Countering Social Engineering Through Social Media: An Enterprise Security Perspective

Heidi Wilcox and Maumita Bhattacharya

School of Computing & Mathematics, Charles Sturt University, Albury, Australia
{hwilcox,mbhattacharya}@csu.edu.au

Abstract. The increasing threat of social engineers targeting social media channels to advance their attack effectiveness on company data has seen many organizations introducing initiatives to better understand these vulnerabilities. This paper examines concerns of social engineering through social media within the enterprise and explores countermeasures undertaken to stem ensuing risk. Also included is an analysis of existing social media security policies and guidelines within the public and private sectors.

1 Introduction and Background

Social media sites such as Facebook, MySpace, LinkedIn, and Twitter are a data mining goldmine for readily available personal and sensitive information made publicly for the web, especially when the majority of participants are using default privacy settings. (King, 2008; Furnell, 2008; Slonka, 2014; Nayak Prince & Robinson 2014; Wong et al 2014). The increased adoption of social media technologies and failing to protect company information may result in data leakage, business continuity failures and compliance breaches, reputational risks through loss of valuable intellectual property, consumer confidence and competitive advantage (Colwill, 2009; Almeida, 2012). Traditional security countermeasures are not keeping up with these changes in the workplace as more businesses are encountering breaches targeting the human elements, such as social engineering. (Colwill, 2009; Rudman, 2010; He, 2012). Social engineers exploit human behaviour idiosyncrasies to form an attack from the outside that leads them to gain inconspicuous entry into protected areas of the company for their own illicit use. (Mitnick & Simon, 2001).

As the line between business use and personal use is often blurred, social engineers can gather sensitive data from any number of social media accounts to form a personal resume on a targeted employee. (Meister & Willyerd, 2010). Traditionally, email was the primary vector for spam and phishing exploits, however, the popularity and scope for large volume targets in social media has seen these threats moving away from email and on to social platforms. Web based attacks such as phishing are consistently found to be the leading transport vectors for cyber-attacks; social media and social gaming provides the perfect vehicle or attack surface for delivering lures and payloads. (Arachchilage & Love, 2014; Ikhalia, 2014). The top three social media issues negatively experienced by organizations include: employees sharing too much
information, the loss of confidential information, and increased exposure to litigation (Symantec, 2011). Other equally important results include losses concerning employee productivity and increased risk of exposure to virus and malware (Almeida, 2012). These platforms enable social engineers to operate freely, efficiently and cost effectively with low margins for getting caught. (Franchi, Poggi & Tomaiuolo, 2014).

Boudreaux (2010a), and Foreshew (2012), propose that organizations protecting information assets through effective security policies and governance will more effectively manage the business risks of the future. Social media policies and guidelines provide advice on how social media participation will be applied to all of the members of an organization (Bell, 2010). It is also reported that the most effective security countermeasure against social engineering is to increase employee awareness of the many tricks employed by social engineers against them in the workplace. (Bada & Sasse, 2014).

The remainder of the paper is organized as follows. In Section 2 we explore those countermeasures currently offered by enterprise to address the challenges faced by social engineering through social media concerning people, process and technology. We also review existing social media policies from opposing sectors and compare areas of coverage in Section 3 with some concluding remarks presented in Section 4.

2 Countering Social Engineering through Social Media: Current Perspectives

The following global perspectives underline information security practices concerning people, process and technology that are currently used by enterprise in an attempt to decrease loss attributed to their social media usage.

2.1 People

Global organizations are embracing new technologies that explore huge business benefits but also bring catastrophic organizational risk. (Almeida, 2012). Countermeasures for online social engineering concerning people and employees have had various levels of success. Information security taskforces aligned to assess such threats are now heading in a positive direction towards understanding the motivations behind these attacks. These paths include establishing types of threat vectors and introducing awareness initiatives that effectively reduce business risk. (VMIA, 2010). Current practices focus on creating individual employee awareness and training in both the public and private sectors; whether they are online at home or work. There is a general consensus from both sectors that there needs to be collaboration from government and business in all industries to increase cyber security effectiveness.

The UK and US governments are guiding business and consumers with awareness initiatives in response to a trend in developed nations to adopt a web 2.0 and social business model framework for all government departments and processes. Recent awareness campaigns include the introduction of a national computer emergency