Information Security among SMEs in Hungary - An Overview

N. Mike*, E. Krén** and T. Kecskeméti**
* Corvinus University of Budapest / Librantis, Budapest, Hungary
** Librantis, Budapest, Hungary
all authors: firstname.lastname@librantis.hu

***Abstract* - Information and cyber security are important for SMEs. The level of security contributes greatly to the competitiveness of companies, but it is greatly underrepresented among SMEs in Hungary. The study aims to answer the question of whether accelerated digitization harms information security in Hungary. The analysis mainly focuses on companies actively involved in e-commerce during and after the Covid-19 era. Further, the trends in information security are compared within Hungary and the European Union, highlighting a local-specific deficit. The study presents the results of 2020, 2021, and 2022 quantitative research conducted by Digimeter company, as well as publicly available data from the European Union's DESI index (Digital Economy and Society Index) and NCSI (National Cybersecurity Index). The expected results of the research confirm that the lack of information security is visible in Hungary.**

Keywords* - *information security, data protection, data clustering.

I. INTRODUCTION

Readers may know the story of the three little pigs. There are several lessons to be learned from this story. The first is that consolidating an infrastructure is best done by trial and error. After being chased from the haystack and destroyed woodshed, the piglets finally reach the safe place: a brick house. The second lesson is that danger often takes the form of a similar threat. The aim of the wolf has always been to catch the piglets, only the manner has not changed. The third lesson is that strong infrastructure can be a strategic advantage. This means that improved security requires proactive planning.

In this study, the authors set out to investigate the information security (IS) level in small and medium-sized enterprises (SMEs) in Hungary. The need for the study is motivated by the increasing contribution of IS to competitiveness.

The authors argue that IS remains underrepresented in the SME sector. Even among European Union (EU) Member States, the level of IS in Hungary is considered immature, but there are already signs of its need. This study also aims to identify the sectors where SMEs have enhanced IS.

II. RESEARCH METHODOLOGY

The study attempts to answer the question of whether accelerated digitalization has a negative impact on the level of IS in the lives of SMEs in Hungary. The analysis focuses on companies actively involved in e-commerce and does not identify them individually. The research is based on a case study where manipulation of participants' behavior is neither the goal nor the option [1]. The desired effect is not intervention, but observation and reporting.

Among the available research frameworks, a pragmatic approach is chosen [2], which allows for effective focusing of the research question [3, 4] and its examination through multiple lenses [5,6].

The study begins with a review of the literature to provide the theoretical background and briefly introduces the indicators used in the study. Then the reader is led to the research findings and their evaluation.

To answer the proposed research question data provided by the Digimeter Index (DI) was used. DI is operating as a questionnaire-based empirical research tool to assess the digital presence of companies in Hungary.

The sample size varies from year to year: 777 responses submitted in 2020; 757 in 2021 and 674 in 2022. No different level of significance is observed: The most represented group consists of responses from SMEs with 5-9 employees, established or working in Pest county. The results are presented using cluster analysis [7]. The paper concludes with a description of the limitations of the research and a conclusion.

III. LITERATURE REVIEW

IS stands for the protection of information during its creation, processing, storage, and transmission. The disposal can be achieved through logical, technical, physical, and organizational measures that compensate for the potential loss of confidentiality, integrity, and availability [8].

IS should be managed globally according to the ISO /IEC 27001 standard [21]. Organizations are expected to comply with the standard, which covers security management, security of corporate assets, and IT security expectations.

Understanding of IS as a concept is context dependent as it carries some level of subjectivity [9]. The following two definitions summarize what the authors consider appropriate for IS:

"An activity or process, a capability or skill, a condition by which information and communication systems and the information they contain are protected from damage, unauthorized use, modification, or exploitation." [10].

"Cybersecurity is a collection of tools, policies, security concepts, safeguards, guidelines, risk management approaches, measures, training, best practices, and technologies that can be used to protect the cyber environment and the assets of the organization and the user." [11].

