Does Ubuntu Influence Social Engineering Susceptibility?

Ntsewa B. Mokobane, Reinhardt A. Botha

▶ **To cite this version:**

Ntsewa B. Mokobane, Reinhardt A. Botha. Does Ubuntu Influence Social Engineering Susceptibility?. 14th International Symposium on Human Aspects of Information Security and Assurance (HAISA), Jul 2020, Mytilene, Lesbos, Greece. pp.97-108, 10.1007/978-3-030-57404-8_8 . hal-03657723

HAL Id: hal-03657723
https://inria.hal.science/hal-03657723

Submitted on 3 May 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Does ubuntu influence social engineering susceptibility?

Ntsewa B Mokobane [0000-0003-1777-9682] and Reinhardt A. Botha#[0000-0002-6176-3007]

Center for Research in Information and Computer Security
Nelson Mandela University, South Africa
#reinhardta.botha@mandela.ac.za

Abstract. Ubuntu refers to living according to a set of values shared by people who believe in a certain way of life. The values of ubuntu include group solidarity, conformity, compassion, respect, human dignity, a humanistic orientation, and collective unity. Some people consciously live by ubuntu values while others do so unconsciously. Ubuntu is ingrained in human beings. The values of ubuntu in aggregate build trust, which inadvertently feeds into the social engineering approach used in information security attacks. Ubuntu appears to increase vulnerability to the success of a social engineering attack. Social engineering is a key threat to information security in many organizations. Social engineers target employees as human beings are naturally vulnerable.

This study argues that ubuntu influences the success of social engineering attacks. It views ubuntu as foundational in making humans vulnerable to social engineers. The values that ubuntu is based on lead humans to trust, conform, be compassionate and loyal, and desire to help others. Social engineers exploit these values to obtain information, which they use to breach the information security of the targeted organization. Because of ubuntu, the extensive work of building rapport and elicitation, which would otherwise have been exhausting, is already completed and ready to be exploited by the social engineer. This paper exposes the potential influence of ubuntu on social engineering attacks. It concludes that security awareness, education and training programmes must be adapted to counter these influences and safeguard information assets.

Keywords: Attitude, Subjective Norms, Behaviour, Elicitation, Ubuntu, Social Engineer, Social Engineering.

1 Introduction

Despite ever-improving technical information security measures, training, and awareness programmes, information security breaches still rage on [19, 16]. Technical measures cannot adequately protect information and ensure information security by themselves [16]. These technical measures are dependent on the users of the information asset. These users are the weakest link in information security efforts [8, 11]. Several factors are responsible for the weak nature of the human in information security. Some centre around the humanness of the users [19].

Ubuntu is a Zulu word that describes “a quality that includes the essential human virtues; compassion and humanity” [24]. However, it is often used in a more philosophical sense to mean "the belief in a universal bond of sharing that connects all humanity”. This paper investigates the influence of ubuntu on the success of social engineering attacks on information users. Social engineering in the context of information security

is the act of manipulating people into performing actions or divulging confidential information that can be used for a malicious purpose [14]. Social engineers target the ubuntu in the user and exploit the trust that humans have by nature to obtain specific information [30]. This information enables the social engineer to breach the target's information security. A social engineer is a person who uses deception to manipulate individuals into divulging confidential or personal information in order to gain unauthorized access to information and subsequently use that information for malicious purposes [12]. The theory of planned behaviour explains possible reasons why the social engineer easily triggers the ubuntu in the user.

This paper aims to analyze ubuntu and understand how it influences social engineering susceptibility. Ubuntu disarms the victim. It creates a blind spot in evaluating the security threat, as the level of security skepticism required to protect the information is overwhelmed by the values of ubuntu in the victim. Ubuntu influences one's attitude and how one reacts to a situation requiring action. Ubuntu's analysis is performed through the application of the theory of planned behaviour, which helps predict planned human behaviour. Understanding the impact of ubuntu on users' susceptibility to social engineering attacks will enable the development of more effective information security awareness and training programmes, specifically regarding defenses against social engineering attacks [2].

