Chapter 85
Information Security and Privacy in Social Media: The Threat Landscape

Hemamali Tennakoon
Kingston University, UK

ABSTRACT

Information security and privacy are multi-faceted concepts, and earlier definitions of information security and privacy seem inadequate in the context of emerging technologies such as social media. Hence, this chapter presents an analysis of the concept of information security followed by a discussion of computer security, information security, network security, personal privacy, informational privacy, etc. Then the discussion narrows down to information security and privacy on Social Networking Sites (SNS) followed by an analysis of the consequences of information security and privacy breaches from individualistic and organizational perspectives. The lack of understanding of the complex nature of security and privacy issues are preventing businesses from gaining the full economic benefit, especially on SNS. Therefore, some solutions and recommendations are suggested towards the end of the chapter, including the need for a common legal framework. Finally, the chapter ends with suggestions for future research.

INTRODUCTION

Information security and privacy is a vital concern for organizations and individuals operating in today's digital society. Gordon et al. (2010) argue that the rise of the Internet and e-commerce has elevated the value of information as an organisational asset. However, protecting such information assets against cyber-crimes such as "denial-of-service attacks, web hackers, data breaches, identity and credit card theft, and fraud" etc. (Smith, Winchester, Bunker, & Jamieson, 2010, p.1) is posing a major challenge to organizations operating on the web. Breaches of information security could have a significant negative effect on the value of an organization (Campbell, Gordon, Loeb,, & Zhou, 2003; Cavusoglu, Mishra, & Raghunathan 2004; Kritzinger & Smith 2008; Johnston & Warkentin, 2010), not only in terms of losing time, manpower, money and/or business opportunities (Dhillon & Moores, 2001; Whiteman & Mattord, 2003) but also in losing the trust, loyalty and goodwill of

DOI: 10.4018/978-1-4666-8614-4.ch085

their customers (Jarvenpaa, Tractinsky, & Saarinen, 2000; Miyazaki & Fernandez, 2001; Lee & Turban, 2001; McKnight, Choudhury, & Kacmar, 2002; Gefen, Karahanna, & Straub, 2003; Liu, Marchewka, Lu, & Yu, 2004; Chen & Barnes, 2007). Despite these negative consequences, many organisations, particularly those with commercial interests, have continued to use and consider the Internet as a lucrative business platform. However, in recent years, a notable change has taken place in terms of how online businesses interact with their customers, which has considerably changed traditional online business practices. This new paradigm shift involves the use of social media as a cost effective, convenient and efficient means of conducting business (Kaplan & Haenlein, 2010; Mangold & Faulds, 2009). As mentioned before, the concern for the susceptibility of information assets belonging to businesses operating on the Internet is on the rise and the emergence of online social media driven business models adds to, if not increases the concern for online security. Apart from businesses organisations, governmental and other non-profit organisations have also had their fair share of security issues in recent years. Recent incidents involving attacks on government systems using fake social media profiles is one good example (Constantin, 2013).

From an individual point of view, Symantec recently revealed consumers have high levels of trust in social media, which results in vast quantities of self-disclosed information (BusinessTech, 2013). This is not only limited to disclosure of information but extends to monetisation of social networks including the use of digital currency, purchase of virtual gifts and online credit used in services such as gaming and Voice over IP (VOIP). Cyber-criminals have taken to exploiting the information available on social media and commercial application on social media platforms. Cyber security predictions for 2013 include an increase in social media-oriented security threats such as malware attacks targeting monetary and non-monetary information, targeting both the individual users and online businesses (BusinessTech, 2013). Recent incidents such as the Sony PlayStation information security breach (Minihane, 2011), and criticisms against Facebook apps tracking/selling personal information (Hickins, 2012) suggest there is room for further enquiry pertaining to social media security and privacy.

Bearing such issues in mind, this chapter meets three objectives. First, a brief discussion of the historical development of security is presented followed by an analysis of the meaning of security and privacy in an online context. The intention of the analysis of security and privacy definitions is to highlight the conceptual differences between the two terms. This is in response to the criticism that the term 'security' is used in a somewhat "confusing manner in the industry" and that "some people equate security for privacy" (Bergeron, 2000).

The second objective of this chapter is to develop and attempt to prove that security and privacy on social media differ from the rest of the Web. One sect of scholars argues that 'virtual criminality' is the same as 'the terrestrial crime' differing "only in terms of the medium" of technology involved (Grabosky, 2001, p.243) and it is a case of 'old wine in new bottles' (Weir, Toolan, & Smeed, 2011, p.38). The opponents of this belief argue that this is not the case (Casprini & Di Minin, 2013, p.13) mainly owing to the differences in content and connectivity between 'Web 1.0 based network economy' and 'Web 2.0 network society'. Using prior works by Schneier (2010), Rose (2011) and other information security researchers, unique attributes of Social Networking Sites (SNS) are identified and it is argued that the information security and privacy risks of social media users are different from general Web users.

Thirdly, this chapter aims to discuss information security and privacy threats and their implications from individual and organizational perspectives, with emphasis on the evolution of the threat landscape from general Web security to SNS security. Organizational issues are discussed in terms of business and public sector security and