DETERMINING THE MAIN CAUSES THAT LEAD TO CYBERSECURITY RISKS IN SMES

Andrei-Laurențiu MITROFAN
Faculty of Entrepreneurship, Business Engineering and Management – University POLITEHNICA of Bucharest, Bucharest, Romania
andrei_mitrofan@yahoo.com

Elena-Veronica CRUCERU
Faculty of Entrepreneurship, Business Engineering and Management – University POLITEHNICA of Bucharest, Bucharest, Romania
elena_cruceru97@yahoo.com

Andreea BARBU
Faculty of Entrepreneurship, Business Engineering and Management – University POLITEHNICA of Bucharest, Bucharest, Romania
barbu.andreeab@yahoo.com

Abstract

The online environment brings business opportunities and connections that can help the development of small and medium companies, but it also contains many risks. The objectives proposed for this research are to identify the main concerns of entrepreneurs regarding cybersecurity and to determine the main causes of cybersecurity risks in micro, small, and medium-sized enterprises (SMEs). To determine the main causes that lead to the emergence of existing cybersecurity risks in SMEs, the authors conducted primary research, using the survey method through an online questionnaire. Among the research results it can be mentioned the need to strengthen the defense structure against cyberattacks for SMEs. The authors highlighted the issues related to the low level of preparation that entrepreneurs have regarding cyber threats because in a dynamic environment, such as cyberspace, the most vulnerable companies are those that do not invest in the cybersecurity structure.

Keywords: cybersecurity, cyberspace, causes of cyberattacks in SMEs, cybersecurity risks in SMEs, lack of cybersecurity knowledge of SMEs entrepreneurs

1. INTRODUCTION

Nowadays, the Internet connection has become vital for businesses of all sizes. Due to the rapid development of technology, everyone uses cyberspace daily, for at least one activity, and some users are not paying enough attention or are not aware as a result of a lack of knowledge about risks that can appear in this environment.

The cyberspace consists of all computers, interconnected data networks, and all services related to the internet (Vevera, 2016). Cyberspace is invading almost every field, from video games to work or socializing, which is why it is increasingly important for people to understand the basics and technical operations of cyberspace, as well as the capabilities, threats, and the impact on the individual's daily life.

The contexts that can lead to cyberattacks on Small Medium-sized Enterprises (SMEs) are diverse and multiple, making it difficult for a company to understand them all, but by knowing the basics on which cyberattacks can occur, companies will be able to reduce the risk of spreading these attacks.

Today, companies are creating easy environments that lead to the creation of effective business practices based more than ever on technology. Therefore, by accessing a dynamic environment, every company and every employee must be able to understand that it is prone to cyberattacks, and to minimize the risks of their occurrence, they must create cybersecurity actions to combat these attacks.

The existence of cybercrime, through various actors (states, criminal groups, and hacktivists), is a growing threat to micro, small and medium enterprises (SMEs). A study conducted by the University of Maryland (Cukier, 2007) claimed that the attacks are growing, hackers attacking every 39 seconds, which brings to a total of about 2.444 times/day, the attacks happening all the time on computers with internet connections.

Thus, the object of this paper is to determine the main causes leading to existing cybersecurity risks in SMEs. To achieve this goal, the authors sought to identify the main concerns of entrepreneurs regarding cybersecurity through interviews, identify existing cybersecurity threats, vulnerabilities and risks in SMEs, and determine the main causes of cybersecurity risks in SMEs.

These objectives proposed by the authors are intended to help SME entrepreneurs to become aware of existing cyber risks and how these risks can be mitigated or eliminated; the lack of knowledge in cybersecurity is the main problem identified and analyzed by the authors.

2. LITERATURE REVIEW

Due to the lack of reliable data, it is difficult to estimate the impact of inadequate preparedness for cyberattacks. The economic impact of cybercrime has increased fivefold between 2013 and 2017, affecting both governments and businesses, regardless of their size. This trend is reflected by the projected increase in cyber insurance premiums, from € 3 billion in 2018 to € 8.9 billion in 2020 (European Book of Accounts, 2019).

