The Social Engineering Personality Framework

Sven Uebelacker
Hamburg University of Technology
Security in Distributed Applications
21071 Hamburg, Germany
Email: uebelacker@tuhh.de

Susanne Quiel
Hamburg University of Technology
21071 Hamburg, Germany
Email: susanne.quiel@gmx.de

***Abstract*—We explore Information and Communication Technology (ICT) security in a socio-technical world and focus in particular on the susceptibility to social engineering attacks. We pursue the question if and how personality traits influence this susceptibility. We use Cialdini's principles of influence to categorise social engineering attacks. First we show with a comprehensive literature review how existent research approaches social engineering susceptibility.**

Based on this review we construct suggestions for plausible relations between personality traits of the Five-Factor Model (Big 5) and the principles of influence. We propose our – at this stage theory-based – "Social Engineering Personality Framework" (SEPF) which we will evaluate in future empiric research. The characteristics of victims' personality traits in the SEPF will support and guide security researchers and practitioners in developing detection, mitigation, and prevention strategies while dealing with human factors in social engineering attacks.

I. Introduction

One of the biggest challenges nowadays in security research is in how to deal with human factors as a pervasive issue. Besides the fact that over decades extensive research was conducted in the disciplines of Information and Communication Technology (ICT) security, data protection, and privacy, the main work focused predominantly on the digital and physical domain, e.g. entering premises protected by access control systems (physical) or accessing servers guarded by firewalls (digital). Recent developments – like in cloud infrastructures (Where is my server located?) or in "Bring Your Own Device" (Mixing personal and business use cases) – blur the once established security borders and bring traditional, domain-specific security measures to its knees. Socio-technical security and risk management spotlight the social domain as a potent threat and approaches all three domains holistically. That is, organisational procedures for detection, mitigation, and prevention need to be adapted accordingly.

Social attacks (also known as Social Engineering (SE)) are exploiting the social domain, thus, its targets are members of an organisation: they pose with their insider knowledge a threat for organisational security. The notion of "insiderness" defined by Probst et al. [1] gives insight to which extent an insider has access to locations or assets as attack-worthy resources ("reachability") in order to assess insider threats. In this regard, we examine which factors contribute to facilitate these attacks to gain insider knowledge.

Coping with employees as an asset leads to different views on security measures. A manager can possibly disclose more valuable information than a cleaning worker. However, one single person in an organisation who gives an attacker information – no matter how insignificant it may appear – suffice to compromise systems or access confidential data.

In the next sections we will sketch SE as well as provide our methodology and research questions followed by an overview of the rest of this paper.

A. Social Engineering

Influencing and manipulating persons to reveal sensitive information or granting access to restricted areas is widely known as Social Engineering (SE). Surveys, like Verizon's "Data Breach Investigations Report 2012" [2], state that SE threatens not only companies and government agencies, but also individuals (mostly regarding identity fraud). Recent incident showed that Snowden persuaded multiple colleagues successfully to obtain login credentials of NSA accounts in Hawaii leading to the disclosure of sensitive information [3].

Hadnagy [4] defines SE as "the act of manipulating a person to take an action that may or may not be in the target's best interest. This may include obtaining information, gaining access, or getting the target to take certain action". Schneier [5] says about SE that it bypasses every digital and physical security feature. SE attacks can be conducted face-to-face or using ICT: in the latter case the attacker can automate malicious attempts and lower attacking costs, e.g. by sending phishing e-mails – exploitation via the digital domain [6], [7], [8], [9], [10]. Phishing attacks are extremely well researched in many experiments such as in an university environment [6], the individual vulnerability [9] or how to understand phishing victims [10], and the susceptibility related to their personality [8].

Concerning sensitive information gathered via social networks, Huber et al. [11] introduce an attack called "automated social engineering", where bots are used to collect information freely available in a social network, and to directly contact people via social networks to elicit information. Technique

This is the accepted version of our STAST workshop paper published by IEEE under DOI 10.1109/STAST.2014.12.

propagation [12] can be applied on automated SE attacks as well taking the attack frequency to a new level.

Many authors explicitly include the exploitation of human traits like trust and emotions in their research of SE malware [13], user privacy-education [14] or vulnerability to SE in general [15].

B. Methodology / Research Questions

Our methodology at this stage is a theoretical, positive research approach which we intend later on to validate with and ground on empirical data.

