Chapter 87
The "Human Factor" in Cybersecurity:
Exploring the Accidental Insider

Lee Hadlington
De Montfort University, UK

ABSTRACT

A great deal of research has been devoted to the exploration and categorization of threats posed from malicious attacks from current employees who are disgruntled with the organisation, or are motivated by financial gain. These so-called "insider threats" pose a growing menace to information security, but given the right mechanisms, they have the potential to be detected and caught. In contrast, human factors related to aspects of poor planning, lack of attention to detail, and ignorance are linked to the rise of the accidental or unintentional insider. In this instance there is no malicious intent and no prior planning for their "attack," but their actions can be equally as damaging and disruptive to the organisation. This chapter presents an exploration of fundamental human factors that could contribute to an individual becoming an unintentional threat. Furthermore, key frameworks for designing mitigations for such threats are also presented, alongside suggestions for future research in this area.

INTRODUCTION

The focus of this current chapter is to examine the impact human factors, including aspects of personality traits or cognitive factors that can serve to influence cybersecurity practices and behaviors. The background against which this exploration is framed is related to the insider threat, more specifically those that have no specific motive or malicious intent. The chapter will begin with an examination of key statistics related to cybercrime in business as well as introducing current concerns related to the 'insider threat'. The typology of the insider threat will be discussed in brief, but then will shift to focus more directly on the notion of an 'accidental insider' – those individuals who have no malicious intent to commit transgressions of cybersecurity, but do so through misjudgment, ignorance and lack of understanding/knowledge.

DOI: 10.4018/978-1-7998-7705-9.ch087

Following on from this, the focus will then turn towards research examining key human factors that could influence the cybersecurity posture of the individual. This includes potential links between psychology traits such as impulsivity, decision-making and conscientiousness and information security. The concluding aspects for the chapter will focus on key techniques and frameworks that have the potential to change the behaviors of end-users. These techniques hopefully move individuals towards better cyber-inoculation, and provide mitigation for the threat from the accidental insider.

BACKGROUND

In a recent report published by the Office of National Statistics (ONS, 2016) it was estimated that online fraud was costing companies an estimated £193bn. Furthermore, the survey also noted that 5.8 million individual incidents of cybercrime had been reported in the year 2015-16; these were split between fraudulent activities (bank/credit card account fraud/advance fee fraud) and computer misuse (distribution of computer viruses/unauthorized access to computers/hacking). The Business Crime Survey (BCS, 2015) also noted a 55% increase in reported online fraud between 2014-15. In the same report, one of the key concerns raised was the growing threat from individuals within the organization, or the so called 'insider threat'. This latter point is mirrored by an apparent realization by researchers within the information security community that, for the most part, the weakest element in the cybersecurity chain is that of the human (Anwar et al., 2016; Nurse, Creese, Goldsmith, & Lamberts, 2011; Sasse, Brostoff, & Weirich, 2001; Sasse & Flechais, 2005).

In the context of the continued fight to protect business and organizations from the threat being posed by information theft and cybercrime a great deal of attention is devoted to improving the existing security infrastructure (Pfleeger & Caputo, 2012). Attempts to enhance network security via technological solutions such firewalls, intrusion detection, and biometric devices provide some legitimate protection against a wide variety of threats. However, these steps make an assumption that all threats to the security of the organization are inward facing, and come from an external source or attacker. Early commentators in the area of cybersecurity noted that one of the biggest barriers to creating effective information security strategies is the human elements within the system (Whitten & Tygar, 1998). From a usability perspective it is noted that, for the most part, security protocols and systems are either too confusing or too difficult for the average end-user to engage in effectively (Whitten & Tygar, 1998; Sasse & Flechais, 2005). Accordingly, Sasse and Flechais (2005) noted that the situation is further complicated by additional aspects related to human factors including:

- A lack of understanding on behalf of employees about the importance of the data, software and systems within an organisation
- Ignorance about the level of risk attached to the assets for which they have direct responsibility for and
- A lack of understanding about how their behaviour could be putting the same assets at risk (Sasse & Flechais, 2005).