2 Human behaviour

Humans are active in nature. From time to time social and other activities require that they take action and behave in particular ways to socially fit and survive in their day-to-day lives [26]. Behaviour choices are motivated by immediate personal interest and wider social interest. The individual chooses the behaviour that is most beneficial [25]. Social evaluation of the behaviour either encourages or discourages individual behaviour [21]. There is always a balance between personal and social interests.

Ubuntu, demographics, culture, stereotypes, stigma, personality, moods, and emotions determine what an individual perceives to be the right balance between personal and social interests [5]. Human behaviour is a product of individual beliefs, how individuals evaluate the outcome of a certain behaviour, their perception of the social acceptance of the behaviour, their motivation to carry out the behaviour, and their ability to carry out the behaviour [9]. The attitude of an individual is formed by beliefs about and an evaluation of the behaviour outcome. In contrast, the perception of social acceptance of the behaviour and the motivation to implement the behaviour form the subjective norms [3].

In this paper, the theory of planned behaviour is applied to discuss and understand ubuntu and how it influences attitude as well as how the values of ubuntu influence subjective norms. Figures 1 to 5 show our attempt at explaining the influence of ubuntu on human behaviour through the application of different elements of the theory of planned behaviour. The relationship between ubuntu, some biases, social bond theory, and personality traits and their influence on attitude and subjective norms are illustrated through Ajzen [2]'s theory of planned behaviour.

3 Ubuntu

Ubuntu is a way of life, with pillars of personhood, humanity, humaneness, and morality [21]. Group solidarity, conformity, compassion, respect, human dignity, a humanistic orientation, and collective unity have, among others, been defined as key social values of ubuntu [22]. According to Metz [21], ubuntu promotes the spirit that one should live for others. Harmony, friendliness, and community are seen as great goods. According to ubuntu, one becomes a moral person insofar as one honours communal relationships [21]. Furthermore, a human being lives a genuinely human life to the extent that he/she prizes identity and solidarity with other human beings, and an individual realizes his/her true self by respecting the value of friendship [21].

The social values of ubuntu are engrained in human existence. People have always lived in groups and used to communicate around the fire, in city markets, in pubs, or in cafés [30]. Today social media has presented instant access to millions of people and individuals have new ways of interacting and fulfilling the ubuntu life philosophy.

The status of ubuntu as a golden thread and shared set of values has also allowed judges to feel at ease with freely applying ubuntu to new areas of law [15]. Figure 1 shows how ubuntu influences the behavioural beliefs of the individual and how the individual evaluates the outcome of a specific behaviour in a given situation. Behavioural beliefs together with an evaluation of the behaviour outcome determine the individual's attitude. The attitude is one element of behaviour intention.

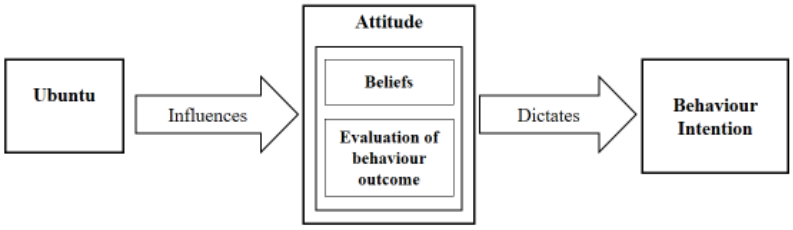

Fig. 1. Relationship between ubuntu, attitude, and behaviour intention [Author hypothesized relationship]

The values of ubuntu influence the worth of social agreement that specific reactions or behaviours are appropriate in a given situation. The individual who lives by ubuntu values always needs to comply with ubuntu values in their actions and inactions. Figure 2 shows the relationship between ubuntu values, subjective norms, and behaviour intention. Social pressure from family, friends, and others who matter to the individual urges the individual to behave and act in conformity with ubuntu values. The normative belief that an individual should comply with social expectations together with the desire to and confidence that one can live by ubuntu values form subjective norms [2].

