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 categories: (i) privacy related threats (e.g., digital dossier of personal information; face recognition; content-based image retrieval; image tagging and cross-profiling; difficulty of complete account deletion); (ii) social networking sites (SNS) variants of traditional network and information security threats (e.g., spamming; cross site scripting, viruses and worms; SNS aggregators; (iii) identity related threats (e.g., phishing; information leakage; profile squatting through identity theft); and (iv) social threats (e.g., stalking; corporate espionage). Devmane & Rana (2013) highlight three classes of risks in the use of online social sites, namely: (i) information leakage; (ii) spam; and (iii) profile cloning. In this field, one of the most complete studies was developed by Rathore et al. (2017) that classifies SNS security threats in three dimensions: (i) multimedia content threats (e.g., multimedia content exposure, share ownership, manipulation of multimedia content, steganography, metadata, shared links to multimedia content, static links, transparency of data centers, video conference, tagging, and unauthorized data disclosure); (ii) traditional threats (e.g., phishing, malware, sybil attack, spamming, clickjacking, de-anonymization attack, inference attack, profile cloning attack); and (iii) social threats (e.g., cyber-bullying and grooming, corporate espionage, cyber stalking).

In recent years, several studies have emerged that explore essentially the social threats of using social networks. These studies adopt a global perspective, involving the use of social networks regardless of their place of access. Lewis (2015) refers that despite the positive impact of social media in daily life, it also conversely exacerbates the risk of social media users being guilty of claims of defamation worldwide. Seabrook et al. (2016) report depression and anxiety symptoms motivated by the use of social networks. According to Best et al. (2014) social media use may increase an individual's exposure to negative social interactions like cyberbullying, which may negatively impact mood and mental health. The association between social media use and depression and anxiety symptoms has been used in studies to chart a usage profile that increases these risks. Primack et al. (2017) use logistic regression models to establish a linear association between the number of platforms used and depression and anxiety, whereas Shensa et al. (2018) identify 5-cluster distinct patterns of social media use to assess associations between those patterns and depression and anxiety.

There are also studies that explore the security challenges in social networks considering their features and particularities. Silic & Back (2016) conducted a study with Chief Information Security Officers (CISOs) in which they sought to understand employee behavior in using LinkedIn. The data of this study prove that employees are easily victimized by attacks on their personal information and organizations lack mechanics to control SNS online security threats. Jabee & Alam (2016) analyze the security challenges of Facebook users. Using a questionnaire sent to two universities in India it was possible to conclude that the majority of users (around 85%) of this social site intend improvements in default privacy settings and identify any scope of improvement in the security setting of Facebook.

Several authors have suggested guidelines for organizations. Patel & Jasani (2010) present a set of steps that should be adopted by organizations to encourage the secure participation of employees in social networks. Kumar et al. (2013) follow a distinct approach, and they establish a set of daily and operational practices that users must adopt to obtain greater security in the use of social networks in a business context. For its part, Almeida (2012) argues that a security policy should be based on four principles: (i) involvement of stakeholders; (ii) based on principles; (iii) effectively communicated; and (iv) alignment with current information security policies. Liang et al. (2014) extend the privacy analysis to mobile social networking and explore possible methods to deal with the associated security and privacy challenges considering three categories of mobile applications, such as autonomous platform, business card and service review.

Tayouri (2015) advocates that social media risks and damages may be reduced by combining education (e.g., formation, interactive video games) and technology (e.g., monitoring tools, check the reliability of friendship suggesting). The security awareness training should be tailored to focus on the potential strengths and weaknesses of each personality type. In this field, some regional initiatives have also emerged, such as Siddique's (2015) that report the implementation of employee training on security issues exploited by the use of networking sites in Dhaka city.

Some studies also intend to link the potential risk of social engineering attacks with the use of social networks. These studies are based on the idea that social networks provide an environment that facilitates the emergence of this type of attacks, mainly motivated by careless human behavior. Conteh & Schmick (2016) perform a critical reflection on social engineering attacks considering that it is difficult for organizations to have dedicated resources to pursue internet crimes and criminals. It is also worth mentioning the study by Edwards et al. (2017) in which the possibility of the existence of social engineering attacks on critical infrastructure organizations is demonstrated.