As the financial impact of cyberattacks continues to grow, there is an alarming discrepancy between the costs of launching an attack and the costs of prevention, investigation, and repair. For example, € 15 per month is sufficient to carry out a Distributed Denial-of-Service (DDoS) attack, while the losses suffered by the companies concerned, including damage to their reputation, are considerably higher (European Book of Accounts, 2019).

Although 80% of companies in the European Union (EU) faced at least one cybersecurity incident in 2016, the level of risk awareness is still alarmingly low. 69% of EU businesses do not understand their exposure to cyber threats or have only a vague idea of it, and 60% have never estimated potential financial losses. Besides, according to a global study, a third of organizations would rather pay the ransom demanded by a hacker than invest in information security (European Book of Accounts, 2019).

The global attacks Wannacry (ransomware) and NotPetya (malware of deletion) affected more than 320.000 victims in about 150 countries in 2017. These incidents have led to some global "awakening" to the threat posed by cyberattacks, with a new impetus to integrate cybersecurity into conventional policy reflection. Besides, 86% of EU citizens now believe that the risk of becoming a victim of cybercrime is increasing (European Book of Accounts, 2019).

The days when few SMEs were targeted by cyberattacks are gone. It is now very profitable for cybercriminals to target SMEs because they are easier to attack than large companies. In the last 12 months, 21% of SMEs have been the victims of a cyberattack. Even if the damage from these attacks rarely exceeds 10.000 euros, there are rare cases in which the victim companies do not recover, especially in situations where the case becomes public (Spella, 2019).

According to (MXHOST, 2019), there were 7 billion records of cyberattacks exposed by the second half of 2017, of which 97% of them could have been avoided, using basic security protocols. Only 14% of online small business owners put cybersecurity first. The main problem is that 60% of small companies will go bankrupt after the first cyberattack.

Researches from all over have also begun to investigate various aspects of cybersecurity, from preventive measures (Khan & AlShare, 2019), vulnerabilities (Humayun et al., 2020), risks (Kure et al., 2018), effects (Smith et al., 2019; Asslani et al., 2018), strategies (Boys, 2018; Kovács, 2018) to the impact that this topic has on a company's employees (Li, et al., 2019). If in the past, much of the research focused on studies of cyberattacks among large companies, now the focus has begun to turn to the SMEs.

Over the last few years, many researchers have started to analyze the main causes and problems of cyber-attacks in the case of SMEs, and also the factors that can be considered important in implementing information security management. The analyzed studies showed that in the case of SMEs, one of the most common problems is the bad password (Jenkins et al., 2013; Lee & Yim, 2020).

Among the biggest problems that small companies face (compared to large companies) are the following: there is no specific department or team to deal with security issues, there is no separate budget to deal with security issues, not enough resources are allocated for security issues or there are no specialists in the area of data security in the IT department (Dekýš, 2010). Taking into account these aspects, SMEs are a very easy target for cyber attackers who are looking for small companies with simple goals and a minimal investment in security (Millaire et al., 2017; Závadský & Závadský, 2018).

There are several factors that SMEs do not take into account when it comes to cybersecurity. These factors consist of: their strategy against threats, training their own employees, and solutions that ensure recovery in case of an attack on their systems. According to a report by Hiscox (2018), almost half (52%) of small businesses have a clearly defined strategy around cybersecurity, which is worrying because there is a very high percentage who say that most SMEs are not prepared to do so. cope with cyber threats. This report also claims that less than a third (32%) of small businesses conducted phishing experiments to assess employee behavior and availability in the event of an attack, which does not include even half of all companies, being a problem. obvious impact on SMEs.

One of the SMEs' problems is that they are so preoccupied with the simple goals that they don't even know they are the victims of cyber-attacks or find out about these problems much too late, sometimes even a year after the appearance of these attacks (Hau et al., 2016).

Alahmari and Duncan (2020) highlighted in their systematic literature review about the Cybersecurity Risk Management in Small and Medium-Sized Enterprises that there are 5 main dimensions that companies should focus on: threats, behaviors, practices, awareness, and decision-making.