Companies, but especially SMEs, are forced to deal with IS. Their business operations depend on the use of information technologies and network systems which are essential to support their decision-making processes. This dependence can make them particularly vulnerable to threats from IS as they have limited human and technical resources and limited ability to address such vulnerabilities [12].

In 2012, there were almost 30,000 enterprises in Hungary, not counting sole proprietorships and micro-enterprises. Both international and Hungarian surveys show that companies do not pay enough attention to IS. The situation is particularly depressing for SMEs. The expectations placed on them are changing rapidly and dramatically, as is their business environment.

Although SME IS activities or lack thereof, pose less risk, they must be constantly monitored and renewed. There are many ways to IS. To raise awareness the European Union Agency for Cyber Security (ENISA) has produced a specific publication to help businesses develop IS [13]. There is a need to invest in IS systems that in turn protect against security incidents [14].

SMEs need an IS system that is affordable, easy to implement, easy to use, and prevents damage from security incidents. An unused IS system is like a lock on an unlocked door. A security system that does not prevent theft does not protect users or SMEs against security incidents [15]. Assessing the IS level of SMEs in Hungary the authors used the following indexes:

A. Digital Economy and Society Index (DESI)

DESI is a composite index measuring the progress of EU countries in the digital economy and society. The index is calculated by the European Commission (EC) and covers four key dimensions of the digital economy and society: (a) human capital, (b) connectivity, (c) digital technology integration, and (d) digital public services [16].

B. National Cybersecurity Index (NCSI)

NCSI is a measure of a country's overall cybersecurity posture that takes into account several factors, including the country's legal framework, technical infrastructure, and public awareness and understanding of cybersecurity issues. The index provides a comprehensive picture of a country's cybersecurity environment and efforts. It is used to assist in assessment and improvement.

C. Global Cybersecurity Index (GCI)

GCI is a composite index developed by the International Telecommunication Union (ITU) to measure the cybersecurity readiness of countries around the world. The GCI aims to provide a comprehensive overview of countries' cybersecurity capabilities and help identify areas for improvement. The GCI measures cybersecurity readiness through the following main pillars: (a) legal measures, (b) technical measures, (c) organizational measures, (d) capacity building, and (e) cooperation. These pillars are then broken down into sub-indicators that are used to assign a score to each country [17].

D. Digimeter Index (DI)

DI is a digital presence measurement tool developed by Smartcommerce Consulting, Reacty Digital, Virgo, and eNET to measure the digital readiness and capabilities of organizations in Hungary [19]. The tool provides a comprehensive assessment of an organization's digital maturity and covers several areas. The DI consists of six sub-indices: (a) digital presence, (b) digital daily life, (c) corporate governance, (d) sales and marketing, (e) digital finance, and (f) IT security [20]. The assessment is usually conducted online, and respondents are answering a series of questions about their digital capabilities in each of the areas covered above.

IV. RESEARCH RESULTS

Based on the data received from DI, the companies were divided into four different categories using cluster analysis. The differences between the groups in terms of IS can be seen in Figure 1. The distribution of scores for each group differs significantly. A simple interpretation is that the clusters formed as a group of companies all have different IS systems and strategies.

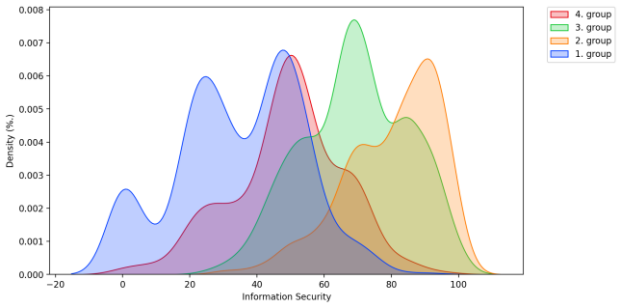

Figure 1. The density of cluster groups.