In this paper we focus on human targets (employees) and exclude attacker profiling. Successful SE attacks are determined by the victim's ability to resist the manipulation, by detecting it, and/or behaving in a attack-coping manner. Thus, we put our research questions: why do employees succumb to SE attacks in general? Does the susceptibility to SE differ between employees according to their personality traits? Our approach discusses personality traits as one influential factor. Others, like the influence of organisational culture and cultural background [16], situational conditions, gender and age, or attacker-target-relation [17], are not considered at this stage but will be observed in future studies.

As a first step we conducted a comprehensive literature review on SE presented in section III-A. Section IV constructs our Social Engineering Personality Framework (SEPF) by refining the literature review. It suggests research proposals for hitherto untried relations. We close in section V with an outlook for getting a glimpse of our research agenda. But first, we introduce Cialdini's work on persuasion (section II) followed by an introduction to personality traits (section III) on both of which our developed framework relies.

II. Psychology of Persuasion

Most appraisals and decisions in daily life base on heuristics to reduce cognitive load by incompletely analysing each situation. [5], [18]. However, similar to risk perception, these heuristics are not suited to every situation and can be exploited. The Dual Process Model of Persuasion [19] defines two different ways how we process information: the peripheral route or heuristic processing via intuition (system 1) and the central route via reasoning (system 2) (cf. [18]). Attackers can target both systems. Having this in mind, countermeasures – like awareness trainings – should address this accordingly.

An attacker can influence the decision-making process to her favour. Research exists for influential factors in decision-making, e.g. strong affect, lack of motivation, lack of personal relevance of the topic, lack of knowledge about a topic, lack of cognitive ability to process a message, lack of time, cognitive comfort due to trust, and communication modes where the influence agent is salient [7], [20], [21], [19], [22].

In marketing Cialdini deduced six principles of influence by experimental and field studies. To demonstrate that Cialdini's principles are applicable in context of SE, we refer to the findings of Scheeres [15]. He compares Cialdini's principles of influence with Gragg's psychological triggers [23], which are explicitly referred to as being utilised by SE attacks. Based on Scheeres' findings [15] we use Cialdini's psychology of persuasion as a theoretical basis for SE.

The six principles consist of:

Authority. Most people comply to authorities (cf. Milgram experiments [24]), even if they persuade them to act against their beliefs and ethics. It also works for symbols of authority, e.g. uniforms, badges, and titles or in telephone conversations where authority can easily be claimed. Two types of authority exist: one based on *expertise* and one relying on the relative *hierarchical position* in an organisation or society [19].

Commitment & Consistency. Commitment is an act of stating what one person thinks he is and does, while consistency makes that same person behave consistently according to his or her commitments and beliefs revealing a a highly successful influence principle [19].

Reciprocity. A strong social norm that obliges us to repay others for what we have received from them. Relationships rely and societies are built on it. Reciprocity helps establishing trust with others and refers to our need for equity. The power of reciprocity can be so high that the target would return an even greater favour than what was received.

Liking. "If you make it plain you like people, it's hard for them to resist liking you back" [25]. We prefer to comply with requests from people we know and like due to the fundamental motive to create and maintain social relationships. Perceived similarity enhances compliance as it can originate from a potential friend. These can be as superficial as shared names or birthdays.

Social Proof. Besides adapting beliefs and behaviour of people around in order to become socially "accepted", social proof also implies higher trust levels towards people who share alike opinions, especially in ambiguous situations.

Scarcity. We assign more value to less available opportunities due to a short-cut from availability to quality. Moreover, if something becomes scarce, we sense losing freedoms. Reactance Theory [26] suggests that we respond to scarcity by wanting to have what has become rare more than before. Even information with limited access persuades better.

III. Personality Traits influence Psychology of Persuasion

In psychology, personality is defined as a person's relatively stable feelings, thoughts, and behavioural patterns. These are predominantly determined by inheritance, social and environmental influence, and experience, and are therefore unique for every individual [27]. The most common classifications try to extrapolate as few statistically independent dimensions as possible.

Each dimension is labelled as personality trait and defined as relatively stable disposition that manifests across situations and specific time spans. The Five-Factor Model (FFM), also known as the Big 5 [27], has established itself a widely used and extensively researched approach. It is best suited to ICT security because its generalisable taxonomy permits its use across research disciplines. Moreover, the behavioural patterns

associated with its factors are extensively researched [28] (first FFM classifications appeared in the 1950s [27]). Validated questionnaires of various depth exist [29]. We use McCrae and John's introduction to the FFM from 1992 [27].

