Advances in Economics, Business and Management Research, volume 156
2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020)

Strategic Measures in Improving Cybersecurity Management in Micro and Small Enterprises

Talu S.*

Technical University of Cluj-Napoca, Cluj-Napoca 400020, Romania
**Corresponding author. E-mail: stefan_ta@yahoo.com*

ABSTRACT
This paper analyzed the organizational factors, and risk management cybernetic practices, that affected the cybersecurity in European micro and small enterprises (MESEs). To achieve this goal, the study was based on an online questionnaire distributed using the Google Forms platform addressed to representatives of European MESEs. The results showed that there were internal organizational differences that affected cybersecurity management and their integrated management in the current activities of MESEs. On the other hand, it was found that MESEs applied risk assessment analyzes, and methods of dealing with these cybernetic risks.
Keywords: *computer system, security of information systems, information security, risk management practices*

1. INTRODUCTION

According to the World Bank, micro-enterprises are defined as enterprises with less than 10 employees and an annual turnover or a total annual balance sheet not exceeding EUR 2 million; small enterprises are defined as enterprises with less than 50 employees and whose annual turnover or annual balance sheet total does not exceed EUR 10 million. The thresholds for the turnover and the balance sheet total are adjusted regularly, to take account of changing economic circumstances in Europe (normally every four years).

In the last decades, micro and small enterprises (MESEs) played a major role in the business ecosystem, as they were the main source of job creation and were the driving force behind innovation and sustainability in the private sector [1, 2].

Compared to large companies, MESEs have a simple organization, with low bureaucratic practices and poorly formalized relationships, which allows a rapid process of operational decision-making, given the high capacity for flexibility and adaptation to market changes. Last but not least, small-scale units are more susceptible to change and very reactive and receptive to socio-economic conditions, such as the introduction of new products, new production methods, new materials, new markets, new forms of organization, etc.

On the other hand, MESEs have to deal with complex threats, such as high vulnerability to changes in the external environment, syncopes in the supply of global resources, barriers to accessing technological, financial, and human resources. These challenges highlight the fact that MESEs are constantly faced with various risks on various levels, and their survival is more difficult due to the limited resources they have access to: both financial and non-financial. Among the economic risks, fiscal crises in key economies and high structural unemployment or underemployment, together with the failure of rational regional or global governance, have been the biggest risks for MESEs.

William Ford Gibson invented in 1982 in a short story "Burning Crome", the phrase "cyberspace", and in 1984 the concept was popularized in his debut novel "Neuromancer". This term became known to the general public in the 1990s, with its appearance on the World Wide Web.

Cyberspace is correlated with different related terms, such as virtual reality, online environment, digital space, which, together, it is a conceptual apparatus developed in extension, depth, and nuances, which has generated a multitude of perspectives for analysis on the definitions and theories of cyberspace. In practical terms, it is found that cyberspace is a domain formed by the interaction of three different components: physical (hardware), virtual (software and data), and cognitive (people) [3-5].

In the last decades, in cyberspace, cybercrime has become a harsh reality, executing with great speed and breadth on the computer systems and networks of the MESEs [6-9].

Vulnerability in cyberspace is a weakness in the design and implementation of cyberinfrastructures or related security measures, of a human, technical or other nature procedural, which can be exploited and transformed by a cybernetic opponent.

The cyber threat is a potential threat to cybersecurity and is characterized by heightened dynamics, asymmetry, and diversity. In general, in the case of a classic cyber attack, the opponent aims to take control of the computer system, to obtain valuable information, or to partially or totally destroy the system by inactivating it.

Determining the source, location, and identity of an attacker is a difficult, complex task, as there are no clear reliable means to track the location of the message, and smart hackers hide in the maze architecture on the Internet or can simulate the true origin of an attack through a series of compromised computers or may leave "false flags" that innocently incriminate another entity.

In general, system administrators use Intrusion Detection Systems and Intrusion Prevention Systems, designed to prevent advanced intrusion attempts within systems, or the use of honeypots, in order to collect information about the attacker.

Cybersecurity represents the totality of measures taken to protect a computer or computer system from unauthorized access or attack. Measures taken for cybersecurity may include policies, security concepts, standards and guidelines, risk management, training and awareness activities, implementation of cyber infrastructure protection techniques, and consequence management [10-14].

