Development of a Social Engineering Exposure Index (SEXI) for C-Level Positions of US Corporations

by

William Shawn Wilkerson

A Pre-idea paper submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Engineering and Computing
Nova Southeastern University

2016

Chapter 1

Introduction

Problem Statement

The research problem that this study will address is the existing exposure of C-level executives of US corporations that contribute to social engineering (SE) attacks due to publically available information (Heartfield & Loukas, 2015; Mitnick & Simon, 2011). Prior research has shown the information being used to execute SE attacks typically originates at the target or those closely associated with them (Heartfield & Loukas, 2015; Luo, Brody, Seazzu, & Burd, 2013). Studies have also shown a significant increase of personal information exposed on social networking sites (SNSs) and the overall willingness to provide personal content (Acquisti, Brandimarte, & Loewenstein, 2015; Hong & L. Thong, 2013).

"Exposure involves the exposing to others of certain physical and emotional attributes about a person" (Solove, 2006, p. 533). Ku, Chen, and Zhang (2013) found that a positive association exists between the gratification provided by using SNSs with the intention for continued usage though privacy concerns may have an effect on the correlation. Some studies even suggest that people willingly expose private information in exchange for content gratification, even after adjusting their settings for better privacy (Sutanto, Palme, Chuan-Hoo, & Chee Wei, 2013).

When Facebook first went public, it targeted business users and was later expanded to include any user (Acquisti et al., 2015). The majority of information shared by its original users was related to business efforts providing very few descriptive items

for the user shareable to only a limited scope of people (Acquisti et al., 2015; Pew Research Center, 2013). By 2014, the basic and extended profiles of a user's personally identifiable information (PII) were shareable to anyone on the internet (Acquisti et al., 2015). This availability of public information allows social engineers to glean necessary data to successfully social engineer an exposed target via a myriad of attack vectors (Heartfield & Loukas, 2015; Luo et al., 2013). Acquisti et al. (2015) found that the number of Facebook categories of exposure increased from three to eight between 2005 and 2014 beginning with text and progressively expanding to including video content.

According to the U.S. Federal Bureau of Investigation (FBI) (2015), Business Email Compromise (BEC), a single attack vector of SE, affected over 7000 organizations within the United States approaching $800 million in losses between October 2013 and August 2015. A substantial increase of over 270 percent in the number of BEC cases occurred during the opening months of 2015 indicating SE attacks are dramatically on the rise (Federal Bureau of Investigation, 2015).

Phishing is another attack vector of SE, whereby the target is baited with a fake copy of a web page or website to solicit sensitive information or to inject malware onto the computer (Heartfield & Loukas, 2015). Neupane, Rahman, Saxena, and Hirshfield (2015) conducted phishing research and found that the longer an individual looked at the content on a fake web page, during each 10-second trial, the more likely they would accept it as being authentic. If the participant was distracted or sleep-deprived the possibility of a successful phishing event significantly increased (Neupane et al., 2015).

The October 2015 BEC attack on the Director of the U.S. Central Intelligence Agency (CIA) provides an example which suggests the need for this research. Teenagers

were able to gather data from open source information located across multiple online accounts belonging to the CIA Director using the information to pretext, another SE attack vector, customer service representatives via telephonic communication into exposing more information. Using the combined data, the attackers obtained the necessary information to access the CIA Director's personal email account. Subsequently, the attackers released social security numbers and other sensitive PII of many of the Director's associates and subordinates to WikiLeaks (Franceschi-Bicchierai, 2015; Kopan, 2015). As the CIA director lamented his embarrassed level of exposure, the series of attacks across multiple attack vectors in this instance suggests that having access to open source information (OSI) provided a mechanism for attackers to execute a myriad of SE attacks on their intended target (Tetri & Vuorinen, 2013).

Research Goals

The main goal of this research is to develop a social engineering exposure index (SEXI) to assist in identifying and classifying SE vulnerabilities of C-level executives of United States Corporations. The need for this work is demonstrated by the work of Mitnick and Simon (2011), Tetri and Vuorinen (2013), Heartfield and Loukas (2015), and Mouton, Leenen, and Venter (2016) who acknowledge the progressive expansion of SE attack vectors, the lack of a predictive threat system, the availability of OSI which circumvent organizational cyber-security technologies, and the dearth of data on information gathering techniques for the execution of prior SE attacks.

Mouton et al. (2016) describe the difficulty in performing SE research due to the lack of information provided in news articles, especially the organization methodology of a particular SE attack and where the information was gathered to prosecute the intended

target. Even with their proposed templates which map an SE attack to a "template" the lack of knowing what OSI is available and how exposed a potential target remains a critical issue (Mouton et al., 2016). Mouton et al. (2016) reinforce the sentiment found in Mitnick and Simon (2011) that the human component is the weakest link for organizational security serving both as a bypass to security technologies and as the fountain of information by which SE attacks occur. Additionally, Mouton et al. (2016) suggest that SE research is still in its infancy even in the midst of the rapid growth of information security research.