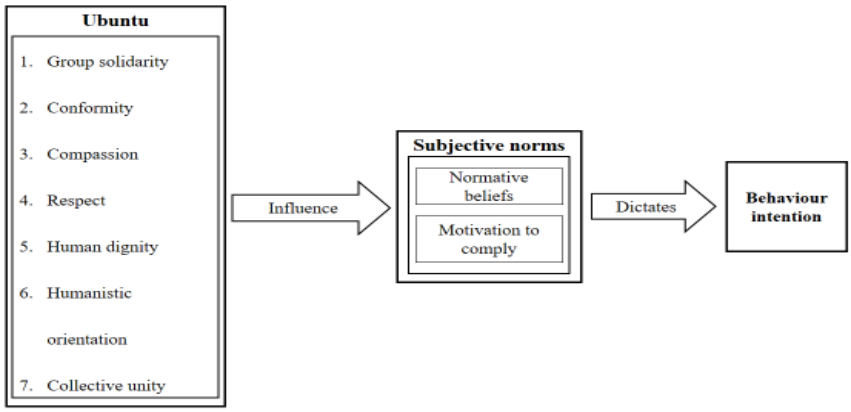

Fig. 2. Relationship between ubuntu values, subjective norms, and behaviour intention [Author hypothesized relationship]

The actual individual behaviour in a given situation is determined by factors such as predispositions, biases, traits, knowledge, ability, and skills. The values of ubuntu are some of the predispositions. Predispositions are important factors that influence an individual's emotions and behaviour [28].

Figure 3 outlines the bias ubuntu brings that influences the attitude of the individual in specific situations. Bias is a variable in the outcome evaluation and therefore sways the attitude towards, for example, the situation. Bias prevents the person from being objective [25]. Owing to the bias effect, people behave in particular ways because of how they feel rather than on a rational basis. People evaluate the outcomes of their behaviour through the frames of their bias.

Ubuntu engrains conformity, compassion, respect, human dignity, a humanistic orientation, and collective unity. These values bring the framing bias in that individuals evaluate their actions or respond to situations based on the question: "Will I still be respected if I behave in this manner or that manner?" Ubuntu brings the optimism bias in that the individual sees that behaving in a manner that is seen through the ubuntu value system confirms the humanness of the individual in the eyes of the group. It also brings the affect heuristic bias in that individuals choose how to behave based on the feelings of the group [25].

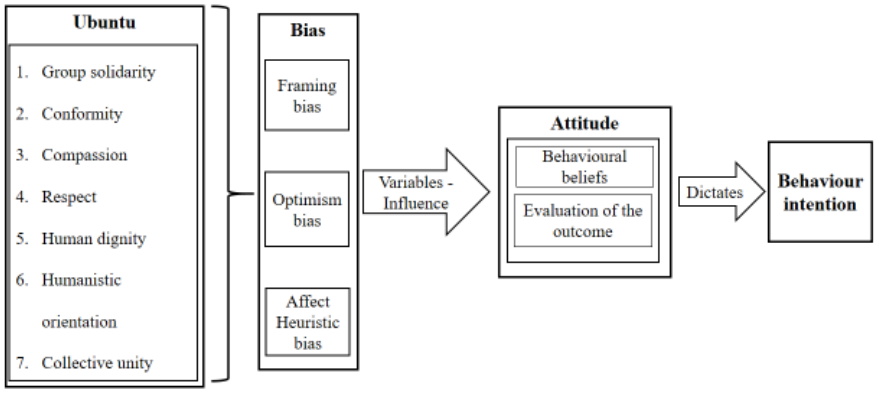

Fig. 3. Ubuntu controls attitude through bias [Author hypothesized relationship]