Cybersecurity is essential for the prosperity of companies, as their activities increasingly depend on digital technologies. Various studies showed that cybercrime has increased rapidly in recent times having a high economic and psychological impact on MESEs [15-18].

In the current period, the cybersecurity incidents diversify both in terms of both the responsible entity and the purpose pursued, having the final in the blocking of the activity of companies. However, digital blackmail programs and cyber threats are generated by various cyber threats actors, being generally profit-driven, but can also be with political and strategic objectives. It is worth noting that the threat of crime is amplified by blurring the line between cybercrime and "traditional" crime, as criminals have adopted the Internet as a way to intensify their illegal activities and as a source to find new methods and tools to commit crimes. However, legally, the chances of identifying the offender have been found to be minimal in the vast majority of cases, and the probability of prosecuting him and recovering the damages is even lower. It should be emphasized that the ability to block cyber attacks by stepping up activities to detect, detect, and prosecute those responsible for attacks is not always successful [19, 20].

At the same time, illegal cyberspace actors achieve their goals through more refined, more discreet cyber tools, using cyberspace as a platform for obtaining confidential information about all companies' operational structures, either as a whole or as part of a large-scale hybrid approach. Thus, it is found that cyber operations that generally target critical infrastructures have developed on multiple levels and require an adequate response because the risk increases in proportion to the digital transformation. The risk of variously motivated attacks on targets and the inability to protect companies' cyber systems could have devastating consequences and could profoundly affect consumer confidence in emerging technologies.

Numerous studies have been recorded in the literature over the years, in which researchers have developed a general set of leadership practices that exemplary leaders apply to give cybersecurity the priority needed to strengthen resilience in both normal and normal times. and in times of crisis, emphasizing that these common practices bring a decisive advantage in the management of the organization.

Vulnerabilities of cyber users are represented both by the low awareness of the risks and threats of cyberspace and by the lack of knowledge or disinterest in daily activities when many employees are not fully aware of the pitfalls of social platforms, which are a preferred environment of those who carry out such activities [21].

The objectives of this study were: (1) to examine how MESEs are protected from cyberattacks; (2) the impact, and classification of risks of these cyber threats; (3) the identification of good practices in the field of cybersecurity to support MESEs in reducing the risk of a cyber attack and in actions to promote and raise awareness of the cybersecurity culture.

2. RESEARCH METHODOLOGY

In this study, about "Modern challenges in information security and protection of confidential information" a set of questions [22] was proposed:

1. Is information security a priority in your company?
   - Yes, at the IT department level.
   - Yes, at the management level.
   - Yes, both at the management level and at the IT department level.
   - Yes, at all levels.
   - No, it's not a priority.

2. Do you consider that, in general, in terms of information security and protection of information confidentiality, the greatest risk comes from the outside or from the inside?
   - The risks of external penetration are higher.
   - Risks of leakage (both involuntary and voluntary) of inside information are higher.
   - The two risks are or should be of equal importance.

3. Do you have an information security and privacy protection program in your company?
   - We do not have.
   - We are currently working on such a program.
   - We are interested in developing such a program in the next period.

4. If you have or are working on such a program of information security and confidentiality of company information, which of the following elements are or will be included in it?
   - Internal policies / procedures and good practices for data protection and for their management in optimal conditions

   Are already in place - Going to be - Not applicable
   - Periodic audits of own information security procedures and current / new risks

   Are already in place - Going to be - Not applicable
   - Periodic audits of information security procedures of suppliers

   Are already in place - Going to be - Not applicable
   - Uniform integration of information security procedures in all company operations

   Are already in place ▪ Going to be ▪ Not applicable
   - Procedures for detecting security incidents in a timely manner and for resolving them quickly and with minimal effect

Are already in place - Going to be - Not applicable

– Periodic updating of the information security and information confidentiality program

Are already in place - Going to be - Not applicable

5. Do you use the following technologies? Check next to the ones you use:

– Data encryption
– Securing password access
– Securing access in 2 steps (eg by password + confirmation from another device)
– Protecting information sent by email
– Securing wired / wireless networks
– Hardware device tracking
– Other? Please specify them here:

6. For the management of security solutions, do you use internal resources or external suppliers?

– Exclusive internal resources
– Exclusive external resources
– Both

7. Have you had any security issues that you have dealt with within in the last 5 years?

– No, no one.
– Yes, 1-3
– Yes, 4-10
– Yes, more than 10
– Yes, more than 50

8. But in the field of activity of your company, locally, have you heard that there have been security problems in the last 5 years?

