Social Engineering Attacks: An Augmentation of the Socio-Technical Systems Framework

Nobubele Angel Shozi[1] and Mapule Modise[2]
[1]Council of Scientific and Industrial Research (CSIR), Defence Peace Safety Security, Pretoria, South Africa
[2]University of South Africa (UNISA), South Africa
ashozi@csir.co.za

Abstract: Social engineering attacks pose huge security threats to companies today. These attacks have succeeded mainly because they come from weaknesses that combine the social engineering practices that exploit the human vulnerabilities, with technical skills to bypass the defences of information systems. This paper is founded on the premise that social engineering attacks result from interdependent yet interrelating factors that combine to give an attacker the ability to compromise an individual or organisation's information. We analyse social engineering attacks as a Socio-technical System because it recognises the interaction between people and technology in a work environment. In the case of social engineering attacks, the social subsystem would encompass the people (both victim and attacker), the environmental subsystem would be the environment in which the social engineering attack occurs and the technical subsystem would be the technology used to perform the social engineering attack. The Socio-technical subsystems are further mapped against an existing framework known as the Socio-technical systems framework. This paper applies the currently existing Socio-technical systems framework along with the Socio-technical subsystems mappings to analyse a social engineering attack case study to help identify the underlying factors that made the attack successful. The case study is a popular attack known as 'The Francophone attack', which is an attack that was carried out on a French bank. Through the analysis of the case study, the researchers found that in order to analyse a social engineering attack using the framework, it is pivotal to augment the framework by adding an Information node in the environmental subsystem as one of the aims of any social engineering attacks is to trick you into handing over passwords or other sensitive financial and personal information. The outcome of this research is twofold – firstly, it aims to provide an in-depth perspective into the factors that can allow a social engineering attack to be successful and secondly, to augment the socio-technical systems framework to suit analysis of social engineering attacks when identifying socio-technical system factors.

Keywords: socio-technical systems, social engineering attack, socio-technical systems framework

1. Introduction/background

A large number of companies and ordinary people continue to fall victims to social engineering attacks despite the continued efforts to improve user awareness about information security, and investments on advanced technical and technological security solutions. According to Power and Forte (2006), the social engineering threats have evolved in sophistication and at a faster pace than the countermeasures. With the growth and sophistication of social engineering based attacks occurring and the vulnerabilities that are inherent in humans, the question of interest is "how then can organisations prepare for these attacks?". This paper argues that detection and subsequent prevention of social engineering based attacks depend largely on a clear understanding of these attacks. This understanding, however, should go beyond definition and identifying the human as the weakest link. This understanding requires a deeper analysis of all other factors facilitating the successful social engineering based attacks. Although the paper does not dispute the huge role that human weakness plays in the success of any social engineering attack, it is however, the authors' view that the aspect of human weakness is overrated at the expense of other factors. A social engineering attack is multidimensional and its success is an outcome of interaction of interdependent factors with strong social and technical aspects. Such factors include among others the information security policies, organisational setting, and awareness level of employees (Tetri & Vourien, 2014). It is against this background that this paper uses a multidimensional approach, that is, socio-technical framework to analyse social engineering attacks. The framework is applied to a case study with the view to gain a holistic insight to social engineering attacks.

This paper is structured as follows: The Definition of Key Concepts (Section 2) presents brief definitions of socio-technical systems, socio-technical systems framework and social engineering attacks. This is followed by an explanation of the Socio-technical systems framework applicability to Social engineering attacks (Section 3). A social engineering attack case study is analysed in section 4 using the socio-technical system framework. The paper ends with a conclusion in section 5.