Finally, it is important to recognize the benefits brought by the use of social networks in a business context. Moqbel et al. (2013) found that social networking use intensity has a significant effect on job performance and increases job satisfaction indicator. They advocate that social networking sites can be used by employees to balance their work-life realms, which benefits all the organization. Ashraf & Javed (2014) advocate that the use of social networking like Facebook, Twitter, Slideshare and Linkedin have a positive impact on employee performance, which affect their skills/ability, knowledge/qualification, productivity/outcomes and motivation level. Yokoyama (2016) reports benefits and challenges of integrating them into human resources activities. The author advocates that HR professionals should use SNS as a component of their activities. Haddud et al. (2016) explore the relationship between internal social media usage and employee engagement with multinational North American organizations. The results provide evidence that internal social media usage is positively correlated with the level of employee engagement. Additionally, this study reveals that social media networks can also promote competencies of entrepreneurship, communication, and readiness for change. Lastly, Gunnlaugsdottir (2016) reports a positive attitude toward the use of social media and internet during the working time, if it is within an agreed limited and according to the policy of the organizations. This study reports that employees should not use more than 10% of their time at work on social media for private concerns.

Despite the important benefits brought by the adoption of social networks in SMEs mentioned by Bakeman & Hanson (2012) and Nobre & Silva (2014), namely in the marketing activities, to support collaboration among employees and to improve knowledge management, there is an absence studies to assess the privacy, safety and social risks of these employees' actions in the activities performed by companies, particularly in the SME segment. In this sense, conducting a study to assess the risks of using social networks in SME business context becomes relevant with potential impact at practical and scientific levels.

METHODOLOGY

This study aims to identify and characterize the practices adopted in the use of social networks by employees working on SMEs. The study adopts a quantitative approach and uses a questionnaire created using the Google Drive platform to gather this data. The questionnaire was distributed to the business partners of the educational institution and was also posted in two professional security groups on LinkedIN. It was available to the community during the entire month of April 2018.

The questionnaire is composed of 22 questions divided into four sections like it is depicted in Table 1. The first section (control data) aims to gather contextual information, such as the age, academic qualifications, size of the company and years of working in the company. Next, contextualization section intends to characterize the behavior pattern of employees in the use of social networks. Subsequently, it is intended to characterize the practices adopted by companies in the establishment of a security policy in the access and use of social networks. Finally, the last section intends to identify employees' perceptions about the risks that exist in the use of social networks in a business context. These risks were grouped in Table 2 according to those identified by each author. The following acronyms are used: "-" means that this security risk is not referred in a given study; "Y" the security risk is explicitly mentioned in a given study; whereas "P" means that the security risk is only implicitly considered. The main security risk referred by studies is the risk of access to private

Table 1. Structure of the questionnaire

Section	Description
Control data	Information regarding age, academic qualification, years of working in the company, and size of the company.
Contextualization	Information regarding the use of social networks in the business environment, usage regularly, usage in working hours, and awareness of social networks risks.
Practices adopted by companies	Policy adopted by companies in terms of security, formation and auditing.
Risks perception by employees	Seven risks were considered: (i) loss of productivity; (ii) malware installation; (iii) phishing; (iv) data leaks; (v) cyberbullying; (vi) defamation; and (vii) depression.

data, both personal and corporate. These risks were grouped together in a single dimension entitled "data leaks". Other risks like phishing and malware installation are also referred by some authors. Finally, in this study are still considered risks inherent in the loss of employee productivity and also social risks, such as cyberbullying, defamation and depression. The data of the Table 2 allow us to conclude that there are research gaps in exploring the social aspects of the security risks and vulnerabilities faced by employees at corporate environment. Most studies focus their analysis on the impact of these security risks for the company, considering essentially the productivity and technical dimensions, but don't look to the impact on employees.

In the majority of the questions, checkboxes and multiple choices were used. In the last section of the questionnaire we use a multiple-choice grid with the following scale: 1. not at all; 2. slightly; 3. moderately; 4. very; and 5. extremely. This approach allows respondents to easily identify each risk and respond quickly to the survey. Additionally, this format allows a comparative analysis of responses.

The use of a questionnaire allows us to deliver it to a large number of participants with little effort. Additionally, they provide an efficient means for data analysis, while ensuring the anonymity

Table 2. Classification and comparative analysis of security risks

Security Risk	Skeels & Grudin (2009)	Wang & Kobsa (2009)	Hasib (2009)	Devmane & Rana (2013)	Rathore et al. (2017)	Lewis (2015)	Seabrook et al. (2016)
Loss of productivity	Y	P	P	-	-	-	-
Privacy personal data	P	Y	Y	P	P	P	-
Privacy corporate data	P	Y	Y	P	P	P	-
Malware	-	-	Y	-	Y	-	-
Phishing	-	-	Y	-	Y	-	-
Corporate espionage	-	P	Y	-	Y	-	-
Profile cloning	-	-	P	Y	Y	-	-
Information leakage	-	Y	Y	Y	P	-	-
Multimedia content threats	-	-	-	-	Y	-	-
Clickjacking	-	-	-	-	Y	-	-
Cyber-bullying	-	-	-	-	Y	-	-
Defamation	-	-	-	-	-	Y	-
Depression and anxiety	-	-	-	-	-	-	Y

of responses (Queiros, Faria & Almeida, 2017). Some considerations were taken in designing the questionnaire, namely: (i) it must be usable so that the reader can easily understand, interpret and complete it; (ii) it is commonly accepted that a questionnaire should not be over long; (iii) similar question should be grouped under a common themed heading to help the respondent contextualize the subsequent questions; (iv) it is important to consider if each question will have the same meaning for everyone; and (v) different types of questions and scales should be used homogeneously. Finally, in order to avoid multiple responses from the same user, the IP address of respondent was collected to ensure that only the latter response is used in the data analysis process.