According to (Kabanda et al., 2018), there are five factors that influence how SMEs perceived cybersecurity: the budget of the company, IT complexity, attitude toward security, the lack of management support, and compliance to regulations. The last two elements were also highlighted by (Ključnikov et al., 2019) who also reminds us that security controls and organizational awareness are success factors in the security department.

Concerns over the rise of cyberattacks in the context of the COVID-19 pandemic in December 2019 have created a panic that has led entrepreneurs to claim that they intend to allocate more resources to cybersecurity in 2020. countries that have a weaker defense are even more vulnerable to cyber-attacks. A similar survey by the Cyber Readiness Institute (CRI) on small businesses found that 60% of small businesses do not have a cybersecurity policy. The survey, which included 412 small business owners, found that while most of the small business owners are worried about cyberattacks, many do not have the resources to invest in the necessary security measures, and half of them are worried that work at a distance will lead to more problems from cyberspace on companies (CISCOMAG, 2020).

In the last 5 years, Romanian researchers have started to analyze the cybersecurity situation in Romania as well, the papers from 2020 representing a quarter of the total articles published on Google

Scholar in the period 2015-2020 (4400 articles in total), very few of them analyzing the situation of SMEs in Romania, especially in terms of cybersecurity risks.

According to (CERT-RO, 2018), it was found that the main problem detected in Romania in 2018 is represented by the vulnerabilities in companies' systems. More than 80% of incident classes refer to the issue of vulnerabilities, which means that companies do not pay too much attention to updates to the programs and operating systems used, which leads to their exploitation. Also, the second type of threat highlighted by CERT-RO is a botnet, which makes this threat a bigger problem, due to the fact that any infection from a botnet can turn that device into part of the botnet network. of which the malicious part is part. These two attacks eventually lead to compromised systems.

Lately, the advancement of technology has brought added value among many companies but cyberattacks have developed and are increasingly present and dangerous. At the same time, with this continuous development, those in charge of SMEs are becoming more and more aware of technology, its advantages and also its disadvantages, and, theoretically, they should protect companies from possible attacks that are more dangerous than ever. Thus, this paper aims to analyze the main causes leading to the existing cybersecurity risks in Romanian SMEs by analyzing the main concerns of entrepreneurs regarding the cybersecurity sector.

3. METHODOLOGY

To determine the main causes that lead to the emergence of existing cybersecurity risks in SMEs, the authors conducted primary research, using the survey method. As a working tool, the authors used the online questionnaire, which was created using the Google Forms platform. Using the two fundamental concepts of research, namely measurement, and scaling, we determined that:

- assuming that the objectives set out above must be explored, namely identifying the main concerns of entrepreneurs regarding cybersecurity and determining the main causes of cybersecurity risks in SMEs, and this way the paper will answer the question "What do we measure?"
- using Google Forms to record the answers, interpreting them later the paper will answer to the question "How do we measure?"

The questionnaire used in this research contains the filter question "Is there a cybersecurity department in your company?", a question that will have the role of dividing entrepreneurs between those who have a cybersecurity department and those who do not have this department. The questions addressed to both categories can be seen in the appendix. Of the two categories of entrepreneurs, through this research, efforts and analysis will focus on entrepreneurs who do not have a cybersecurity department in their company. Thus, for this pilot study, the authors analysed the responses of the 10 entrepreneurs who do not have a cybersecurity department in their company.

For this category of entrepreneurs, the proposed questions are divided as follows: one question with grid answer, only one answer can be chosen, and four open-ended questions. To maintain the confidentiality of the data, the names of the entrepreneurs and the companies they run will not be disclosed.

4. RESULTS

The authors sent the online questionnaire to 50 entrepreneurs who own SMEs from Bucharest and obtained a response rate of 20%. The analysed companies have over five years of experience, they are active in different industries from pharma to agriculture, from small shops to the construction industry. The authors are not allowed to offer more information because these represent security concerns.

All 10 entrepreneurs who own companies with several employees (between 7 and 15 employees) continued the interviews with the second part of the questions, formulated especially for those who do not have a cybersecurity department. Table 1 presents the analysed variables, as well as the questions used in this analysis.