Heartfield and Loukas (2015) describe the ineffectiveness of studying "semantic attacks" as it occurs after the damage is done and may be limited by a lens focused on a singular attack vector (p. 31). Of significance, for this research proposal, is the call for a prediction mechanism for determining exposure in real time, automatically updated with a rapid response window (Heartfield & Loukas, 2015).

Acquisti et al. (2015) describe the exponential increase of OSI via SNSs while Tetri and Vuorinen (2013) found that its availability enabled and facilitated SE attackers across a broad spectrum of attack vectors. Current research and defense mechanisms tend to focus on a single attack vector or technique thereby drastically limiting the actual benefits of the study or the security strategy (Tetri & Vuorinen, 2013). Specifically, Tetri and Vuorinen (2013) suggests that research might include an evaluation of where the information was obtained that was used in the SE attack as well as how the attacker vectors were possible in the first place (p. 1020). This dissertation proposal builds on previous research by attempting to investigate the lack of attention given to the contribution of OSI to SE exposure. This study proposes to provide an index of exposure

to social engineering due to the availability of open source information which can be used to assist in identifying and classifying SE vulnerabilities of C-level executives of United States Corporations. This study proposes to provide a mechanism which may determine the sources of information used in SE attacks.

The first specific goal of this research study is to gather the requirements for establishing exposure to C-level executives. The second specific goal of this research study is to develop an index of social engineering exposure. The third specific goal of this research study is to evaluate the exposure of various C-level executives using SEXI and classify the targets based on the results. The forth specific goal of this study is to use the same index on non-C-level personnel and compare the results to the classification of the C-level executives.

The main research question that this study will address is: what is the SEXI of C-level executives of US corporations that contribute to social engineering (SE) attacks due to publically available information? The four specific research questions that this study will address are:

RQ1. What are the requirements to develop an index of social engineering exposure?

RQ2. What is the framework for a Social Engineering Exposure Index (SEXI)?

RQ3. How are the ten C-level executives classified on the SEXI?

RQ4. How does a set of ten non-C-level personnel differ in their SEXI from the classification of the C-level executives?

SE attacks are on the rise, and the OSI used to perpetrate these crimes is far too readily available (Acquisti et al., 2015; Federal Bureau of Investigation, 2015). The merit

of the development of an exposure index is that it can assist in the prediction of the SE exposure of targets, the content of potential attacks, and possible attack vectors which current security structures may fail to detect (Heartfield & Loukas, 2015; Mouton et al., 2016).

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514. doi:10.1126/science.aaa1465

Federal Bureau of Investigation. (2015). Business e-mail compromise. *Stories.* Retrieved from https://www.fbi.gov/news/stories/2015/august/business-e-mail-compromise/business-e-mail-compromise

Franceschi-Bicchierai, L. (2015). Teen hackers: A '5-year-old' could have hacked into CIA director's emails. Retrieved from https://motherboard.vice.com/read/teen-hackers-a-5-year-old-could-have-hacked-into-cia-directors-emails

Heartfield, R., & Loukas, G. (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Comput. Surv., 48*(3), 1-39. doi:10.1145/2835375

Hong, W., & L. Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly, 37*(1), 275-298.

Kopan, T. (2015). Cia Director John Brennan 'outraged' by hack of his emails. Retrieved from http://www.cnn.com/2015/10/27/politics/john-brennan-email-hack-outrage/

Ku, Y.-C., Chen, R., & Zhang, H. (2013). Why do users continue using social networking sites? An exploratory study of members in the United States and Taiwan. *Information & Management, 50*(7), 571-581. doi:10.1016/j.im.2013.07.011

Luo, X. R., Brody, R., Seazzu, A., & Burd, S. (2013). Social engineering: The neglected human factor for. *Managing Information Resources and Technology: Emerging Applications and Theories: Emerging Applications and Theories*, 151.

Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*: John Wiley & Sons.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security, 59*, 186-209. doi:http://dx.doi.org/10.1016/j.cose.2016.03.004

Neupane, A., Rahman, M. L., Saxena, N., & Hirshfield, L. (2015). *A multi-modal neuro-physiological study of phishing detection and malware warnings*. Paper presented at the Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, Colorado, USA.

Pew Research Center. (2013). Social networking fact sheet. Retrieved from http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154,* 477+.

Sutanto, J., Palme, E., Chuan-Hoo, T., & Chee Wei, P. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly, 37*(4), 1141-A1145.

Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. *Behaviour & Information Technology, 32*(10), 1014-1023. doi:10.1080/0144929X.2013.763860

College of Engineering and Computing (CEC)

Certification of Authorship of Doctoral Course Assignment

Submitted to (Professor's Name): Dr. Yair Levy

Student's Name: W. Shawn Wilkerson

Date of Submission: May 29, 2016

Purpose and Title of Submission: Assignment 1: Risk Management in Information Systems Security Theory Focused Paper, Literature Summary Table, and Reference List on the Topic of Cyber Swarm Intelligence

Certification of Authorship: I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas, or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for this purpose.

Student's Signature: W. Shawn Wilkerson