Finally, it is important to mention that in addition to the statistical analysis of the survey dimensions, it is also relevant to explore how some fundamental characteristics of employees and companies influence the perception of security risks in the use of social networks. In this sense, four research questions (RQs) were defined:

RQ1: Are the risks of using social networks perceived differently by employees with different age groups?
RQ2: Are the risks of using social networks perceived differently by employees with different academic qualifications?
RQ3: Are the risks of using social networks perceived differently by employees with different number of years working in the same company?
RQ4: Are the risks of using social networks perceived differently by employees working in different company's size?

FINDINGS AND DISCUSSION

A total of 395 responses were received. Twenty-two responses were considered invalid due to having some missing data. The final accepted sample is 372, which is a relevant and appropriate number to perform a quantitative data study. The collected data have the following distribution:

- **Age:** 102 (18-29 years old); 138 (30-39 years old); 98 (40-49 years old); 26 (50-59 years old); and 8 (60 years and over). Therefore, 64.52% of our respondents are under 40 years old;
- **Academic qualifications:** 33 (did not complete high school); 87 (high school); 118 (bachelor's degree); 101 (master's degree); and 33 (Ph.D. degree);
- **Number of years working in the company:** 101 (less than 1 year); 47 (1-3 years); 26 (3-5 years); and 198 (more than 5 years). It should be mentioned that 44.68% of the respondents who work less than one year in the same company are less than 30 years old;
- **Size of the company:** 13 (nano-enterprises); 44 (micro enterprises); 51 (small companies); and 264 (medium-sized companies). Therefore, 70.97% of our respondents work in medium-sized companies;
- **Used social networks:** Facebook is the most adopted social network with 368 of respondents in our sample, followed by LinkedIN, Google+ and Instagram. A total of 238 respondents (63.98%) reported that use social networks at work during only 5-15 minutes per day. Only 25 respondents (6.72%) reported more than one hour of daily use;
- **Use of social networks during working hours:** 202 respondents (54.3%) responded positively. Among them, they emphasized the use of social networks to exchange personal experiences and to interact with friends. Around 61% of the respondents emphasized that they use social networks essentially during job breaks. However, 89.25% of the respondents stated that they never left a business task to go to their social network;
- **Knowledge the risks of using social sites:** Only 22 respondents (5.91%) of the respondents stated that they don't know the risks of using social networks. On the other side, around 54%

stated that they know the risks and approximately 40% of the respondents declared that they know some of them;

- **Implementation of social networking security policies:** 122 respondents (32.8%) stated that their companies implement social networking security policies. However, a total of 142 respondents (38.17%) referred that their companies audit the use of social networks by employees. These results indicate that there are some companies that although they do not have any established security policy, the use of social networks is audited. On the other hand, the number of respondents (17.2%) who mentioned the existence of specific security formation in the use of social networks is much smaller.

Two further questions were raised in the survey whose analysis is fundamental to this study. The first intends to assess whether employees consider social networks are a problem for companies. The results obtained in Figure 1 are divergent and indicate that there is no consensus on this topic. The number of employees who strongly disagree or strongly agree is reduced, especially in those who fully agree with the existence of risks for the companies that represent only 2% of the respondents.

Another question raised was the identification of the typology of risks in using social networks. Table 3 summarizes the results obtained for each considered risk. It is possible to conclude that defamation and cyberbullying stand out as the main risks with a mean higher than 3. Nevertheless,