TABLE 1. ANALYZED VARIABLES AND QUESTIONS

Analyzed variables	Questions
The responsible for cybersecurity	Who handles the security of the computer network in your company?
Solutions	What solutions you or the person in charge of ensuring security for your company against cyberattacks implemented?
General information about the current situation	Are you informed about the possible attacks that can take place on SMEs in Romania, Europe, or the rest of the world?
Incident history	Have you had a cybersecurity incident against your company in the last year? (If yes, detail it)
Information about risk factors	Are you constantly informed about the elements that can lead to cybersecurity risks? (If yes, detail the sources from which you are informed)

Source: Authors' own contribution

Figure 1 shows the results obtained from the question "Who handles the security of the computer network in your company?" in the form of a pie-chart diagram.

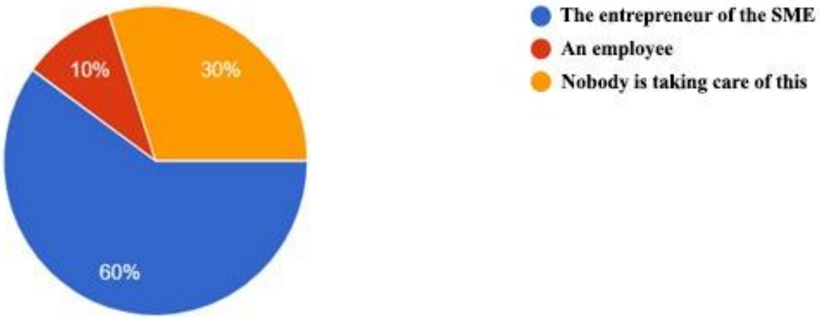

FIGURE 1. THE RESULTS OF THE QUESTION "WHO HANDLES THE SECURITY OF THE COMPUTER NETWORK IN YOUR COMPANY?"

Source: Authors' own contribution

Regarding the existence of a person responsible for the security of the computer network in the analysed company (Figure 1), it can be seen that 6 (60%) of the 10 entrepreneurs stated that they deal with the cybersecurity of their company, 1 (10%) among the respondents has a person responsible for this activity, and 3 (30%) claimed that no one in the company deals with this sector. Thus, it can be seen that in over 50% of cases, entrepreneurs are aware of the dangers that come from cyberspace and deal with the implementation of solutions.

For the solutions implemented within the company to ensure security against cyberattacks, the authors have identified that those solutions are 70% based on the use of licensed antivirus for computers and laptops in the company, which means that it provides minimal security, but often insufficient for all types of attacks.

Seven entrepreneurs of these 10 stated that they pay for these antivirus licenses, and of these 7, 5 entrepreneurs do not consider other solutions for their companies to be unnecessary. One of the contractors confirmed that he uses the antivirus for monthly scans, and the others claimed that they only make these licenses available to employees, and what happens next is the employees' problem and considers that everyone is responsible for his actions.

Two of the entrepreneurs confirmed that they have implemented other solutions besides antivirus. The one who stated that he attaches more importance to cybersecurity and who brought the most solutions to reduce the risks of a cyber problem for his company is the one who has a person in charge of implementation. The entrepreneur stated that he is passionate about this field. He made several implementations on the company, such as weekly scans for each computer, checking for the latest updates of operating systems and applications and, where appropriate, updating them, configured the firewall of the router, and implemented a system that sends emails to all employees of the company within one month asking them to change passwords for important accounts they use and confirmation after each has successfully changed their password.

The second entrepreneur to bring an implementation in addition to antivirus confirmed that he attaches importance to the complexity of password security for all accounts held by him and his employees and therefore bought licenses for Keeper Password Manager, a password manager that helps employees manage all their accounts by storing them in this application, and so they can put more complex passwords to their accounts.

The negative part determined by this study consists of the statements made by three of the entrepreneurs who do not consider it necessary to implement solutions to secure their network in reducing the risk of cyber events for implausible reasons. They consider that:

- the company is not a target for a cyberattack;
- employees must be responsible for their actions;
- the negative actions of employees have consequences that they must bear.

In terms of information on possible attacks on SMEs in Romania, Europe or the rest of the world, 90% of respondents said they were not interested in finding out about existing attacks, except for one of the entrepreneurs who he has an employee who deals with the cybersecurity of the company.