The FFM consists of five broad, empirically derived personality dimensions or traits, which split in several subtraits and are used across research areas with high validity: these traits are defined as **Conscientiousness** which focus on competence, self-discipline, self-control, persistence, and dutifulness as well as following standards and rules. **Extraversion** comprises positive emotions, sociability, dominance, ambition, and excitement seeking. **Agreeableness** includes compassion, cooperation, belief in the goodness of mankind, trustfulness, helpfulness, compliance, and straightforwardness. **Openness** to experience encompasses as a preference for creativity, flexibility, fantasy as well as an appreciation of new experiences and different ideas and beliefs. **Neuroticism** describes the tendency to experience negative emotions, anxiety, pessimism, impulsiveness, vulnerability to stress, and personal insecurity.

A. Personality impacts Susceptibility to Social Engineering

To analyse how personality traits influence the susceptibility to SE we conducted a comprehensive literature review as follows.

Based on their motivational systems [30] people with high values in extraversion are motivated by rewards and social attention. High values in agreeableness correspond with communal goals and interpersonal harmony. Conscientious individuals are motivated by achievement, order, and efficiency. People with high values in neuroticism are sensitive to threats and uncertainty, while openness corresponds with creativity, innovation, and intellectual stimulation [30]. Three out of five personality traits (Conscientiousness, Extraversion, and Openness) show both increased and decreased susceptibility to SE depending on context and sub-traits. Agreeableness increases and Neuroticism decreases susceptibility. The literature research pertaining to these findings will be subsumed for each trait as follows.

Conscientiousness. Continuance commitment, which is related to conscientiousness, increases SE vulnerability [7]. For instance, although people are concerned about their personal information, they are willing to trade-off privacy for convenience in return for a positive cost-benefit association to the advantages of perceived rewards [7]. Opposed to this, Darwish et al. [10] state in their survey of recent studies about phishing attacks and related backgrounds of victims that conscientious people present a lower rate of security risk if they are more mature and show respect for standards and procedures. Parrish et al. [8] argue that this applies only to standards and procedures that are existent as well as communicated. They also declare that security trainings can decrease SE susceptibility especially strongly for conscientious individuals [8]. This is supported by research from Sagardo et al. [31] where low levels of conscientiousness predict deviant workplace behaviour such as breaking rules or generally behaving irresponsibly. That is, people with lower values are breaking rules more likely if attacked by a social engineer.

Extraversion. Extraverted individuals are becoming a higher security risk [10]. Extraverted persons are also more likely to violate cyber-security policies, thus, accepting to disobey policies in order to comply to (malicious) requests [32]. Workman [7] investigated the effect of different types of commitment to SE susceptibility. He ascertains that people with high affective commitment as well as high normative commitment are more likely to fall prey to SE attacks. Both types of commitment relate significantly to extraversion [33]. Weirich and Sasse [34] report that employees who did not disclose their passwords, thus showing a low level of SE susceptibility, are regarded as unsociable and loners by their colleagues, which implies low extraversion values. Controversially, Cialdini et al. [35] show that people who are rated low on the preference-for-consistency-scale, thus being less vulnerable to commitment-and-consistency-techniques, present a greater extraversion.

Agreeableness. "Agreeableness is possibly the personality trait that is most associated with it [phishing]" and in a greater scope SE [8]. More agreeable individuals are at a higher rate of security risk [10]. Generally, younger people and women present higher values of agreeableness [10], thus explaining some of the demographic differences found in phishing susceptibility. The relation between agreeableness and SE susceptibility is assumed to be mostly established by trust, a sub-trait of agreeableness. This was shown in studies by Weirich and Sasse [34] as well as by Workman [7]. In the latter study, high normative commitment (see "Extraversion") show increased SE vulnerability. It significantly relates to agreeableness just like to extraversion [7], [33] and other subtraits (altruism, compliance) are directly targeted by social engineers [8]. Sagardo et al. [31] contradict these findings: low levels of agreeableness predict deviant workplace behaviour such as breaking rules. This can hint at some interaction or constructional problem that should be examined in the future.