Figure 1. Opinion of employees on social networks issues for companies

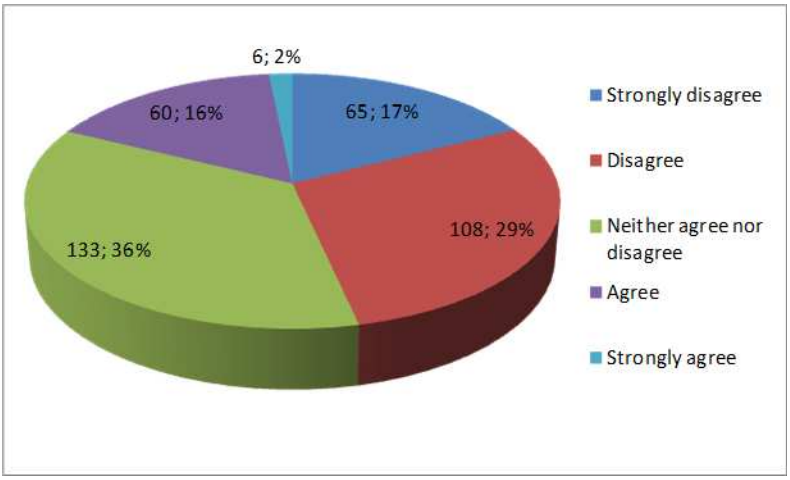

Table 3. Statistical analysis by risk typology

Type of Risk	Mean	Median	Std. Dev.
Loss of productivity	2.508	2	1.045
Malware installation	1.906	2	0.878
Phishing	2.148	2	0.876
Data leaks	2.229	2	0.911
Cyberbullying	3.083	3	1.052
Defamation	3.277	3	1.044
Depression	2.341	2	0.833

these two risks present the highest values of standard deviation along with the risk associated with the loss of productivity. This situation indicates that there is a high discrepancy in the response of employees to these questions.

RQ1: Are the risks of using social networks perceived differently by employees with different age groups?

A two-tailed t-test with a significance level of 5% (α=0.05) was performed in order to find evidence of a significant difference considering different age groups. For that, two classes of ages are considered: (i) 18-29 years old; and (ii) 60 years and over. These two classes are selected to test whether a significant age difference of respondents influences the perceived security risks of social networks in the business environment. The results of Table 4 indicate the existence of significant statistical evidence in the following dimensions:

- Younger respondents (age between 18 and 29) have a lower overall perception of social networks risks. The same situation occurs for the risks related to “loss of productivity”, “malware installation”, “phishing” and “data leaks”. The study conducted by Williams et al. (2009) also confirms this vision, in which it has been identified that younger online social network users are less concerned about information privacy and, consequently, they post more sensitive information on their profile which can increase their vulnerability to cyberattack. It is important to recognize that there are asymmetries within this age group (18-29 years old). Murnane (2016) states that younger millennials (18-24 years old) appear to be more sensitive than older millennials about protecting themselves online. Despite this observation, it is important to recognize that there is a quite consistent pattern in which young people tend to take a more liberal approach to issues around cyber security (Henley, 2013);
- Older respondents (60 years and over) have a greater perception of the existence of security risks in the use of social networks in a business environment. This is also true for “loss of productivity” and “malware installation” risks. Vyas & Choudrie (2013) conducted a study in the UK in which it was observed that privacy concerns towards online social networks have a negative effect on their adoption. Additionally, the findings of this study refer that most of the older people see the

Table 4. Hypothesis test for respondents’ age

Type of Risk	Mean of all Responses	Mean (age = 18-29)	Pr(|T| > |t|)	Mean (Age = 60 and Over)	Pr(|T| > |t|)
Overall perception of social networks risks	2.554	2.275	0.0087	3.875	0
Loss of productivity	2.508	1.990	0	3.625	0.0107
Malware installation	1.906	1.598	0.0001	2.75	0.0309
Phishing	2.148	1.814	0	2.75	0.0962
Data leaks	2.229	1.902	0	2.75	0.1404
Cyberbullying	3.083	3.029	0.6190	2.75	0.3233
Defamation	3.277	3.255	0.8224	3.375	0.8014
Depression	2.341	2.176	0.0347	2.5	0.4280

computer as a business tool, not something designed for personal purpose and social interactions. This limited use of technology by older people decreases their comfort level with technology. Therefore, the results obtained in this study can be understood as fundamental causes for a greater perception of the risks of social networks by older respondents.

RQ2: Are the risks of using social networks perceived differently by employees with different academic qualifications?

Three clusters were built: (i) did not complete high school plus high school respondents; (ii) respondents with BSc. and MSc. degrees; and (iii) respondents with PhD degree. The results of Table 5 indicate that respondents of the first cluster have a lower overall perception of social networks risks, while respondents of the third cluster show an opposite behavior. There is also significant statistical evidence on the risks of using social networks at the workplace in the following dimensions: (i) loss of productivity; (ii) phishing; and (iii) depression. In these three dimensions, respondents of the cluster 1 indicate a greater perception of these risks, whereas the respondents of the third cluster have an inverse perception.

The results suggest that employees' academic qualifications are an important factor in the awareness of the risks inherent in the use of social networks. Academic formation should also be complemented with workplace training. According to Safa et al. (2015) training in information security in organizations can play an important role in increasing the perception of these risks, and it is likely that this impact will be higher among employees with lower academic qualifications.

RQ3: Are the risks of using social networks perceived differently by employees with different number of years working in the same company?