In the case of these entrepreneurs, there is misinformation, which leads to the risk of a cybersecurity incident happening in their company, and they do not know or predict what is happening, which will lead, in time, to serious problems and much more expensive than if it had been resolved in time.

Analysing the answers received regarding the cybersecurity incidents, the authors determined that 4 of the 10 entrepreneurs had no cyber incidents in the last years on their companies. They also mentioned issues such as:

- "I don't know of any cybersecurity incidents from any of my employees."
- "I can say that I am lucky to be bypassed by these events and I think that I will not have them either because the activity that my company undertakes does not require much activity on the Internet."
- "Fortunately, we did not have any cybersecurity incidents, and we hope not to have any. We rely on the implementations and decisions taken by the responsible employee with cybersecurity for our company."
- "No, I hope we don't have such incidents."

It can be seen that only one of the 4 entrepreneurs rely on the implemented cybersecurity solutions and is sceptical about future events, and the others consider that such things cannot happen against their companies. The other study participants confirmed cybersecurity incidents but did not experience largescale incidents that would require monetary costs to resolve the issues. Those incidents were due to the negligence of employees who downloaded infected files that could be deleted by the antivirus, access to e-mails from anonymous sources, which led to the infection of computers or simply access to web pages which caused the hosts infected with Adware.

According to the answers of the 10 participants in this study, more than 50% of them had incidents, and two of them stated that as a result of the incidents, they had to reinstall the operating system, and thus lost some documents. The biggest problem for entrepreneurs is related to their employees who are not aware of the risks and damages they can cause through their actions.

The last question of the study refers to the constant information of entrepreneurs about the elements that can lead to cybersecurity risks within companies. To this question, 90% of entrepreneurs stated that they are not interested in informing about the elements that can cause risks to companies. They believe that their business is too small to have such problems or to be in the sights of attackers. Only one entrepreneur confirmed that he has a security employee who is constantly informed.

5. CONCLUSIONS

Cyberattacks are now an international concern and these raise many concerns for the entire economy, as security attacks could jeopardize the global economy. Organizations transmit sensitive data over networks and other devices in the course of their business, and cybersecurity protects that information and the systems used to process or store it.

Entrepreneurs who run SMEs are not aware of the real problem of lack of knowledge in the field of cybersecurity and do not apply solutions that can protect them from future attacks or reduce the damage caused by these attacks.

As it can be observed in the pilot research conducted, even if respondents' companies have been targeted in the past by incidents involving the introduction of viruses into computers, loss of documents or theft of information, entrepreneurs believe that employees who are not aware of the risks and the damage they can cause are the main culprits of these attacks.

Entrepreneurs are also not interested in this area because they consider that their company is too small to be the target of such attacks or the company's field of activity does not require a high level of use of devices such as smartphones, laptops, computers. These results are also supported by (Renaud & Weir, 2016) who highlighted in their work that small and medium enterprises do not use efficient security measures, underestimating the possible cyber threats. Furthermore, (Barlette et al., 2017) discussed in their paper that SMEs believe that they are too small to be vulnerable to cybercrimes, despite the fact that those cyber threats could be very dangerous to any firms, even for the small ones (Alahmari & Duncan, 2020).

The main limitation of this paper is that the sample is limited to 10 entrepreneurs invited to answer the set of questions. Thus, the results must be interpreted carefully as this study is a pilot one, as the time to gather and process information was limited, and the current conditions do not allow travel and reach more entrepreneurs.

Finally, we state that all the conclusions are drawn from the research, the identified limits, and the proposed future directions, may be an alarm signal for SME entrepreneurs who have not yet implemented solutions to reduce the risks caused by cyber-attacks.

REFERENCES

Alahmari, A., & Duncan, B. (2020). Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, (pg. 1-5). Dublin.

Asslani, A., Lari, A., & Lari, N. (2018). Strengthening information technology security through the failure modes and effects analysis approach. *International Journal of Quality Innovation*, 5-19.

