Chapter 1
Social Engineering in Information Security Breaches and the Factors That Explain Its Success:
An Organizational Perspective

Jhaharha Lackram
University of KwaZulu-Natal, South Africa

Indira Padayachee
University of KwaZulu-Natal, South Africa

ABSTRACT

Social engineering refers to the art of using deception and manipulating individuals to gain access to systems or information assets and subsequently compromising these systems and information assets. Information security must provide protection to the confidentiality, integrity, and availability of information. In order to mitigate information security's weakest link, it becomes necessary to understand the ways in which human behavior can be exploited via social engineering. This chapter will seek to analyze the role of social engineering in information security breaches and the factors that contribute to its success. A variety of social engineering attacks, impacts, and mitigations will be discussed. Human factors such as trust, obedience, and fear are easily exploited, thereby allowing social engineers to execute successful attacks. However, with effective countermeasures such as information security awareness training, education, and audit procedures, the impacts of social engineering can be decreased or eliminated altogether.

DOI: 10.4018/978-1-5225-4763-1.ch001

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

The fourth industrial revolution, or Industry 4.0 as it is commonly referred to, has been set in motion and will in due course have an impact on the way individuals and society functions as a whole. In Industry 4.0, all systems communicate with each other, as well as with humans thereby making data accessible via a medium such as the internet for operators and users alike (Chung and Kim, 2016). This element of human interaction and human accessibility poses a threat to information security which needs to be considered, since it is the human who poses the most risk in the information security chain (Workman, 2007; Pavkovic and Perkov, 2011).

A growing segment of research within the domains of information systems, information technology and computer science focuses on information security, which is a sub-discipline that centres on the protection of information assets from users with malicious intent (Pieters, 2011). In the event of an attack or security breach, it is imperative that the confidentiality, integrity and availability of information, commonly referred to as the CIA triad, must be protected via information security mechanisms and tools (Pieters, 2011).

The security of information systems is largely dependent on a myriad of both technical and non-technical aspects (Pavkovic and Perkov, 2011). The efficacy of technical-based attacks such as traditional hacking or malicious code attacks has decreased considerably due to the provision and adoption of technological security solutions by organizations (Janczewski and Fu, 2010). Due to the advent of advanced computer-based security or technical security, it has become common for attackers to instead rely on an alternative, non-technical means of gaining access to systems (Thompson, 2004). This phenomenon is referred to as social engineering, which refers to an attack that utilises the art of manipulating and using human interaction to execute an action or obtain valuable information. This ill-gotten information can be used to access or compromise the information systems of an organisation, thereby sabotaging the financial and economic health of the organisation (Jannson, 2011; Orgill et al, 2004; Kvedar, Nettis and Fulton, 2010).

As stated by Vidalis and Kazmi (2007), the human factor is a shared vulnerability of perceptions and decision making in the sense that it is human beings who interact with computers by typing in commands, automating processes and turning computers off should they think that it is not operating properly by misinterpreting its reactions.

A successful social engineering attack can result in the social engineer gaining control of an entire company's network servers (Manske, 2000). Social engineering leaves even the most technically secured computer systems extremely vulnerable, as it relies on the social engineers' social skills to compromise the information security of the organisation (Thompson, 2004). Most often, social engineering attacks are carried out with deception to the degree that the victim does not realize that (s)he has been manipulated, thereby making the identification of social engineering attacks extremely difficult (Gulati, 2003; Bezuidenhout, Mouton and Venter, 2010). Social engineering transpires at a psychological level with psychology being used to generate an authoritative atmosphere where the victim is persuaded into divulging information pertinent in the accessing of a system. Furthermore, these attacks also take place at a physical level, namely at the workplace where the victim feels secure via the medium of work telephone numbers or email (Orgill et al, 2004). More recently, the trend of Bring Your Own Device (BYOD) and cloud computing has given social engineers more opportunities to carry out attack vectors in the workplace (Kromholz et al, 2014; Hatwar & Chavan 2015).

24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/social-engineering-in-information-security-breaches-and-the-factors-that-explain-its-success/206778

Related Content

Quantifying Unknown Unknowns in an Oil and Gas Capital Project
Yuri Raydugin (2012). *International Journal of Risk and Contingency Management (pp. 29-42).*
www.irma-international.org/article/quantifying-unknown-unknowns-oil-gas/67373

Tools for Representing and Processing Narratives
Ephraim Nissan (2007). *Encyclopedia of Information Ethics and Security (pp. 638-644).*
www.irma-international.org/chapter/tools-representing-processing-narratives/13536

A Generic Self-Evolving Multi-Agent Defense Approach Against Cyber Attacks
Stephen Mugisha Akandwanahoand Irene Govender (2018). *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution (pp. 165-181).*
www.irma-international.org/chapter/a-generic-self-evolving-multi-agent-defense-approach-against-cyber-attacks/206783

Large Key Sizes and the Security of Password-Based Cryptography
Kent D. Boklan (2011). *Security and Privacy Assurance in Advancing Technologies: New Developments (pp. 60-66).*
www.irma-international.org/chapter/large-key-sizes-security-password/49495

Comparison of Various DoS Algorithm
Mainul Hasan, Amogh Venkatanarayan, Inder Mohan, Ninni Singhand Gunjan Chhabra (2020). *International Journal of Information Security and Privacy (pp. 27-43).*
www.irma-international.org/article/comparison-of-various-dos-algorithm/241284