– No, no one.
– Yes, 1-3
– Yes, 4-10
– Yes, more than 10
– Yes, more than 50

9. Which of the following problems did you have in the last 5 years?

– Unauthorized network access
– Viruses
– Leakage of confidential information by email
– Leakage of confidential information through social media
– Identity theft
– DOS attacks, broken sites
– Lack of management interest in security issues
– Security holes
– Cyber terrorism
– Physical attacks on equipment

10. How many security issues do you think you might face in your company in the last 5 years?

– No, none.
– Yes, 1-3
– Yes, 4-10
– Yes, more than 10
– Yes, more than 50

11. What about other companies in your company's field of activity, how many do you think each one will face?

– No, none.
– Yes, 1-3
– Yes, 4-10
– Yes, more than 10
– Yes, more than 50

12. What problems do you think you might face in the next 5 years?

– Unauthorized network access
– Viruses
– Leakage of confidential information by email
– Leakage of confidential information through social media
– Identity theft
– DOS attacks, broken sites
– Lack of management interest in security issues
– Security holes
– Cyber terrorism
– Physical attacks on equipment

13. You have within your company an allocated budget for information security

– Yes, as a dedicated budget
– Yes, included in the IT budget
– Yes, included in other budgets
– Not

14. Do you consider that the security budget you have is sufficient to create a competitive information security system?

– Yes
– Not

15. If the security budget is included in the IT budget, what is its proportion in this year? (Answer with a number between 0-100 which represents the percentage of the security budget from the IT budget)

– Percentage

16. What was and what do you think will be the evolution of your company's security budget?

– Previous year: Increased by ...% Decreased by ...%
– Current year: Increased by ...% Decreased by ...%
– Next year: Increased by ...% Decreased by ...%

17. What about the IT budget in general?

– Previous year: Increased by ...% Decreased by ...%
– Current year: Increased by ...% Decreased by ...%
– Next year: ▪ Increased by ...% ▪ Decreased by ...%

18. What type is your company?

– micro-enterprises
– small enterprises

19. What is the sector of activity of your company?

– Agriculture, forestry
– Extractive industry
– Industry

- Construction
- Trade
- Tourism, the hotel industry
- Transport
- Communications
- Finance and Banks
- Administration
- Education
- Health
- Services

20. What is the turnover of your company?
    - 100-500,000 euros
    - 501-1,000,000 euros
    - 1-5,000,000 euros
    - 5-10,000,000 euros
21. What are your age and gender?
    - 31-40 years - 41-50 years - 51-60 years - 61-70 years
    - male - female
22. Choose your business location and address.
    - Country
    - City
    - Address
    - Tel. and Fax
    - E-mail
23. Choose your years of experience in IT positions
    - below 1 year
    - 1 to 5 years
    - 6 to 10 years
    - over 10 years
24. If you have an opinion that you want to express on one of the topics opened in this questionnaire, or on the topic of information security in general, please include it in a section dedicated to it.

From September 1st - November 1st, 2020, the Information security questionnaire_Powernet [4], including 24 questions, was administered as an online questionnaire using the Google Forms platform, to 108 leaders and specialists of the management of cybersecurity in micro and small European enterprises (MESEs).

The chosen MESEs (108 companies) are operating in 108 different cities from 25 European countries: Finland (6), Germany (4), United Kingdom (5), France (4), Italy (4), Spain (5), Poland (3), Romania (8), Netherlands (3), Belgium (6), Czechia (6), Greece (4), Portugal (5), Sweden (4), Hungary (4), Austria (4), Moldova (6), Norway (5), Slovenia (4), Luxembourg (3), Liechtenstein (3), Lithuania (3), Switzerland (3), Bulgaria (3), and Denmark (3).

