligned with organizational and IS DNA values, which should demonstrate fairness amongst all employees, and does not exploit employees. When trust is broken, it can have serious adverse effects on a group's performance [41] and IS behavior. This finding was obtained in a prior study where there seems to be a significant correlation between the sum of trust factor scores (1.5 out of a possible total of 6) and level of human inflicted vulnerability experienced within the company under study [8]. The IS DNA Model aims to promote leadership behavior and co-worker/subordinate behavior, with a focus on trust factor elements by establishing a culture of security consciousness, constantly reminding employees, irrespective of their role to be deeply aware of how they think and behave and are perceived by others as being aware of their own and others' values/moral perspectives, knowledge, and strengths; aware of the context in character [42-45]. From a leadership perspective, this behavior is defined as Authentic Leadership [46]. Authentic leadership theory has advanced in previous studies as an approach to leadership that includes behaviors such as transparency [42], altruistic actions [47], and behavioral consistency [44], [48], all of which contributes to an IS culture of trust and consequently positive IS behavior.

IV. Discussion

This paper highlights the influence that trust and associated IS trust factors have on IS behavior. If IS behavior cannot be effectively controlled, it serves as a significant vulnerability within the human security perimeter. Malicious individuals thrive on taking advantage of the vulnerable human component, simply because it is much easier, and requires much less effort to hack a human through social engineering manipulation, than it is to hack a well-guarded information system. This paper utilizes the findings of a prior study, building upon the existing ITST model and providing recommendations on how it can practically be implemented within an organization in the form of an IS DNA Model, together with supporting IS initiatives, describing how to create IS awareness / consciousness among employees that will equip them with behavioral attributes and provide guidance on how to practice those attributes in such a manner that will enable the organization to secure its human perimeter from social engineering related attacks. For future studies, it would be valuable to extend this research by testing the IS DNA Model, to establish its perceived usability and completeness in various industries which choose to follow an IS model built on the foundation of trust in which IS maturity is perceived to be relatively low.

References

[1] W. D. Eggers, R. Hamill, and A. Ali. (2013). Data as the new currency: Government's role in facilitating the exchange. *Review of Deloitte*. [Online]. Available: http://deloitte.wsj.com/riskandcompliance/files/2013/11/DataCurrency_report.-pdf

[2] South Africa. (2013). Protection of personal information act, government gazette No. 37067:912 26 Nov. [Online]. Available: www.justice.gov.za/legislation/acts/2013-004.pdf

[3] K. Jansson and R. V. Solms, "Phishing for phishing awareness," *Behaviour and Information Technology*, vol. 32, no. 6, pp. 584-593, 2013.

[4] M. E. Thomson and R. V. Solms, "Information security awareness: Educating your users effectively," *Information Management and Computer Security*, vol. 6, pp. 167-173, 1998.

[5] J. Leach, "Improving user security behaviour," *Computers and Security*, vol. 22, pp. 685-692, 2003.

[6] G. Aaron, "The state of phishing," *Computer Fraud and Security*, vol. 2010, no. 6, pp. 5–8, 2010.

[7] W. D. Kearney and H. A. Kruger, "Considering the influence of human trust in practical social engineering exercises," *Information Security for South Africa (ISSA)*, pp. 1-6, 2014.

[8] I. E. van Vuuren, E. Kritzinger, and C. Mueller, "Identifying gaps in IT retail information security policy implementation processes," in *Proc. SDIWC InfoSec Conference*, 2015, pp. 126–133, South Africa.

[9] CSO. (2012). The 15 worst data security breaches of the 21st century. [Online]. Available: http://www.csoonline.com/article/2130877/data-protection/data-protection-the-15-worst-data-security-breaches-of-the-21st-century.html?page=2

[10] K. Jansson and R. V. Solms, "Phishing for phishing awareness," *Behaviour and Information Technology*, vol. 32, no. 6, pp. 584-593, 2013.

