International Journal of Applied Management Sciences and Engineering
Volume 6 • Issue 1 • January-June 2019

Social Network Security Risks and Vulnerabilities in Corporate Environments

Fernando Almeida, Polytechnic Institute of Gaya, ISPGaya, Portugal
José Pinheiro, Polytechnic Institute of Gaya, ISPGaya, Portugal
Vítor Oliveira, Polytechnic Institute of Gaya, ISPGaya, Portugal

ABSTRACT

Increasingly social networks are used both in the personal and professional levels, being companies and employees also exposed to the risks posed by them. In this sense, it is relevant to analyze employees' perception of the risks and vulnerabilities posed by the use of social networks in corporate environments. For this purpose, a questionnaire was developed and distributed to 372 employees of small and medium-sized companies that allowed the characterization and analysis of those risks. The results indicate that the security risks are perceived moderately by employees, emphasizing the risk of defamation and cyberbullying as being the most pertinent. On the other hand, the findings indicate that older employees, the existence of lower academic qualifications, and those working in medium-sized companies are more aware of these risks.

KEYWORDS

Cyber Security, Security, Security Culture, Security Risks, Social Networks

INTRODUCTION

Social networks are part of everyday users' Internet browsing. Most of them use more than one social network and many of them participate actively in the activities of their group of friends in a social network. However, the use of these social networks leaves users exposed to a set of computer threats, which may harm the published information, the integrity of their personal data and behavior (e.g., postal address, daily routines, consumption habits, bank cards, etc.). In this sense, and with the growing tendency of virtual attacks to use social networks as a means of propagation, it is crucial for users to be protected and use their social networks safely.

For organizations, the safe use of social networks by their employees is a huge challenge. Most companies are only prepared to deal with phishing, malicious links and malware sent by email, but they do not systematically monitor social networking activities (Gangwar & Date, 2015). Social networks like Twitter, Facebook, Myspace or LinkedIn are a source for potential attackers to collect valuable business data or infiltrate in the company's network.

Some organizations, to avoid this issue, have banned and blocked the use of social networks inside the company. Control social media usage in the workplace has emerged as a priority for many

DOI: 10.4018/IJAMSE.2019010102

executives that see social networks as a reason for the decrease of productivity. However, this practice does not solve the problem, because employees can use their own devices to access social networks inside the organization. Additionally, prohibiting the full use of social networks is to ignore the potentialities that a social network can offer to the company, namely greater ease of communication between employees, establishing contact with customers, and improvement of work processes and knowledge transfer.

Needs of the Study

Considering the various approaches adopted by companies that many times are merely reactive to a security incident, emerge the need to have an established social media policy that could mitigate the risks of using social media networks by employees at their workplaces (Forbes, 2017). Additionally, this need is even greater for Small and Medium-sized Enterprises (SMEs) which according to the Allianz Risk Barometer 2018 are not prepared to respond to social media risks incidents that could potentially damage their technological infrastructure, which is vital for their daily operations (Allianz, 2018). The impact of these risks in the daily activities of SMEs is high and may affect not only their operations, but their branding and marketing strategies (Baporikar & Deshpande, 2017).

Objectives of the Study

This study aims to characterize and analyze the main security risks inherent in the use of social networks in corporate environments, particularly within SMEs. Additionally, this study intends to assess whether the employees' perception of these risks is different according to the employee's age, academic qualifications, number of years working in the company and SME' dimension. The manuscript is organized as follows: initially, a contextualization of the main studies available in the social security networks is performed. Next, the work methodology is presented and, after that, the main results are presented and discussed. Finally, the main conclusions are drawn.

Literature Review

Privacy and lack of regulation are one of the issues in using social networks. Spinelli (2010) looks at the effects this lack of regulations has had on the liberties guaranteed by the United States Constitution. In Europe, these issues are also not different or smaller. Kosta et al. (2010) identify also issues in European data protection legislation in the protection of private data of users in social networking. For its side, Abdulhamid et al. (2011) discuss the role of social networks in multiple perspectives, considering citizens, companies and governments. This study emphasizes the dual and antagonistic role of social networks as a conflicting and distorting element of national security, but also as a positive revolutionary force for social justice.

The use of social networks by employees is often accomplished without any security concerns in their behavior. Lehrman (2010) refers that one of the main goals of a cyberattack through social networking sites is to identify a vulnerable target, typically a user who will have access to high level of sensitive information. Baker et al. (2011) look at the impacts of its use considering both employee and company perspectives. This study indicates that a company can face lawsuits and bad publicity; on the employee side, we can see a decrease in their morale and the possible emergence of conflicts with other employees. Holm (2014) emphasizes the difficulties that social network users have in identifying security risks when sharing personal information online. On the same direction, Taylor et al. (2016) state the level of privacy provided by the social media, and the manner in which such privacy levels are defined and used by employees is an important factor in the type of misuse that might occur.

Wang & Kobsa (2009) identified three classes of potential privacy issues of using social networking at work: (i) impression management; (ii) pressure to reveal personal and working information; and (iii) unintentional social undermining in the workplace. Hasib (2009) sought to be more exhaustive and compiled a set of threats of using online social networks. These threats can be grouped into four