As indicated in Figure 2, the values of ubuntu influence a person's subjective norms. Subjective norms are determined by normative beliefs and the motivation to comply with social expectation to act in a particular way. Subjective norms are regulated by social acceptance [8]. Ubuntu promotes group solidarity, conformity, compassion, and collective unity [22]. The individuals within groups are socialized and conformity is promoted through bonds such as attachment, commitment, involvement, and personal norms [16]. Social bond theory postulates that when people build upon such bonds, their urge to indulge in antisocial or anti-establishment behaviours is reduced [16]. The gain from behaving in the ubuntu way is that it brings praise to the individual and respect to the group. People generally have the desire to help other people and the desire to be liked by other people [11, 13]. Figure 4 shows how the influence of ubuntu on subjective norms is catalyzed by the endowment effect, trust, and the agreeable trait found in individuals.

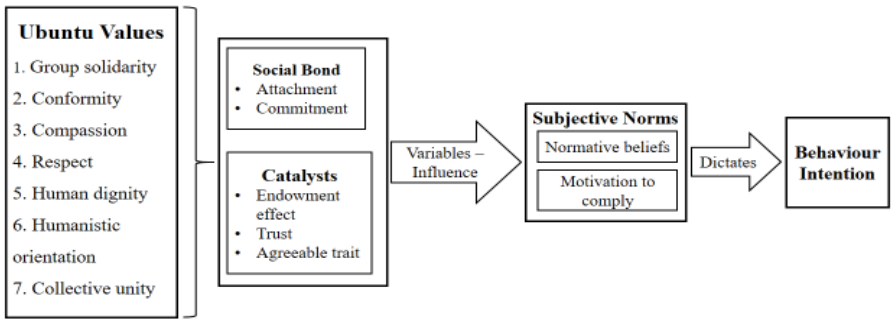

Fig. 4. Influence of ubuntu on subjective norms [Author hypothesized relationship]

Like all other human behaviour, the practicing of ubuntu values occurs when individuals believe they have control. Behavioural controls are determined by control beliefs and perceived power. Perceived behavioural control, as shown in Figure 5, is the perception of the ease or difficulty with which a task or behaviour can be performed [28].

Individuals with apparently high self-esteem become overconfident and take high behaviour risks. The underlying belief is that they are in charge and aware of the risks relating to behaviour [19].

Tendencies such as control bias give individuals an illusion of control. They believe they can control or influence outcomes that they clearly cannot [25]. People with high self-esteem are likely to be under an illusion of control and may unconsciously suffer from confirmation bias, which makes them believe that they are in control and are capable of behaving as expected and as required by their subjective norms.

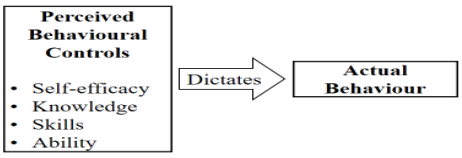

Fig. 5. Perceived behavioural control and actual behaviour [Author hypothesized relationship]

4 Social engineering

Social engineering is increasingly becoming a way of gaining unauthorized access to information systems networks [10, 18]. Social engineering in the context of information security can be defined as the act of manipulating people into performing actions or divulging confidential information that may be used for a malicious purpose [14].

Cybercriminals are turning to social engineering as organizations continue to build enough technical security that is difficult for criminals to compromise. Social engineers target employees' psychological makeup to obtain personally identifiable information that could enable them to breach the information security of the targeted organization [4]. Employees are susceptible to social engineering tricks, as criminals apply complex ways of hacking the human in the employee [20].