From a total of 68 micro-enterprises, 17 have been in operation for less than 5 years, 24 between 6 to 10 years, 14 between 11 to 15 years, 8 between 16 and 20 years, and 5 have been in business for more than 21 years.

From a total of 40 small enterprises, 11 have been in operation for less than 5 years, 9 between 6 to 10 years, 8 between 11 to 15 years, 7 between 16 and 20 years, and 5 have been in business for more than 21 years.

Participation in this study was voluntary; confidentiality was respected during the recruitment of the participants, during data collection, during transcription and data analysis, and during the dissemination of research results. The participants' identities and all the MESEs' names stayed anonymous and were preserved in a safe place and were not revealed. The participants (108 persons) were 72 men and 36 women, with higher education, who served a minimum of 2 years within the field and at least one year in their IT current position. The age of all participants varied between 41-58 years (average 47.1 years for men and 49.4 years for women). The results obtained from the application of the questionnaire were processed using SPSS 20 Statistical Package for the Social Sciences 20, using descriptive analysis, as well as parametric and non-parametric statistical tests.

3. DISCUSSION

The rapid pace of digital technological development, the increasing number, and the severity of cyber-attacks determine significant deficiencies in achieving cybersecurity for micro and small enterprises. Furthermore, the difficulties in the acquisition of cyber protection with the last version software create major difficulties for MESEs can operate safely. It was known that the cyberattacks can be carried out by several types of cybernetic opponents: criminal organizations, individual attackers, dissatisfied employees, and competitors.

It was found that the level of cyber protection of IT systems in studied MESEs varies and is closely associated with the industry that the company operates. The low level to the basic level of IT technical expertise was presented within the company in the non-technology intensive industry (Tourism, Hotel Industry, and Services).

Companies with a medium level of security were found in Agriculture and forestry. Companies that have operated in a high-level technology industry (Extractive Industry; Industry; Construction; Trade; Transport; Communications; Finance and Banks; Administration; Education; and Health) have all reported that they have a high or very high level of high IT technical expertise at the operational level to protect information assets within the company.

Out of the 108 interviewees, only 4 interviewees were either not aware of any specific cyber threat-related training or education program at all.

At 16 micro-enterprises and 35 small enterprises were created specific training programs in the field of cybersecurity with various modules that employees had to go through regularly. In the cybernetic training programs, 12 micro-enterprises and 31 small enterprises regularly conducted phishing cyberattacks on staff and periodic staff checks every 3-6 months.

98 participants demonstrated that they have a general level of understanding and awareness of cybersecurity threats within companies, such as viruses, hacking, phishing, and possible damage associated with their information.

Due to cybersecurity regarding phishing emails and such threats, 4 micro-enterprises have not been sufficiently

aware of these specific threats. In comparison, all small companies demonstrated a higher level of awareness and awareness of potential cybersecurity threats to the company such as "data breach" and "external hacking". We emphasize that all small companies had a large amount of information about their customers.

Following analysis, it was found that the major vulnerabilities in micro-enterprises and mini enterprises are: lack of knowledge of procedures and cybersecurity policies, improper applicability of correct information security standards, and their implementation.

The most important reasons for cyberattacks were: - rapid financial gains (6%); - informational blackmail (3%), theft (9%), manipulation (2%), or modification of information (10%); - obtaining competitive advantages (5%) and confidential information from competitors (15%); - sabotage of the institution concerned or exposure of data for revenge purposes (6%); - promoting social (10%) and/or political ideas (7%); - spreading panic and chaos, practicing terror (3%); - the answer to challenges (15%) and/or to arouse the admiration of famous hackers (9%).

Hackers applied various means of attack, such as:

- malware - the installation of malicious programs designed to disrupt the proper functioning of computer systems and networks (27%). From this one it was counted: viruses (3%), worms (1%), ransomware (malware that encrypts data on an infected computer) (5%), spyware (including trojan horses) (4%), keyloggers (malware that tracks keyboard activity, allowing to copy a user's passwords) (3%), rootkits (enabling administrative access to the victim's computer) (5%) and adware (unwanted and not ordered advertisement software) (6%);
- social engineering - a method of manipulation designed to obtain confidential information, such as passwords, personal data, and bank card information (18%);
- DDoS attacks - designed to block or delay access to an organization's services or systems (15%);
- botnets - the attack comes from a network or a large number of infected computers, used as spammers or viruses or to flood the network with malicious messages, leading to the blocking of the service (19%);
- Advanced Persistent Threats (APT) - sophisticated cyber attacks that use specific tools, advanced knowledge to detect and exploit technology-specific deficiencies (21%).