This study also intends to assess whether the number of years working in an organization has impact on the perception of the risks inherent in the use of social networks. The results of Table 6 are inconclusive, and it is not possible to identify significant statistical evidence in all analyzed dimensions. Likewise, the overall perception of social networks is quite asymmetric, and it is not possible to establish a pattern in relation to the respondents' professional experience.

Table 5. Hypothesis test for academic qualifications

Type of Risk	Mean (aq = cluster1)	Pr(|T| > |t|)	Mean (aq = cluster2)	Pr(|T| > |t|)	Mean (aq = cluster3)	Pr(|T| > |t|)
Overall perception of social networks risks	2.325	0.0117	2.575	0.7543	3.242	0
Loss of productivity	2.867	0.0010	2.365	0.0273	2.152	0.0196
Malware installation	2.208	0.0006	1.753	0.0057	1.818	0.5370
Phishing	2.392	0.0052	2.064	0.1365	1.818	0.0138
Data leaks	2.583	0.0002	2.073	0.0048	1.970	0.0619
Cyberbullying	3.183	0.3811	3.087	0.9550	2.697	0
Defamation	3.383	0.3379	3.274	0.9644	2.909	0
Depression	2.667	0.0003	2.196	0.0051	2.121	0.0047

Table 6. Hypothesis test for respondents' professional experience

Type of Risk	Mean (nyw < 1)	Pr(|T| > |t|)	Mean (1 ≤ nyw < 3)	Pr(|T| > |t|)
Overall perception of social networks risks	1.980	0	3.170	0
Loss of productivity	2.673	0.0700	2.000	0
Malware installation	2.000	0.1758	1.660	0.0107
Phishing	2.317	0.0101	1.915	0.0132
Data leaks	2.505	0.0009	1.979	0.0104
Cyberbullying	3.554	0	3.043	0.3468
Defamation	3.663	0	3.106	0.0031
Depression	2.426	0.2435	2.085	0.0001
Type of Risk	**Mean (3 ≤ nyw ≤ 5)**	**Pr(|T| > |t|)**	**Mean (nyw > 5)**	**Pr(|T| > |t|)**
Overall perception of social networks risks	3.654	0	2.556	0.9824
Loss of productivity	2.385	0.4900	2.561	0.5330
Malware installation	1.577	0.0614	1.960	0.4478
Phishing	2.038	0.5271	2.131	0.8162
Data leaks	2.192	0.8275	2.152	0.2726
Cyberbullying	2.962	0.2516	2.869	0.0142
Defamation	3.038	0.0016	3.152	0.1482
Depression	2.077	0.0021	2.394	0.4458

RQ4: Are the risks of using social networks perceived differently by employees working in different company's size?

The results of Table 7 suggest that structure of the company is a determining factor in the perception of the risks of the use of social networks in a business environment. Nano-enterprises (<3 employees) and micro-companies (<10 employees) are less aware of these risks, while employees of medium-sized companies (<250 employees) are more aware of these risks. For small companies (<50 employees) it was not possible to identify statistical significance. Cyberbullying and defamation emerge as the two dimensions that exhibit significant statistical evidence in these three types of firms, such that employees of nano-enterprises and micro companies consider that the risks of these two dimensions are higher to those experienced by employees of medium-sized companies.

These results confirm the concerns suggested by several experts in the security field that small and medium-sized businesses are potential victims of a cyberattack (Banham, 2017; Simpson, 2017; Wall, 2018). On the other hand, Camillo (2017) advocates that the rapid pace of technological change and the growing connectivity of devices increase the cyber vulnerabilities to medium-sized companies. In this sense, the results obtained reflect the safety concerns expressed by employees of medium-sized companies. Despite this, the perceived risks in the dimensions of cyberbullying and defamation are smaller within medium-sized companies.

In smaller companies (nano-enterprises and micro companies) the perception of risks is smaller since these companies typically have a smaller and more flexible organizational structure. In this cluster of companies, it is typical to find company's security practices that are not formally defined

Table 7. Hypothesis test for respondents' company's size

Type of Risk	Mean (Nano-Enterprise)	Pr(|T| > |t|)	Mean (Micro)	Pr(|T| > |t|)
Overall perception of social networks risks	1.769	0.0005	1.773	0
Loss of productivity	3.462	0.0008	2.727	0.0719
Malware installation	2.538	0.0048	1.932	0.7968
Phishing	2.538	0.0543	2.432	0.0013
Data leaks	2.538	0.1168	2.568	0.0002
Cyberbullying	4.077	0.0013	3.682	0
Defamation	4.000	0.0145	3.705	0.0002
Depression	3.231	0.0081	2.341	0.990
Type of Risk	**Mean (Small)**	**Pr(|T| > |t|)**	**Mean (Medium-Sized)**	**Pr(|T| > |t|)**
Overall perception of social networks risks	2.608	0.7396	2.712	0.0081
Loss of productivity	2.412	0.3090	2.443	0.3503
Malware installation	2.000	0.3372	1.852	0.3527
Phishing	2.255	0.1790	2.061	0.1408
Data leaks	2.451	0.0773	2.114	0.0501
Cyberbullying	3.275	0.0199	2.898	0.0075
Defamation	3.510	0.0035	3.125	0.0295
Depression	2.118	0.0001	2.341	0.9987