Staying with Figure 1, it is worth noting that the peaks of the distribution curves showing the mode of each category cluster around these values: (a) 45 points for 1. group; (b) 92 points for 2. group; (c) 67 points for 3. group; (d) 50 points for 4. group. The average scores were 34, 80, 69, and 49 points, respectively. This shows that each of the clusters formed has, on average, different IS systems or measures, if any, in the companies. An obvious question is if the overall score of the IS index separates the clusters in this way, how much variation is to be expected in the other aspects and characteristics?

It is also important to note that the most frequent scores, i.e. the mode of each group, are invariably 10-20 points lower than the mode of the next category. This shows that moving up to the next group is only possible at the price of

implementing significant additional security measures, even at the strategic level.

This is confirmed by the greater divergence of the 2. group from the other clusters. It should be noted, however, that the average IS score for this group is 80 points, which shows that, as with the other groups, it is not a completely homogeneous group, so there is still room for improvement even among the companies that score below average.

The assumption that companies with a lower level of digitalization care less about IS finds further support. Figure 2 describes the relationship between IS as a subset of DI and DI in isolation. SMEs with a lower index also either protect information to a lesser extent or have not yet focused on this aspect of their business. Taking into account the trends of recent years, one can even conclude that this level of preparedness is likely to move to a higher level shortly.

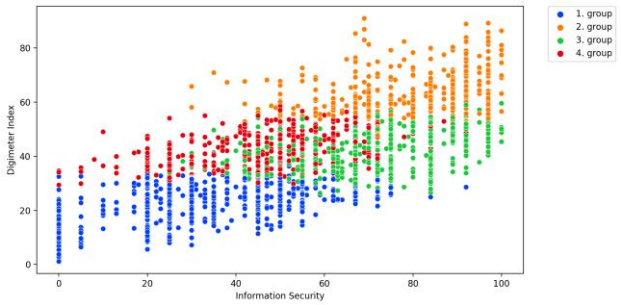

Figure 2. Clustered relationship between IS and DI.

Further analysis shows that one of the most meaningful links is between IS and sales and marketing, as shown in Figure 3. Companies that are leaders in digitalization are thus placed in this category not only because of their different digital presence but also because the IS level within these companies is higher. The sales and marketing activities confirm exactly this, as companies that frequently advertise and sell online must have up-to-date knowledge in the area of IS and data protection.

One of the main reasons for this is likely to be that compliance with legislation and the ever-changing demands of a digital presence requires constant adaptation. The need to adapt and stay up to date can only be achieved through a strong focus on this area. Without this, it would be exceedingly difficult for companies to continue their digital expansion.

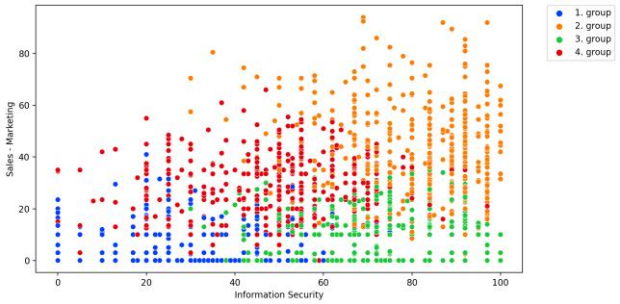

Figure 3. Clustered relationship between IS and Sales - Marketing.

Meanwhile, DESI has been measured every year in the European Union since 2014, so that changes in Hungary's situation can be tracked continuously. According to DESI, Hungary ranks 22nd out of 27 member states in 2022 [16].

Hungary's overall score of 43.8 shows that the country has developed in line with the EU average in recent years, but still lags significantly behind in the areas assessed in this study. The most disappointing result is in the integration of digital technologies. In this area, Hungary ranks 25th, with 14.5 points behind the EU average [16].