Openness to Experience. People with high openness values are less concerned about privacy problems associated with location-based services [36]. These people's tendency to seek new experiences influences their risk evaluation [36]. This can be conveyed to SE that open individuals underestimate the risk of becoming a target and subsequently do not develop adequate coping strategies. Controversially, more open individuals are less likely to violate cyber-security policies [32]. However, this effect is contradicted when personality is not evaluated as direct influence but as a moderating factor. In this case, open individuals have been found to be more likely to violate cyber-security policies [32].

Neuroticism. More neurotic individuals are less likely to violate cyber-security policies [32]. People low on self-images and with self-admitted paranoia are more probable to not disclose personal information [34], hence showing a low level of SE susceptibility. This is based on fear of being held responsible for security breaches [34]. Bansa et al. [37] report findings that neurotic individuals act more sensitive towards

privacy issues.

In some research reviewed above, specific personality traits cannot be assigned to a single FFM trait: in Workman's study [7], high continuance commitment (significantly related to Openness, Conscientiousness, Extraversion, and Neuroticism [33]) increases SE vulnerability. Obedience to authority increases SE susceptibility, which supports Cialdini's principle of authority [7]. Unfortunately, we have not found any study that proves a distinct relation between specific personality traits and obedience to authority. Other studies exist that investigate relations between personal attributes and susceptibility to the principles of influence (see [7] for examples). However, as these do not clearly relate to comprehensive personality theories, we have not considered these for the literature review because of discussions that the discriminant validity of narrow personality traits is not sufficiently high [36]. Furthermore, it is questionable whether domain-specific personality traits can be considered personality traits at all. One of the main aspects of personality traits is their manifestation in behaviour across different situations and contexts.

IV. Social Engineering Personality Framework

Our comprehensive literature review provides relations between personality traits and SE in general. We want to extend this result to include specific correlations between personality traits and single principles of influence. Figure 1 shows our approach called the Social Engineering Personality Framework (SEPF). For some traits we generalise assumptions found in the literature. We explain our proposed relations for each personality trait as follows. We intend to evaluate our correlations by future questionnaires and experiments in order to provide worthwhile coping strategies. At this stage we focus on the physical domain. Future scenarios and coping strategies will include the digital domain as well (e.g. phishing attacks).

A. Conscientiousness

Since conscientious people adhere to existing rules, we assume that they are more vulnerable to SE techniques that exploit rules, social norms, and policies. Thus, we propose that conscientious targets are more likely to succumb to the principles authority, reciprocity, and commitment-consistency. Concerning commitment and consistency, we suppose an increased vulnerability only when commitments are made public (pressure to stay consistent) or refer to commitments regarding rules. We expect no correlation for principles that do not exploit rules, such as liking, social proof, and scarcity. Otherwise, conscientiousness can decrease SE susceptibility for every principle if sensible security policies exist that contain behavioural codex for coping with SE attacks and human errors.

Example Attack: In most organisations management receive as VIP special treatment. Social engineer impersonates authority roles via telephone to get the target to reset a password. If there are no sensible password policies in place, a conscientious target complies within the organisational hierarchy in order to do a good job.

Coping Strategies: Awareness trainings can prove essentially beneficial for conscientious individuals and can complement other trainings (e.g. team building). An organisation should create comprehensible policies addressed to each involved employee, i.e. check the efficiency before deploying – especially for emergency protocols when response time is critical (scarcity attacks). An organisational culture which can cope with human errors supports conscientious employees in communicating errors and social engineering attacks by preventing fear of embarrassment.

B. Extraversion

SE attacks using liking or social proof can work well on extraverted individuals as they rely on social aspects because extraversion relates to sociability, a sub-trait of extraversion. The excitement seeking is one sub-trait that can lead to greater vulnerability for the scarcity principle – getting something scarce is usually described as exciting. However, for high values in extraversion we assume a decreased vulnerability towards commitment and consistency techniques, since extraverted individuals tend to have a lower preference for consistency.

Example Attack: A social engineer attends a social event on a conference in order to attack an extroverted individual to reveal sensitive information. To receive social attention and become a member of a social group the employee gives in and acts against official company policies.

Coping Strategies: Rewards for achieved awareness trainings, for instance showing success rate in awareness learning system on company's internal social network (visible to all employees). Establish a system where employees suggest improvements for security policies and procedures – number of submitted suggestions per employee will be displayed on internal social networking site.