[11] E. D. Frauenstein and R. V. Solms, "Phishing: How an organisation can protect itself," in *Proc. Information Security South Africa (ISSA)*, pp. 253-268, Johannesburg, South Africa, 2009.

[12] E. D. Frauenstein and R. V. Solms, "Combatting phishing: A holistic human approach," *Information Security for South Africa*, 2014.

[13] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, vol. 13. no. 3, pp. 319-339.

[14] T. A. E. Ebert, "Facets of trust in relationships — A literature synthesis of highly ranked trust articles," *Journal of Business Market Management*, vol. 3, no.1, pp. 65-84, 2009.

[15] D. Gefen, E. Karahanna, and D. W. Straub. "Trust and TAM in online shopping: An integrated model," *MIS Quarterly*, vol. 27, no. 1, pp. 51-90, 2003.

[16] D. H. McKnight, M. Carter, J. B. Thatcher, and P. F. Clay, "Trust in a specific technology: An investigation of its components and measures," *ACM Transactions on Management Information Systems*, vol. 2, no. 2, pp. 12:11-12:25, 2011.

[17] D. H. McKnight, V. Choudhury, and C. Kacmar, "The impact of initial consumer trust on intentions to transact with a web site: a trust building model," *The Journal of Strategic Information Systems*, vol. 11, no. 3, pp. 297-323, 2002.