Barlette, Y., Gundolf, K., & Jaouen, A. (2017). CEOs' information security behavior in SMEs: Does ownership matter? *Systèmes d'Information et Management*, (pg. 7-45).

Boys, J. (2018). The Clinton administration's development and implementation of cybersecurity strategy (1993–2001). *Intelligence and National Security*, 755-770.

CERT-RO. (2018). *Report on the evolution of cyber threats in 2017.* CERT-RO.

CISCOMAG. (2020). *67% of Small Businesses Aim to Increase Cybersecurity in 2020: Report.*

Cukier, M. (2007). *Hackers Attack Every 39 Seconds*. Preluat de pe https://www.livescience.com/4332-hackers-attack-39-seconds.html

Dekýš, P. (2010). Information security management in small and medium-sized companies. *Focus*, 12-13.

European Book of Accounts. (2019, March). *Challenges for an effective EU cybersecurity policy.* Preluat de pe eca.europa.eu

Hau, B., Penrose, M., Hall, T., & Bevilacqua, M. (2016). *Mandiant Consulting M-Trends 2016, EMEA Edition.*

Hiscox. (2018). *Small Business Cyber Risk Report.*

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering* , 3171-3189.

Jenkins, J., Grimes, M., Proudfoot, J., & Lowry, P. (2013). Improving Password Cybersecurity Through Inexpensive and Minimally Invasive Means: Detecting and Deterring Password Reuse Through Keystroke-Dynamics Monitoring and Just-in-Time Fear Appeals. *Information Technology for Development*, (pg. 196-213).

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, 269-282.

Khan, H., & AlShare, K. (2019). Violators versus non-violators of information security measures in organizations - A study of distinguishing factors. *Journal of Organizational Computing and Electronic Commerce*, 4-23.

Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: factors of success. *Entrepreneurship and Sustainability Issues*, 2081-2094.

Kovács, L. (2018). Cyber Security Policy and Strategy in the European Union and Nato. *Journal of Organizational Computing and Electronic Commerce*, 16-24.

Kure, H., Islam, S., & Razzaque, M. (2018). An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Sciences*, 898-927.

Lee, K., & Yim, K. (2020). Cybersecurity Threats Based on Machine Learning-Based Offensive Technique for Password Authentication. *Applied Sciences 10, 1286.* Asan.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees’ cybersecurity behavior. *International Journal of Information Management*, 13-24.

Millaire, P., Sathe, A., & Thielen, P. (2017). *What All Cyber Criminals Know: Small & Midsize Businesses With Little or No Cybersecurity Are Ideal Targets.* Preluat pe 11 28, 2020, de pe Chubb: https://www.chubb.com/us-en/_assets/doc/17010201-cyber-for-small_midsize-businesses-10.17.pdf

MXHOST. (2019). *Useful security practices for site owners*. Preluat de pe https://www.mxhost.ro/: https://www.mxhost.ro/practici-utile-de-securitate-pentru-proprietarii-de-site-uri-in-2019/

Renaud, K., & Weir, G. (2016). Cybersecurity and the Unbearability of Uncertainty. *Cybersecurity and Cyberforensics Conference (CCC)*, (pg. 137-143).

Smith, K., Jones, A., Johnson, L., & Smith, L. (2019). Examination of cybercrime and its effects on corporate stock value. *Journal of Information, Communication and Ethics in Society, 17*, 42-60.

Spella, D. (2019, Septembrie 05). *From IT security to cybersecurity - a paradigm shift for micro, small, and medium-sized enterprises that is still unaware?* Preluat de pe https://www.bursa.ro/de-la-securitatea-it-la-securitatea-cibernetica-o-schimbare-de-paradigma-inca-neconstientizata-de-catre-microintreprinderi-si-firmele-mici-si-mijlocii-49729737

Vevera, V. (2016, 06 16). *Cyberspace - the new fighting field.* Preluat pe 05 2020, de pe Romanian Journal of Informatics and Automation: https://rria.ici.ro/wp-content/uploads/2016/10/04-art-2.-Adrian-2.pdf

Závadský, Z., & Závadský, J. (2018). Quality managers and their future technological expectations related to Industry 4.0. *Total Quality Management & Business Excellence*, 1-25.