C. Agreeableness

Individuals who are more trusting raised fewer concerns about privacy invasion by location based services [36], which we assume to be generalisable to fewer privacy concerns. We predict higher SE vulnerability because of the higher likelihood of disclosing private information if a social engineer established a trust relationship. Regarding the principles of influence, we expect an increased vulnerability towards authority, reciprocity, liking, and social proof. Generally, every technique that involves opinions of other people can succeed due to the trusting nature, the helpfulness, and the belief in the goodness of mankind. The motivational system of agreeable persons consists of pursuing communal goals and seeking interpersonal harmony [30]. The latter can be exploited by an attacker with an importunate attitude.

Example Attack: Social engineer invests in small gift and favours to gain target's trust. After a while attacker addresses target to reciprocate a favour in helping out in an awkward situation like forgetting office keys.

Coping Strategy: For agreeable persons implement awareness trainings that focus on story-telling personal attack cases

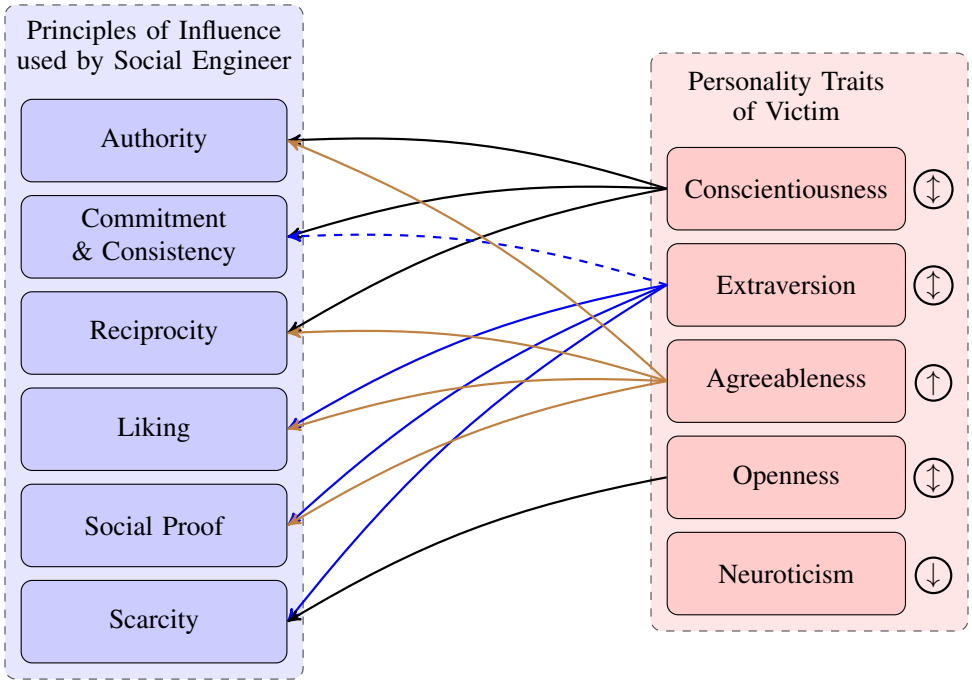

Fig. 1: **SEPF**: Specific personality traits (according to FFM) of a victim increase (solid line) or decrease (dashed line) the susceptibility to Cialdini's principles of influence which are used for attacks by a social engineer (for better readability some arrows are coloured.). General personality assumptions about susceptibility (higher, lower, or both) for each trait are depicted by corresponding arrows (↑, ↓, ↕).

to impart SE experience. This can alter the perspective who to trust.

D. Openness to Experience

Considering the lures used in SE attacks, openness to experiences and strong fantasy leads to higher susceptibility [8]. On the other hand, openness is associated with technological experience and computer proficiency [38]. Therefore, openness reduces SE vulnerability as more digitally literate users better detect SE attacks. We propose that scarcity only shows significant relation because of a perceived constriction of freedom – something aversive for an open individual. For the other principles, we conjecture no correlation.

Example Attack: First ten employees only can log in and evaluate company's new intranet wiki at an external website of a (fictitious) wiki service provider before it becomes productive. Employees can share their award-worthy improvements while the attacker collects their passwords.

Coping Strategy: We suggest e-learning systems that include edutainment and that use gamification where the user plays a creative part in e.g. advancing security policies. The motivational system contains creativity, innovation, and intellectual stimulation [30].