[18] M. Sȍllner, A. Hoffmann, H. Hoffmann, A. Wacker, and J. M. Leimeister, "Understanding the formation of trust in IT artifacts," in *Proc. the International Conference on Information Systems (ICIS) 2012*, Orlando, Florida, USA, 2012.
[19] W. Wang and I. Benbasat, "Trust in and adoption of online recommendation agents," *Journal of the Association for Information Systems*, vol. 6, no. 3, pp. 72-101, 2005.
[20] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Not so different at all: A cross disciplinary view of trust," *Academy of Management Review*, vol. 23, no. 3, pp. 393-404, 1998.
[21] (Nov. 20, 2015). Macquarie Dictionary. [Online]. Available: http://www.macquariedictionary.com.au
[22] (Nov. 20, 2015). Macmillan dictionary. [Online]. Available: http://www.macmillandictionary.com/dictionary/british/trust
[23] A. D. Veiga and J. H. P. Eloff, "A framework and assessment instrument for information security culture," *Computers and Security*, vol. 29, no. 2010, pp. 196-207, 2010
[24] B. V. Solms, "Information security — The third wave?" *Computers and Security*, vol. 19, pp. 615-620, 2000.
[25] A. Martins and J. H. P. Eloff, "Information security culture," *Security in the Information Society*, pp. 203-214, 2002.
[26] G. T. Doran, "There's a S.M.A.R.T way to write management's goals and objectives," *Management Review*, vol. 70, no. 11, pp. 35-36, 1981.
[27] *ISO Plan-Do-Check-Act Model*, ISO standard 14001. (2015). [Online]. Available: https://committee.iso.org/sites/tc207sc1/home/projects/published/iso-14001---environmental-manage/plan-do-check-act-model.html
[28] A. H. Williams, "What does security culture look Like for small organizations," in *Proc. the 7th Australian Information Security Management Conference*, pp. 48-54, 2009.
[29] S. Petronio, *Bondary of Privacy: Dialectics of Disclosure*, SUNY Press, New York: SUNY Press, 2002.
[30] S. Petronio and J. Reierson, "Regulating the privacy of confidentiality," *Uncertainty, Information Management, and Disclosure Decision: Theories and Application*, pp. 365-383, 2009.
[31] S. M. R. Covey and R. R. Merrill. The speed of trust: The one thing that changes everything. [Online]. Available: https://summaries.com/Platinum/The%20Speed%20of%20Trust.pdf
[32] Soundview executive book summaries. (2012). Smart trust — Creating prosperity, energy, and joy in a low-trust world. [Online]. 34(8). Available: http://www.gc.astd.org/Resources/Documents/Forums/Learning%20Leaders/execsummaries-smart_trust.pdf
[33] A. Hassan and F. Ahmed, "Authentic leadership, trust and work engagement," *International Journal of Social, Behavioral, Educational, Economic and Management Engineering*, vol. 5, no. 8, pp. 150-156, 2011.
[34] E. M. Whitener, S. E. Brodt, M. A. Korsgaard, and J. M. Werner, "Managers as initiators of trust: An exchange relationship framework for understanding managerial trustworthy behavior," *Academy of Management Review*, vol. 23, no. 3, pp. 513-530, 1998.
[35] H. Bracey, *Building trust. How to get it. How to Keep it, Taylorsville*, GA: HB Artworks, Inc., 2002.
[36] L. T. Csorba, *Trust. The One Thing That Makes or Breaks a Leader*, Nashville, TN: Thomas Nelson Publishers, 2004.
[37] K. T. Dirks and D. L. Ferrin, "Trust in leadership: Meta-analytic findings and implications for research and practice," *Journal of Applied Psychology*, vol. 87, no. 4, pp. 611-628, 2002
[38] D. E. Morgan and R. Zeffane, "Employee involvement, organizational change and trust in management," *International Journal of Human Resource Management*, vol. 14, no. 1, pp. 55-75, 2003.
[39] C. A. Rusaw, "The ethics of leadership trust," *International Journal of Organizational Theory and Behavior*, vol. 3, no. 3-4, pp. 547-569, 2000.
[40] L. T. Hosmer, "Trust: The connecting link between organizational theory and philosophical ethics," *Academy of Management Review*, vol. 20, no. 2, pp. 393-403, 1995.
[41] K. T. Dirks and D. L. Ferrin, "Trust in leadership: Meta-analytic findings and implications for research and practice," *Journal of Applied Psychology*, vol. 87, no. 4, pp. 611-628, 2002.
[42] B. J. Avolio, W. L. Gardner, F. O. Walumbwa, F. Luthans, and D. R. May, "Unlocking the mask: A look at the process by which authentic leaders impact follower attitudes and behaviors," *Leadership Quarterly*, vol. 15, no. 6, pp. 801-823, 2004.
[43] B. J. Avolio and W. L. Gardner, "Authentic leadership development: Getting to the root of positive forms of leadership," *Leadership Quarterly*, vol. 16, no. 3, pp. 315-338, 2005.
[44] W. L. Gardner, B. J. Avolio, and F. O. Walumbwa, *Authentic Leadership Theory and Practice: Origins, Effects and Development*, Oxford, UK: Elsevier Science, 2005.
[45] R. Ilies, F. P. Morgeson, and J. D. Nahrgang, "Authentic leadership and eudemonic well-being: Understanding leader-follower outcomes," *Leadership Quarterly*, vol. 16, no. 3, pp. 373-394, 2005.
[46] A. Hassan and F. Ahmed, "Authentic leadership, trust and work engagement," *World Academy of Science Engineering Technology*, vol. 80, no. 8, pp. 750-756, 2011.
[47] S. Michie and J. Gooty, "Values, emotions, and authenticity: Will the real leader please stand up?" *Leadership Quarterly*, vol. 16, no. 3, pp. 441-457, 2005
[48] A. H. Eagly, "Achieving relational authenticity in leadership: Does gender matter?" *Leadership Quarterly*, vol. 16, no. 3, pp. 459-474, 2005.

Ileen E. van Vuuren was born in 1989 and she holds a B.Tech degree in information technology through the University of South Africa, Pretoria in 2012. Van Vuuren is currently in the process of completing a MTech degree in information technology through the University of South Africa, specializing in the field of information security.

She is permanently appointed as an IT risk and security analyst at an IT retail service provider situated in Cape Town, South Africa, providing IT services to 5 retailers with chain stores across Africa and in Asia. Recent work was published in the 2015 SDIWC InfoSec conference proceedings titled: Identifying Gaps in IT Retail Policy Implementation Processes – Towards developing a secure IT enterprise built on trust.