Figure 6 shows the steps followed during a social engineering attack [23]. The social engineering process intends to be deceptive in nature. The social engineer who follows the steps outlined in Figure 6 is likely to succeed in hiding his intentions. Attack formulation is the first stage, during which the goal of the attack and the target are identified. Information about the target is gathered from various sources and thoroughly assessed in the second stage. During the third stage, an attack angle is developed based on the assessment and analysis of the information. A relationship is developed during the fourth stage through communication and rapport building. In the fifth stage, the target is primed, information is elicited, and the attack is implemented. The sixth and final stage consists of aftercare and the closure of the attack assignment.

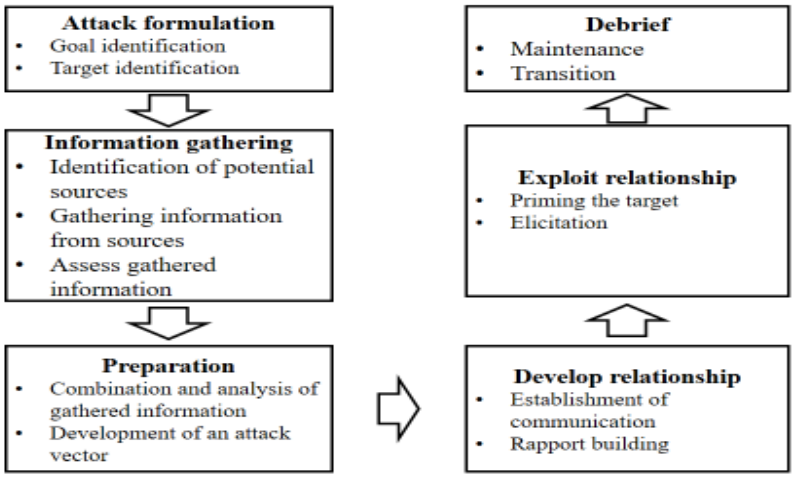

Fig. 6. Social engineering attack cycle [Mouton et al, 2016]

Social engineers use a variety of methods to compromise their targets. These methods may be classified as technical-based, social-based, and physical-based [1]. Technical-based attacks are conducted through the Internet via social networks and online services websites [31], while social-based attacks are performed through forming relationships with the victims in order to play on their psychology and emotions [17]. Physical-based attacks are physical actions performed by the attacker to collect information about the target [29].

5 Ubuntu and social engineering vulnerability

Ubuntu is of value to persons who believe in practicing it. People can live by ubuntu values either consciously or unconsciously. Ubuntu is seen in behaviour. Behaviour is governed by attitudes, predilections, prejudices, emotions, and mental background.

In many circumstances, mental efforts must be accomplished with such rapidity that the opportunity to apply the mind does not exist [5, 8]. Ubuntu, therefore, provides a point of reference for human behaviour in such situations. People's behavioural beliefs and the outcome evaluation of their behaviour are directly influenced by ubuntu. Ubuntu advertently builds trust between human beings. Table 1 illustrates the authors' integration of biases, traits, and ubuntu values that may have relevance to social engineering susceptibility.

While trust between human beings is a noble thing, social engineers exploit the human element of trust to obtain or compromise information about an organization or its computer systems [10, 13, 30]. The social engineering vulnerability resides with human behaviour, human impulses, and psychological predispositions [6]. People generally

have the desire to help other people as well as the desire to be liked by other people, especially strangers. Professionals want to appear well informed and intelligent. If they are praised, they will often talk more and divulge more information. Most people would not lie for the sake of lying, and most people respond kindly to those who appear concerned about them [12].

People are predisposed to trust and cooperate with other people [13]. Figure 7 shows how inherent ubuntu values expose humans as easy targets for social engineers.