E. Neuroticism

Parrish et al. [8] propose that computer anxiety, which is associated with neuroticism, may protect regarding to computer-based SE attacks like phishing because neurotic user act with more caution. In general, we propose that neurotic individuals are less susceptible to most SE attacks. Neuroticism can act as a barrier since the underlying pessimism often assumes the worst in any situation. On the other hand, the motivational system consists of sensitivity to uncertainty and to threats [30]. The latter motivation could be exploited for authority attacks which the victim would *knowingly* succumb to. For now, we expect in general less susceptibility in our hypothesis.

Example Attack: As it is hard to build a trusted relationship with a neurotic individual and we assume no susceptibility to SE, an attacker can still harm an organisation by seeding mistrust and creating ambiguous and uncertain situations (e.g. by exploiting unaligned policies).

Coping Strategies: We do not have mitigation suggestions for neurotic individuals. The mistrusting nature can produce anxiety when reporting self-inflicted errors, therefore, we recommend trainings and supportive organisational culture as mentioned for conscientious employees. But we do not count this as SE attack.

V. Outlook and Future Research

We discussed how individual factors of personality traits relate to success or failure of Social Engineering (SE) attacks based on existent research and developed the more granular Social Engineering Personality Framework (SEPF), which still is based on theoretical assumptions. We will validate the proposed relations between each of the personality traits of the Five-Factor Model and the six principles of influence with

empirical data in future research. Questionnaires will include the Ten Item Personality Inventory (TIPI) [29] for categorising personality as well as knowledge checks and personal experiences of SE attacks via scenario-based design [39]. Furthermore, we will also add questions about gender, age, type of organisation, occupation, affinity to technology, stressors (possibly in combination with Barratt Impulsiveness Scale (BIS-11) [40]), and cultural background. With the combination of existing research data such as cultural studies ([41], [42]), we can hopefully draw promising new conclusions.

The SEPF itself explains differences in vulnerability to SE and will guide researchers by providing a structured approach. Thus, mitigation strategies can be adapted according to each personality and level of insiderness [1]. Understanding which links modify the susceptibility to SE attacks gives us the opportunity to detect – e.g. via penetration tests, questionnaires or flow charts (cf. "Social Engineering Attack Detection Model" (SEADM) for call centre agents [20]) – or even predict which types of attacks are more likely to succeed in a specific personnel constellation. Hence, appropriate countermeasures can be derived, such as advanced personalised awareness trainings (cf. Outcome-Based Education (OBE) [43], [44]), team building or even introduce a cultural change towards a security-aware organisational culture [16].

Our SEPF complements Tetri et al.'s "Social Engineering Framework" [17] which accentuates that SE is not limited on the previously overemphasised interaction between attacker and victim. It also includes situational factors like policies and victim's interpretation of a situation. We argue that these factors are influential and should not be overlooked, but Tetri et al.'s framework carries the risk of marginalising the interaction part. The SEPF addresses a specific relation between the two actors, namely, how the target's personality affects the success of the SE attack. Thus, complementing the previous framework regarding to an important and hitherto mostly unattended aspect.

Acknowledgement

Thanks to Felix Freiling, Dieter Gollmann, and Monique Janneck for their valuable comments and important suggestions for improvements. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318003 (TRE$_S$PASS). This publication reflects only the authors' views and the European Union is not liable for any use that may be made of the information contained herein.

Appendix

FFM Five-Factor Model
ICT Information and Communication Technology
SE Social Engineering
SEPF Social Engineering Personality Framework

References

[1] C. W. Probst and R. R. Hansen, "Reachability-based Impact as a Measure for Insiderness," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 4, no. 4, p. 38–48, December 2013. [Online]. Available: http://eprints.eemcs.utwente.nl/24198/01/jowua-v4n4-3.pdf

[2] Verizon RISK Team, "2012 Data Breach Investigations Report," 2012, accessed: 2013-06-19. [Online]. Available: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf

[3] M. Hosenball and W. Strobel, "Exclusive: Snowden persuaded other NSA workers to give up passwords," 11 2013, http://www.reuters.com/article/2013/11/08/net-us-usa-security-snowden-idUSBRE9A703020131108, last visited April 27th, 2014.

[4] C. Hadnagy, *Social Engineering: The Art of Human Hacking*. Wiley, 2010.

[5] B. Schneier, "The Psychology of Security," in *Progress in Cryptology – AFRICACRYPT 2008*, ser. Lecture Notes in Computer Science, S. Vaudenay, Ed., vol. 5023. Springer Berlin Heidelberg, 2008, p. 50–79.

