Chapter 7
A Socio-Technical Perspective

ABSTRACT

Chapter 7 uses a philosophical approach to discuss the frailty of the human psyche with regards to the implementation and use of systems through our engagement with cyberspace. Our constant exposure to newsworthy cyber security events can desensitize people to the warnings that are either apparent or subliminal. A number of key topical subject areas are discussed exploring human psychology: why people are susceptible to psychological vulnerabilities, characteristics of the human psyche that facilitate errors, how these traits can be exhibited through flawed actions causing mistakes and preventative measures to stop deliberate and accidental actions. This analysis is of vital importance and relevance in order to combat the risks, which to the computer end-user may appear distant and intangible.

INTRODUCTION

This chapter uses a sociological analysis in a technological context to discern the common differentiator in many security breaches – the human. From research conducted between 2009 and 2017 in the U.S. Healthcare Industry, Doctors of Philosophy from Michigan State University and Johns Hopkins Carey Business School concluded that the majority of security breaches are caused unintentionally and through carelessness. A small minority of breaches were classed as intentional acts extrapolating information for unauthorized use, such as fraud (Worth, 2018). However, a study conducted by Verizon using 2015 and 2016 statistical data surmised that 95% of breaches can be

DOI: 10.4018/978-1-7998-3979-8.ch007

categorized by nine patterns – two thirds of which are technology enabled attacks and one third being human facilitated. Strikingly, the patterns with the highest percentile scores were human behaviors, comprising: miscellaneous errors, insider and privilege misuse, and physical theft and loss (Verizon, 2016). While organizations are keen to adopt technology, the human appears to be trailing behind because of misunderstandings in the challenges of implementing technology and the consequences of getting it wrong (Editor, 2016). This has led the U.K. NCSC to call for business boards to take more responsibility and recognize that cyber risk is one of the business risks that can affect enterprises (Ashford, 2019). However, in order to understand this problem more thoroughly, researchers must explore the psychology of the human mind. Hence, the rest of this chapter establishes the reasons behind some user failings and ways of remedying them.

BACKGROUND

In recent years, the Press has reported on users being the major contributory factor in organizational data breaches. The contagion of phishing and spear phishing campaigns from outsiders have fueled this. Insider password re-use that are both exploitable by hackers and state actors alike have also caused data breaches. Users and executives are arguably targets as they are the most exposed within organizations who have access to the Internet on a daily basis and potentially the most naïve or ignorant. Thus, they are targeted like low hanging fruit by the attackers. The employee does not need to be using a higher privilege level for an attack to be a success. Instead, all it needs is an exploitable weakness in unpatched software for an attacker to escalate privileges in a compromised user account (Winkler, 2015). When it comes to taking shortcuts, employees may circumvent technical controls because they are just trying to be more efficient and harbor no malicious intent (Wyatt, 2017).

Passwords are one contributing factor to security breaches. RSA Security's second survey - conducted by the company set named after co-founders Rivest Shamir and Adleman, reported that password overload was a significant cause of security breaches in 2006; thereby indirectly encouraging password re-use to make things simpler for the users (Savvas, 2006). By 2016, advice on password constitution changed from the traditional 'upper, lower case,