Table 1. Comparison of ubuntu values and social engineering (SE) exploitable traits

SE exploitable trait	**Ubuntu values**	**Description of SE connection**
Trust	Group solidarity Conformity Respect	Social engineers develop trust with the target and then exploit that trust to obtain authorized information. Group solidarity, conformity, and respect consolidate trust between friends, associates, and families.
Attachment	Group solidarity Collective unity	Group solidarity and collective unity lead to attachment, which in turn consolidates trust. Social engineers exploit the trust.
Commitment	Collective unity	Collective unity builds trust between individuals. Social engineers exploit the trust.
Agreeableness	Humanistic orientation Compassion	Humans have trust instincts. Humans trust unless proven wrong. Social engineers exploit the trust.
Endowment effect	Respect	Ubuntu values are held in high regard. Individuals who exhibit them are trusted. Social engineers exploit the trust.
Heuristic effect	Compassion Respect Humanistic orientation	Compassionate individuals are respected and trusted. Such individuals are seen as human and therefore earn trust. Social engineers exploit the trust.
Framing bias	Group solidarity Collective unity	Being part of a group is valued among people with ubuntu and therefore consolidates trust. Collective unity is valued among people with ubuntu and therefore consolidates trust. Social engineers exploit the trust.
Optimism bias	Group solidarity Collective unity	Group solidarity and collective unity provide a sense of control, which in turn consolidates trust. Social engineers exploit the trust.

Halevi et al [13] identified five traits generally found in people. Firstly, neuroticism is a tendency to experience negative feelings, including guilt, disgust, anger, fear, and sadness. Neuroticism is likely to shape the attitude in the evaluation of the outcome of

the intended behaviour (Figure 1). People with this trait may tend to find comfort in group solidarity and collective unity, which are values of ubuntu. People with a high level of this trait are susceptible to irrational thoughts, are less able to control impulses, and do not handle stress well. This tendency increases a person's vulnerability to social engineering.

Secondly, people with a high level of the extraversion trait tend to be friendly and outgoing and enjoy interacting with people around them. Extraversion is likely to influence the intended behaviour through subjective norms, as illustrated in Figure 2. Extraversion appears to consolidate trust, which is central to the success of a social engineering attack, as shown in Table 1. It is ubuntu to be friendly to and interact with other people. This trait is also a vulnerability, as these people are welcoming to strangers and probably expose themselves to elicitation by social engineers.

Thirdly, people who score high on openness tend to be imaginative and intellectually curious. They also tend to be open to new and unconventional ideas and beliefs. Such people will likely fall into the trap of wanting to appear well informed and intelligent while inadvertently giving away confidential information or information required by social engineers. Openness is likely to influence the intended behaviour through attitude (Figure 1), motivation to comply (Figure 2), and perceived behavioural control (Figure 5). The exploitable traits in Table 1 could facilitate this influence.

Fourthly, highly agreeable people are co-operative, are eager to help other people, and believe in reciprocity. Agreeable people are by nature susceptible to elicitation by social engineers. Agreeable people practice the values of ubuntu, and this way of life builds exploitable trust.

Lastly, conscientious people have high levels of self-control and are very organized. They are typically purposeful and strong-minded. Their vulnerability to social engineering is likely to come from overconfidence. People with this trait who practice ubuntu are likely to overestimate their perceived behavioural control and engage in behaviours that have good ubuntu intentions but lead them into social engineering traps.

Online behaviour tends to mirror offline behaviour [7, 13, 27]. Therefore, ubuntu values lay the foundation for social engineering attacks, as trust is embedded in these values and social engineers exploit trust in human beings, as shown in Figure 7. The social engineer just needs to be a member or be seen as a member of the real or virtual community in order to build instant rapport and benefit from a social bond (e.g. attachment or commitment) with the target [16].

6 Conclusion

This paper analyzed human behaviour, ubuntu, social engineering, and the complementary relationship between ubuntu and social engineering attacks. Ubuntu can influence intended behaviour. Ubuntu is a likely source of human weakness in social engineering attack resistance. Social engineers who deliberately target ubuntu or its values are likely to succeed in the attack.

The paper identified the balance between personal and wider social interests as a determinant of actual behaviour. Ubuntu was identified as one of the factors that inherently influences individuals in determining what they perceive as the right balance between personal and social interests.