Surprisingly, all the MESEs use advanced password rules and there are no shared passwords amongst their employees but only the personal ones. It was found that 12% of employees use the work email address for personal accounts and 22% of employees use weak passwords for personal accounts.

4. CONCLUSION

In today's cyber global market, awareness of IT users about the vulnerabilities, risks, and threats of cyberspace and their possible impact has become essential, as cybersecurity is constantly evolving and requires ongoing training and education. MESEs have faced many challenges to assure increased levels of security in protecting the information they hold, because the information collected, stored, processed, and communicated by MESEs are sensitive and can have major economic negative consequences if their integrity, confidentiality, or availability would be compromised.

Cyber security in MESEs must be taken seriously and as a whole, and cooperation between management and IT staff must exist closely and permanently, when cybersecurity methods and measures are decided and created. This mutual cooperation between IT staff and MESEs management allows the alignment of cybersecurity with organizational business objectives that enhance the development of the company's business and has the effect of strengthening the sustainable competitive advantage in the market.

In this period it was found that the effects of the actual economic crisis and the precarious situation have faced by a large segment of the European population had the effect of involving IT specialists, in committing cybercrime, which had facilitated their rapid obtaining of financial gains and had favored the recruitment of an increasing number of IT specialists in criminal activities.

It was found that, generally, European MESEs promote a reliable, secure, and open cyber ecosystem to block evolving threats and take measures to withstand cyber attacks and deter them in the future, through operational structures and available capabilities. Also, it was found that the risk of large-scale cyber attacks and the massive incident of data fraud/theft is relatively higher for MESEs than other technological risks. At the same time, it was highlighted that it is necessary to design more effective training and awareness programs that ensure and support, in the long term, the appropriate behavior towards cybersecurity of employees.

It was recommended a shift from a reactive to proactive approach in cybersecurity, responding to both existing and future threats through stronger and more effective structures, with a much larger number of qualified experts, as well as the updating and development of methods for securing information and of the communication systems within European MESEs. Following the study, the following conclusions were drawn:

- the most important risks to cybersecurity were new technologies (Cloud Computing, Big Data, Internet of Things), the risk of the dissatisfied employee who has access to sensitive data and systems and outdated software products;
- cybersecurity owners must be held accountable for ensuring cybersecurity in order to increase their ability to respond to cyber incidents by imposing minimum cybersecurity requirements and ensuring the resilience of cyberinfrastructures;
- any organization must develop response procedures for the worst possible cyber scenarios;
- the cybersecurity culture of all employees must be enhanced by raising end-user awareness of online risks;

– - the sector most affected by security threats cybernetics is represented by the financial-banking sector, followed by sector energy and transport.

REFERENCES

[1] A. Hervé, C. Schmitt, R. Baldegger, Digitalization, entrepreneurial orientation and inter-nationalization of micro-, small- and medium-sized enterprises. Technology Innovation Management Review, 10(4) (2020) 5-17, DOI: 10.22215/timreview/ 1343.

[2] S.K Naradda Gamage, E. Ekanayake, G. Abeyrathne, R. Prasanna, J. Jayasundara, P. Rajapakshe, A review of global challenges and survival strategies of small and medium enterprises (SMEs). Economies. 8(4) (2020) 79.

[3] A. Asgary, A.I. Ozdemir, H. Ozyurek, Small and medium enterprises and global risks: evidence from manufacturing SMEs in Turkey, Int J Disaster Risk Sci., 2020. DOI: 10.1007/s13753-020-00247-0.

[4] M. Heidenreich, Implementation of an IT security measurement method for the evaluation of IT security in micro-enterprises, ICCECE, Southend, UK, 2020, pp. 92-97. DOI: 10.1109/iCCECE49321.2020.9231113.