and, therefore, the employees' behavior is expected to be close to those adopted in their personal context. However, this does not mean that it is not equally important to establish security policies on the part of these companies since many of them make a significant contribution to the national economy. This view is confirmed by Heidenreich (2017) that states that the limited resources of those companies can threaten innovative micro-enterprises as sensitive data may become accessible to malevolent parties.

CONCLUSION

The analysis of the risks posed by the use of social networks in SMEs is a pertinent subject and offers considerable practical applicability. Increasingly companies in the security field establish policies and define security guides to be adopted by SMEs. However, despite this growth interest, it is recognized that most of the risks inherent in the use of social networks are related to the behavior of employees. In this sense, this study proved to be important in the characterization of security perception among SME employees.

The study identified that the perceived security risks posed by the use of social networks in the company are very heterogeneous, with most respondents stating that their impact on the digital security of companies is moderate. Within the various risks assessed, the risk of defamation and cyberbullying emerge as being those that are considered most relevant. These results show that the social dimension risks of using social networks at workplace overlaps their technological dimension risks.

It was also tested whether the perceived security risks were different according to the profile of the respondents. It was possible to conclude that age of employees, their academic qualifications and the company's size are three elements that present significant statistical evidence. Thus, older employees and those with lower academic qualifications tend to have a higher perception of the risks posed by social networks. Concerns about the vulnerabilities posed by the use of social networks in companies are, for their part, mainly addressed to employees working in medium-sized companies.

MANAGERIAL IMPLICATIONS, LIMITATIONS AND FUTURE RESEARCH

As practical implications, the results of this study and the bibliography on social media security domains suggest the need to establish a security policy that also include the social risks of using social networks. Equally important is the establishment of training in this area primarily directed to older employees and with less academic qualification, which typically feel a greater perception of the risks and insecurity in the use of social networks. This security policy must be defined for all SMEs, but is even more relevant for medium-sized companies that have between 50 and 250 employees.

This study presents some limitations that should be properly considered. Firstly, this study adopts only a quantitative approach. A combination of a quantitative and qualitative technique could enrich the study to obtain more detailed and contextual information for each considered security risk. Another limitation of this study is the non-collection of information regarding the sector of activity of each SME. In this sense, and as future work, we intend to explore the impact of this dimension through the use of a mixed method approach. Additionally, it would be important to look in detail for the characteristics of each social network and to the access device. Not only the traditional desktop computers and laptops are at risk, but also users are increasingly accessing corporate social networks through mobile phones. In this sense, it will be relevant to consider a study that can simultaneously look to both characteristics.

REFERENCES

Abdulhamid, S., Ahmad, S., Waziri, V., & Jibril, F. (2011). Privacy and National Security Issues in Social networks: The Challenges. *International Journal of the Computer, the Internet and Management, 19*(3), 14-20.

Allianz. (2018). Allianz Risk Barometer 2018: SME Business Risks. Retrieved June 5, 2018, from http://www.agcs.allianz.com/insights/expert-risk-articles/arb2018-sme-business-risks/

Almeida, F. (2012). Web 2.0 Technologies and Social Networking Security Fears in Enterprises. *International Journal of Advanced Computer Science and Applications*, *3*(2), 152–156. doi:10.14569/IJACSA.2012.030226

Ashraf, N., & Javed, T. (2014). Impact of Social Networking on Employee Performance. *Business Management and Strategy*, *5*(2), 139–150. doi:10.5296/bms.v5i2.5978

Bakeman, M., & Hanson, L. (2012). Bringing Social Media to Small Business: A Role for Employees and Students in Technology Diffusion. *Business Education Innovation Journal*, *4*(2), 106–111.

Baker, D., Buoni, N., Fee, M., & Vitale, C. (2011). Social networking and its effects on companies and their employees. Retrieved from http://www.neumann.edu/about/publications/NeumannBusinessReview/journal/Review2011/SocialNetworking.pdf

Banham, R. (2017). Cybersecurity threats proliferating for midsize and smaller businesses. *Journal of Accountancy*, *7*, 1–5.