The paper demonstrated how ubuntu influences the behavioural beliefs of the individual and how the individual evaluates the outcome of a specific behaviour in a given situation. It further demonstrated the relationship between ubuntu values, subjective norms, and behaviour intention. Bias was discussed as a variable in the evaluation of the outcome of a behaviour. Bias prevents people from being objective in evaluating the outcome of the intended behaviour. The actual behaviour was found to be dependent on the actual or perceived ability, knowledge, and skills of the individual.

This paper concludes that ubuntu builds trust and interdependence between humans, which increases the victim's susceptibility to social engineering attacks.

This paper concludes that ubuntu and social engineering have a complementary relationship. Figure 7 illustrates the relationship between ubuntu and social engineering attacks as well as a possible point of disruption through security awareness, training and education (SATE) programmes. It is, however, acknowledged that the extent of the relationship is not known and further studies need to be done in order to establish the nature and extent of this relationship. In order to mitigate the influence of ubuntu in social engineering attacks, the social engineer's exploitation of ubuntu in the victim should be disrupted. The security awareness, training and education (SATE) programme is the tool used to protect access to ubuntu from the social engineer.

Further work is still required to determine how ubuntu could be factored into security awareness, training and education programmes and to develop an effective SATE framework to counter the influence of ubuntu on people's vulnerability to social engineering attacks. The general limitation of this paper is that empirical research is required to validate the conclusions.

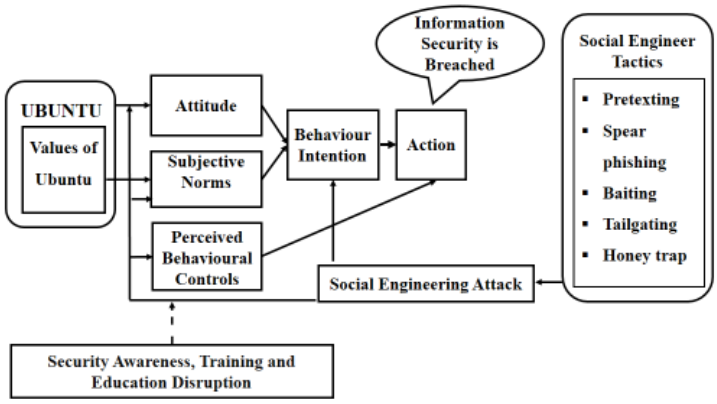

Fig. 7. Illustration of the interconnected relationship between ubuntu, the SE attack and prevention [Author hypothesized relationship]