[6] J. G. Mohebzada, A. El Zarka, A. H. Bhojani, and A. Darwish, "Phishing in a University Community: Two Large Scale Phishing Experiments," in *Innovations in Information Technology (IIT), 2012 International Conference on*. IEEE, 2012, pp. 249–254.

[7] M. Workman, "Wisecrackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security," *Journal of the American Society for Information Science and Technology*, vol. 59, no. 4, pp. 662–674, 2008.

[8] J. L. Parrish Jr, J. L. Bailey, and J. F. Courtney, "A Personality Based Model for Determining Susceptibility to Phishing Attacks," *Little Rock: University of Arkansas*, 2009.

[9] A. Vishwanath, V. Herath, R. Chen, J. Wang, and H. Raghav Rao, "Why do People get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model," *Decision Support Systems*, vol. 51, no. 3, p. 576–586, 2011.

[10] A. Darwish, A. Zarka, and F. Aloul, "Towards Understanding Phishing Victims' Profile," in *Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on*, 2012, p. 1–5.

[11] M. Huber, S. Kowalski, M. Nohlberg, and S. Tjoa, "Towards Automating Social Engineering Using Social Networking Sites," in *Computational Science and Engineering, 2009. CSE '09. International Conference on*, vol. 3, 2009, pp. 117–124.

[12] B. Schneier, *Secrets & Lies – Digital Security in a Networked World*. Wiley Computer Publishing, 2000.

[13] S. Abraham and I. Chengalur-Smith, "An Overview of Social Engineering Malware: Trends, Tactics, and Implications," *Technology in Society*, vol. 32, no. 3, pp. 183 – 196, 2010.

[14] G. L. Orgill, G. W. Romney, M. G. Bailey, and P. M. Orgill, "The Urgency for Effective User Privacy-Education to Counter Social Engineering Attacks on Secure Computer Systems," in *Proceedings of the 5th conference on Information technology education*, ser. CITC5 '04. New York, NY, USA: ACM, 2004, pp. 177–181.

[15] J. W. Scheeres, "Establishing the Human Firewall: Reducing an Individual's Vulnerability to Social Engineering Attacks," DTIC Document, Tech. Rep., 2008.

[16] S. Uebelacker, "Security-Aware Organisational Cultures as a Starting Point for Mitigating Socio-Technical Risks," in *INFORMATIK 2013*, ser. Lecture Notes in Informatics (LNI), Gesellschaft fuer Informatik e.V. (GI), Ed., vol. P-220, Hamburg University of Technology. Bonn: Matthias Horbach, September 2013, p. 2046–2057. [Online]. Available: http://doku.b.tu-harburg.de/volltexte/2013/1227/

[17] P. Tetri and J. Vuorinen, "Dissecting Social Engineering," *Behaviour & Information Technology*, 2013.

[18] D. Kahneman, *Thinking, Fast and Slow*. Penguin Books, 2011.

[19] R. Guadagno and R. B. Cialdini, "Online Persuasion and Compliance: Social Influence on the Internet and Beyond," *The Social Net: Human Behavior in Cyberspace*, pp. 91–113, 2005.

[20] M. Bezuidenhout, F. Mouton, and H. Venter, "Social Engineering Attack Detection Model: SEADM," in *Information Security for South Africa (ISSA), 2010*, 2010, pp. 1–8.

[21] R. B. Cialdini, *Influence: Science and Practice, 5th Edition*. Pearson, 2009.

[22] B. J. Sagarin, R. B. Cialdini, W. E. Rice, and S. B. Serna, "Dispelling the Illusion of Invulnerability: The Motivations and Mechanisms of Resistance to Persuasion," *Journal of Personality and Social Psychology*, vol. 83, no. 3, pp. 526–541, 2002.

[23] D. Gragg, "A Multi-Level Defense against Social Engineering," *SANS Reading Room, March*, vol. 13, 2003.

[24] S. Milgram, "Some Conditions of Obedience and Disobedience to Authority," *Human relations*, vol. 18, no. 1, pp. 57–76, 1965.

[25] L. M. Bujold, *Diplomatic Immunity*. Baen Books, 2002, vol. 14.

[26] J. W. Brehm, "A Theory of Psychological Reactance," *New York*, 1966.