Baporikar, N., & Deshpande, M. (2017). SMEs and Branding Strategies. *International Journal of Applied Management Sciences and Engineering*, *4*(1), 43–55. doi:10.4018/IJAMSE.2017010104

Best, P., Manktelow, R., & Taylor, B. (2014). Online communication, social media and adolescent wellbeing: A systematic narrative review. *Children and Youth Services Review*, *41*, 27–36. doi:10.1016/j.childyouth.2014.03.001

Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy*, *2*(1), 53–63. doi:10.1080/23738871.2017.1296878

Conteh, N., & Schmick, P. (2016). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31–38. doi:10.19101/IJACR.2016.623006

Devmane, M., & Rana, N. (2013). Security Issues of Online Social Networks. In S. Unnikrishnan, S. Surve, & D. Bhoir (Eds.), *Advances in Computing, Communication, and Control. Communications in Computer and Information Science*. Springer. doi:10.1007/978-3-642-36321-4_69

Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017). Panning for gold: Automatically analysing online social engineering attack surfaces. *Computers & Security*, *69*, 18–34. doi:10.1016/j.cose.2016.12.013

Forbes. (2017). Why Your Business Needs A Social Media Policy And Eight Things It Should Cover. Retrieved from https://www.forbes.com/sites/forbeshumanresourcescouncil/2017/05/25/why-your-business-needs-a-social-media-policy-and-eight-things-it-should-cover/#7428e8bd5264

Gangwar, H., & Date, H. (2015). Exploring Information Security Governance in Cloud Computing Organisation. *International Journal of Applied Management Sciences and Engineering*, *2*(1), 44–61. doi:10.4018/ijamse.2015010104

Gunnlausgsdottir, J. (2016). Employee Use of Social Media for Private Affairs During Working Hours. *The Journal of Social Media in Society*, *5*(3), 121–150.

Haddud, A., Dugger, J., & Gill, P. (2016). Exploring the Impact of Internal Social Media Usage on Employee Engagement. *Journal of Social Media For Organizations*, *3*(1), 1–22.

Hasib, A. (2009). Threats of Online Social networks. *International Journal of Computer Science and Network Security*, *9*(11), 288–293.

Heidenreich, M. (2017). How to design a method for measuring IT security in micro enterprises for IT security level measuring? A literature analysis. In *Proceedings of the Communication and Information Technologies (KIT)*, Vysoke Tatry, Slovakia (pp. 1-9). doi:10.23919/KIT.2017.8109447

Henley, J. (2013). Are teenagers really careless about online privacy? *The Guardian*. Retrieved from https://www.theguardian.com/technology/2013/oct/21/teenagers-careless-about-online-privacy

Holm, E. (2014). Social networking and identity theft in the digital society. *International Journal on Advances in Life Sciences*, *6*(3-4), 157–166.

Jabee, R., & Afshar, M. (2016). Issues and Challenges of Cyber Security for Social Networking Sites (Facebook). *International Journal of Computers and Applications*, *144*(3), 36–40. doi:10.5120/ijca2016910174

Kosta, E., Kalloniatis, C., Mitrou, L., & Gritzalis, S. (2010). Data protection issues pertaining to social networking under EU law. *Transforming Government: People*. *Process and Policy*, *4*(2), 193–201.

Kumar, D., Varma, P., & Pabboju, S. (2013). Security issues in social networking. *International Journal of Computer Science and Network Security*, *13*(6), 120–124.

Lehrman, Y. (2010). The Weakest Link: The Risks Associated with Social Networking Websites. *Journal of Strategic Security*, *3*(2), 63–72. doi:10.5038/1944-0472.3.2.7

Lewis, C. (2015). Social Media: Cyber trap door to defamation. *Masaryk University Journal of Law and Technology*, *9*(1), 65–84. doi:10.5817/MUJLT2015-1-5

Liang, X., Zhang, K., Shen, X., & Lin, X. (2014). Security and privacy in mobile social networks: Challlenges and solutions. *IEEE Wireless Communications*, *21*(1), 33–41. doi:10.1109/MWC.2014.6757895

Mogbel, M., Nevo, S., & Kock, N. (2013). Organizational members' use of social networking sites and job performance: An exploratory study. *Information Technology & People*, *26*(3), 240–264. doi:10.1108/ITP-10-2012-0110

Murnane, K. (2016). How older and younger millennials differ in their approach to online privacy and security. *Forbes*. Retrieved from https://www.forbes.com/sites/kevinmurnane/2016/04/13/how-older-and-younger-millennials-differ-in-their-approach-to-online-privacy-and-security/#deb4b6c9aa3b

Nobre, H., & Silva, D. (2014). Social Network Marketing Strategy and SME Strategy Benefits. *Journal of Transnational Management*, *19*(2), 138–151. doi:10.1080/15475778.2014.904658

Patel, N., & Jasami, H. (2010). Social Media Security Policies: Guidelines for Organizations. *Issues in Information Systems*, *XI*(1), 628–634.