[5] A. Dereń, D. Seretna-Sałamaj, J. Skonieczny, Z. Kondracka, Security of Enterprise Information Resources in Cyberspace, 2020. ISAT 2019. Advances in Intelligent Systems and Computing, vol 1052. Springer, Cham. DOI: 10.1007/978-3-030-30443-0_24.

[6] B. Nussbaum, C. Lewis, Sizing up people and process: a conceptual lens for thinking about cybersecurity in large and small enterprises, J. of Cyber Policy, 2(3) (2017) 389-404. DOI: 10.1080/23738871.2017.1398265.

[7] R. Ande, B. Adebisi, M. Hammoudeh, J. Saleem, Internet of Things: Evolution and technologies from a security perspective, Sustainable Cities and Society, 54 (2020) 101728. DOI: 10.1016/j.scs.2019.101728.

[8] Z. Polkowski, J. Dysarz, IT security management in small and medium enterprises, Scientific Bulletin – Economic Sciences, Special Issue EtaEc, 16 (2017)134-148.

[9] A.L. Prioteasa, N. Chicu, A.A. Ștefănescu (Marin), A.M. Bugheanu, R. Dinulescu, Risk management practices in small and medium enterprises: evidence from Romania, Management and Economics Review, 5(1) (2020) 1-15. DOI: 10.24818/mer/2020.06-01.

[10] Y. Miaoui, N. Boudriga, Enterprise security economics: A self - defense versus cyber - insurance dilemma. Applied Stochastic Models in Business and Industry, 35(3) (2019) 448-478.

[11] D. Woods, A. Simpson, Policy measures and cyber insurance: a framework, J. of Cyber Policy, 2(2) (2017) 209-226. DOI: 10.1080/23738871.2017.1360927.

[12] P. Timmers, The European Union's cybersecurity industrial policy, J. of Cyber Policy, 3(3) (2018) 363-384. DOI: 10.1080/23738871.2018.1562560.

[13] D. Wrede, T. Freers, J.M. Graf von der Schulenburg, Herausforderungen und Implikationen für das Cyber-Risikomanagement sowie die Versicherung von Cyberrisiken – Eine empirische Analyse. Zeitschrift für die gesamte Versicherungswissenschaft, 107(4) (2018) 405-434.

[14] A. Vinod K., A.W. Reddie, Comparative Industrial Policy and Cybersecurity: A Framework for Analysis, J. of Cyber Policy, 3(3) (2018) 291–305.

[15] K. Kikerpill, The individual's role in cybercrime prevention: internal spheres of protection and our ability to safeguard them, Kybernetes, 2020. DOI: 10.1108/K-06-2020-0335.

[16] F. Almeida, J. Pinheiro, V. Oliveira, Social network security risks and vulnerabilities in corporate environments. International Journal of Applied Management Sciences and Engineering, 6(1) (2019) 14-28.

[17] Ș. Țălu, Implications of modern digital technologies in higher education. Advances in Economics, Business and Management Research (AEBMR), 105 (2019) 554-557. DOI: 10.2991/iscde-19.2019.107.

[18] Ș. Țălu, New perspectives in the implementation of smart-technologies in higher education. Advances in Economics, Business and Management Research (AEBMR), 138 (2020) 253-257. DOI: 10.2991/aebmr.k.200502.042.

[19] S.S Rupra, A. Omamo, A cloud computing security assessment framework for small and medium enterprises, Journal of Information Security, 11(4) (2020). DOI: 10.4236/jis.2020.114014.

[20] A. Rabii, S. Assoul, K. Ouazzani Touhami, O. Roudies, Information and cyber security maturity models: a systematic literature review, Information and Computer Security, 28(4) (2020) 627-644. DOI: 10.1108/ICS-03-2019-0039.

[21] W. Nesren, T. Rana, K. Mumtaz, Measures for improving information security management in organisations: the impact of training and awareness programmes, UK Academy for Information Systems Conference Proc., 2012. http://aisel.aisnet.org/ukais2012/8.

[22] Chestionar securitate informationala_Powernet. https://www.surveymonkey.com/r/securitinfo2016/.