[27] R. R. McCrae and O. P. John, "An Introduction to the Five-Factor Model and Its Applications," *Journal of Personality*, vol. 60, no. 2, pp. 175–215, 1992. [Online]. Available: http://psych.colorado.edu/~carey/courses/psyc5112/readings/psnbig5_mccrae03.pdf

[28] J. Shropshire, M. Warkentin, A. Johnston, and M. Schmidt, "Personality and IT Security: An Application of the Five-Factor Model," in *Proceedings of the Americas Conference on Information Systems*, 2006, pp. 3443–3449.

[29] S. D. Gosling, P. J. Rentfrow, and W. B. Swann Jr, "A very brief measure of the big-five personality domains," *Journal of Research in personality*, vol. 37, no. 6, pp. 504–528, 2003. [Online]. Available: http://homepage.psy.utexas.edu/HomePage/Faculty/Swann/docu/research_materials/GOSL.PDF

[30] J. B. Hirsh, S. K. Kang, and G. V. Bodenhausen, "Personalized Persuasion Tailoring Persuasive Appeals to Recipients' Personality Traits," *Psychological science*, vol. 23, no. 6, pp. 578–581, 2012.

[31] J. F. Salgado, "The Big Five Personality Dimensions and Counterproductive Behaviors," *International Journal of Selection and Assessment*, vol. 10, no. 1-2, p. 117–125, 2002.

[32] M. Warkentin, L. Carter, and M. McBride, "Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies," in *The 2011 Dewald Roode Workshop on Information Systems Security Research*, 2011.

[33] J. Erdheim, M. Wang, and M. J. Zickar, "Linking the Big Five Personality Constructs to Organizational Commitment," *Personality and Individual Differences*, vol. 41, no. 5, pp. 959–970, 2006.

[34] D. Weirich and M. A. Sasse, "Pretty Good Persuasion: A First Step towards Effective Password Security in the Real World," in *Proceedings of the 2001 workshop on New security paradigms*. ACM, 2001, p. 137–143.

[35] R. B. Cialdini, M. R. Trost, and J. T. Newsom, "Preference for Consistency: The Development of a Valid Measure and the Discovery of Surprising Behavioral Implications," *Journal of Personality and Social Psychology*, vol. 69, p. 318–328, 1995.

[36] I. Junglas and C. Spitzmuller, "Personality Traits and Privacy Perceptions: An Empirical Study in the Context of Location-Based Services," in *Mobile Business, 2006. ICMB '06. International Conference on*, 2006, pp. 36–36.

[37] G. Bansal, F. Zahedi, and D. Gefen, "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online," *Decision Support Systems*, vol. 49, no. 2, pp. 138 – 150, 2010.

[38] A. B. Woszczynski, P. L. Roth, and A. H. Segars, "Exploring the Theoretical Foundations of Playfulness in Computer Interactions," *Computers in Human Behavior*, vol. 18, no. 4, pp. 369–388, 2002.

[39] J. M. Carroll, "Five Reasons for Scenario-Based Design," in *HICSS'99: Proceedings of the Thirty-Second Annual Hawaii International Conference on System Sciences, 3*, vol. 3051, 1999.

[40] J. H. Patton, M. S. Stanford *et al.*, "Factor Structure of the Barratt Impulsiveness Scale," *Journal of Clinical Psychology*, vol. 51, no. 6, pp. 768–774, 1995. [Online]. Available: http://homepages.se.edu/cvonbergen/files/2013/01/Factor-Structure-of-the-Barratt-Impulsiveness-Scale.pdf

[41] Hofstede Center, "Organisational Culture & Change Management," 2014, http://geert-hofstede.com/organisational-culture.html last visited on April 27th, 2014.

[42] ——, "National Cultural Dimensions," 2014, http://geert-hofstede.com/national-culture.html last visited on April 27th, 2014.

[43] W. G. Spady, *Outcome-Based Education: Critical Issues and Answers*. American Association of School Administrators, 1994. [Online]. Available: http://www.eric.ed.gov/ERICWebPortal/contentdelivery/servlet/ERICServlet?accno=ED380910

[44] J. F. Van Niekerk, "Establishing an information security culture in organizations: an outcomes based education approach," Ph.D. dissertation, Nelson Mandela Metropolitan University, 2005, http://hdl.handle.net/10948/164. [Online]. Available: http://hdl.handle.net/10948/164