Primack, B., Shensa, A., Escobar-Viera, C., Barrett, E., Sidani, J., Colditz, J., & James, E. (2017). Use of multiple social media platforms and symptoms of depression and anxiety: A nationally-representative study among U.S. young adults. *Computers in Human Behavior*, *69*, 1–9. doi:10.1016/j.chb.2016.11.013

Queiros, A., Faria, D., & Almeida, F. (2017). Strengths and Limitations of Qualitative and Quantitative Research Methods. *European Journal of Education Studies*, *3*(9), 369–387.

Rathore, S., Sharma, P., Loia, V., Jeong, Y., & Park, J. (2017). Social network security: Issues, challenges, threats, and solutions. *Information Sciences*, *421*, 43–69. doi:10.1016/j.ins.2017.08.063

Safa, N., Sookhak, M., Van Solms, R., Furnell, S., Ghani, N., & Herawan, T. (2015). Information security conscious care behavuoir formation in organizations. *Computers & Security*, *53*, 65–78. doi:10.1016/j.cose.2015.05.012

Seabrook, E., Kern, M., & Rickard, N. (2016). Social Networking Sites, Depression, and Anxiety: A Systematic Review. *JMIR Mental Health, 3*(4). Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5143470/

Shensa, A., Sidani, J., Dew, M., Escobar-Viera, C., & Primack, B. (2018). Social Media Use and Depression and Anxiety Symptoms: A Cluster Analysis. *American Journal of Health Behavior*, *42*(2), 116–128. doi:10.5993/AJHB.42.2.11 PMID:29458520

Siddique, T. (2015). Use of social networking sites at workplace in Bangladesh: employees' perspective. *Global Disclosure of Economics and Business*, *4*(2), 197–204.

Silic, M., & Back, A. (2016). The dark side of social networking sites: Understanding phishing risks. *Computers in Human Behavior*, *60*, 35–43. doi:10.1016/j.chb.2016.02.050

Simpson, A. (2017). 5 Reasons Cyber Security Is Failing and What P/C Insurers Can Do About It. Retrieved from https://www.insurancejournal.com/news/national/2017/08/18/461482.htm

Skeels, M., & Grudin, J. (2009). When social networks cross boundaries: A case study of workplace use of Facebook and LinkedIn. Retrieved from http://research.microsoft.com/enus/um/people/jgrudin/publications/newwave/socialnetworking2009.pdf

Spinelli, C. (2010). Social Media: No 'Friend' of Personal Privacy. *The Elon Journal of Undergraduate Research in Communications*, *1*(2), 59–69.

Taylor, M., Haggerty, J., Gresty, D., Wren, C., & Berry, T. (2016). Avoiding the misuse of social media by employees. *Network Security*, *2016*(5), 8–11. doi:10.1016/S1353-4858(16)30047-2

Tayouri, D. (2015). The human factor in the social media security - combining education and technology to reduce social engineering risks and damages. *Procedia Manufacturing*, *3*, 1096–1100. doi:10.1016/j.promfg.2015.07.181

Vyas, A., & Choudrie, J. (2013). Online Social Networking In Older Individuals: A Study Of Hertfordshire. *ECIS 2013 Completed Research*, 93. Retrieved from http://aisel.aisnet.org/ecis2013_cr/93

Wall, E. (2018). Cyber security threats and provisions for SMEs. Retrieved May 8, 2018, from https://www.itproportal.com/features/cyber-security-threats-and-provisions-for-smes/

Wang, Y., & Kobsa, A. (2009). Privacy in Online Social Networking at Workplace. In *Proceedings of the International Conference on Computational Science and Engineering (CSE'09)*, Vancouver, Canada. doi:10.1109/CSE.2009.438

Yokoyama, M. (2016). How social network sites (SNS) have changed the employer–employee relationship and what are the next challenges for human resource (HR)? *REGE – Revista de Gestão, 23*(1), 2-9.

Fernando Luís Almeida has a PhD in Computer Science Engineering from Faculty of Engineering of University of Porto (FEUP). He holds also MSc in Innovation and Entrepreneurship and MSc in Informatics Engineering from FEUP. He has around 7 years of teaching experience at higher education levels in the field of computer science and management. He has also worked for 10 years in several positions as software engineer and project manager for large organizations and research centers like Critical Software, CICA/SEF, INESC TEC and ISR Porto. During that time, he had the possibility to work in partnership with big international organizations and universities in several European projects. His current research areas include security risks, entrepreneurship, software development and decision support systems.

José Pinheiro has a BSc. in Computer Systems and Networks from Higher Polytechnic Institute of Gaya (ISPGaya). He works in the computer industry field as network administrator. His current research areas include networking management and security policies.

Vitor Oliveira has a BSc. in Computer Systems and Networks from Higher Polytechnic Institute of Gaya (ISPGaya). He works in the computer industry field as software developer. His current research areas include software methodologies, internet security policies and software maintenance.