References

1. Abraham S, Chengalur-Smith I (2010) An overview of social engineering malware: Trends, tactics, and implications. Technology in Society pp 183 – 196 DOI: 10.1016/j.techsoc.2010.07.001.
2. Ajzen I (1991) Organizational behaviour and human decision processes pp 179 – 211 https://doi.org/10.1016/0749-5978(91)90020-T
3. Ajzen I (2005) Attitudes, Personality and Behavior 2nd edition. McGraw Hill House, Maidenhead, Berkshire.
4. Aldawood H, Skinner G (2019) Reviewing Cyber Security Social Engineering Training and Awareness Programs: Pitfalls and On-going Issues. Future internet DOI: 10.3390/fi11030073.
5. Barnard C (1995) Decision processes as analyzed. Journal of Management History pp 4 - 112.
6. Conteh NY, Schmick PJ (2016) Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6 (23) http://dx.doi.org/ 10.19101/IJACR.2016.623006.
7. Campbell C (2019) Solutions for counteracting human deception in social engineering attacks. Information Technology and People pp 1130 – 1152
8. Donalds C, Osei-Bryson K (2020) Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. International Journal of Information Management pp 102056.
9. Fishbein M, Ajzen I (2010) Predicting and changing behavior. Taylor and Francis Group, Madison Avenue New York.
10. Flores WR, Ekstedt M (2016) Shaping the intention to resist social engineering through transformational leadership, information security culture and awareness. Computer and Security pp 26 – 44 https://doi.org/10.1016/j.cose.2016.01.004.
11. Gratian M, Bandi S, Cukier M, Dykstra J (2018) Ginther. A. Correlating human traits and cyber security behaviour intention. computers & security pp 345–358 DOI: 10.1016/j.cose.2017.11.015.
12. Hadnagy C (2011) Social Engineering. The Art of Human Hacking. Weiley Publishers, Indianapolis, Indiana.
13. Halevi T, Lewis J, Memon N (2013) A Pilot Study of Cyber Security and Privacy Related Behaviour and Personality Traits. International World Wide Web Conference Committee pp 13 – 17.
14. Hatfield JM (2018) Social engineering in cybersecurity. The evolution of a concept. Computers and Security pp 102 – 113.
15. Himonga C, Taylor M, Pope A (2013) Reflections on judicial views of ubuntu http://dx.doi.org/10.4314/pelj.v16i5.8
16. Ifinedo P (2014) Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. Information & Management pp 69–79 https://doi.org/10.1016/j.im.2013.10.001.
17. Junger M, Montoya L, Overink FJ (2017) Priming and warning are not effective to prevent social engineering attacks. Computers in Human Behaviour pp 75 – 87.
18. Kaur R, Singh S, Kumar H (2018) Rise of spam and compromised accounts in online social networks. A-state-of-the-art review of different combating approaches. Journal of Network and Computer Applications pp 53 – 88.

19. Kearney WD, Kruger HA (2016) Can perceptual differences account for enigmatic information security behaviour in an organization? Computers & Security pp 46–58 DOI: 10.1016/j.cose.2016.05.006.
20. Krombholz K, Hobel H, Huber M, Weippl E (2015) Advanced Social Engineering Attacks. Journal of Information Security and Applications pp 112 – 122.
21. Metz T (2011) Ubuntu as a moral theory and human rights in South Africa http://www.scielo.org.za/pdf/ahrlj/v11n2/11.pdf.
22. Mokgoro YJ (1997) Ubuntu and the law in South Africa https://journals.assaf.org.za/per/article/view/2897.
23. Mouton F, Leenen L, Venter HS (2016) Social Engineering Attack Examples, Templates and Scenarios. Computers and Security pp 186 – 209 DOI: 10.1016/j.cose.2016.03.004.
24. Oxford University Press (1998) Ubuntu https://en.wikipedia.org/wiki/Oxford_Advanced_Learner's_Dictionary
25. Pfleeger SL, Caputo DD (2012) Leveraging behavioural science to mitigate cyber security risk. Computers & security pp 597 – 611.
26. Popescu G (2014) Human behavior, from psychology to a trans-disciplinary insight. Social and Behavioral Sciences pp 442 – 446.
27. Rosen D, Stefanone MA, Lackaff D (2010) Online and Offline Social Networks: Investigating Culturally-Specific Behaviour and Satisfaction. Proceedings of the 43rd Hawaii International Conference on System Sciences DOI: 10.1109/HICSS.2010.292.
28. Safa NS, Sookhak M, Von Solms R, Furnell S, Ghani NA, Herawan T (2015) Information security conscious care behaviour formation in organizations. Computers & Security pp 65 – 78.
29. Salahdine F, Kaabouch N (2019) Social engineering attacks: A survey. Future internet DOI: 10.3390/fi11040089.
30. Tayouri D (2015) The human factor in social media security. Combining education and technology to reduce social engineering risks and damages. Procedia manufacturing pp 1096 – 1100 https://doi.org/10.1016/j.promfg.2015.07.181.
31. Vishwanath A (2017) Getting phished on social media. Decision Support Systems, 103, 70 – 81 https://doi.org/10.1016/j.dss.2017.09.004.