In terms of sub-scores, we see improvements in several areas, but the results show that there are still many Hungarian companies that do not sufficiently exploit the potential of digital technologies.

Resource planning systems that allow information to be exchanged electronically are used by 21% of companies [16]. 13% of companies have some form of social media presence, which shows that Hungary is well below the EU average in these areas [16]. The use of different systems and platforms does not mean that all companies use them properly and safely. The use of advanced technology would help protect the information, but Hungarian companies perform worst in this area. By advanced technology, the authors mean artificial intelligence, which is used by 3% of companies, Big Data, which is used by 7%, and cloud technology, which is the most widespread and is used by 21% of companies [16].

The DESI surveys SMEs in three areas: (a) online retailers (18%); (b) e-commerce sales (12%); (c) cross-border online sales (9%). There is a slight increase in all three areas. The results show that Hungarian SMEs are lagging in digitalization. One-third of the companies have a basic level of digital presence, which is extremely low compared to the EU average of 55%. In the coming years. It is crucial that SMEs move as close as possible to the EU, which is closely linked to the focus on data protection and IS.

According to the NCSI, Hungary ranks 35th in the world based on the last review, which took place on 13 October 2022, with a score of 65.53 out of a maximum of 100 [17]. The data before the 2022 measurements, taken from 2018 and 2019, clearly show a stagnant situation. This means

that Hungary's information and cyber security have neither increased nor decreased over the last four years.

The above-mentioned score of 65.53 is the result of four components, of which the ICT development index is the least acceptable. If the reader takes only this one indicator as a yardstick, Hungary slips back to 48th place [17]. This observation is consistent with the statements in the DESI.

Also in the ITU 2020 report, Hungary ranks 35th among the countries studied by researchers and 22nd among European countries [18]. ITU research produces a GCI that assesses the commitments of countries participating in the research, by answering to an 82-question questionnaire, divided to five pillars. Figure 4 illustrates Hungary's strengths and potential for improvement.

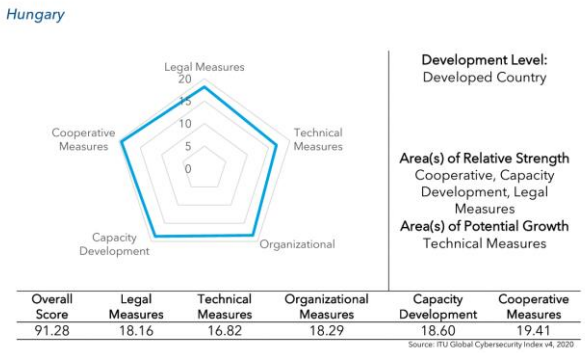

Figure 4. Global Cybersecurity Index (GCI) 2020. [4]

Overall, measures in four of the five pillars are considered sufficient, with room for further improvement in technical measures.

The areas of relative strength are due to successful national transposition of Directive no. 2016/1148 of the European Parliament and of the Council (the NIS Directive) [22], as well as Directive 2022/2555 of the European Parliament and of the Council (the NIS 2 Directive) [23]. Hungary had modified 40 of its national laws as a result of these legal instruments. The most national legislation is the Act CXII of 2011 on informational self-determination and freedom of information. This Hungarian law governs the protection of personal data and the right to access information of public interest. The Act CXII of 2011 is also affected by the applicability of GDPR [24]. This presents the *de lege lata* state concerning IS in Hungary.

The paper is not focused on providing *de lege ferenda* recommendations for changes or improvements to the existing legal framework. However, some potential and generally acceptable recommendations could include: (a) enhanced cybersecurity measures, that are proposing new laws or amendments to existing ones that focus on promoting stronger cybersecurity measures, including incident response planning, risk assessment, and the adoption of best practices across all sectors.

(b) explicit support for SMEs, as they lack the resources and expertise to adequately address IS issues, by inserting specific provisions for support programs, training, and resources specifically aimed at these organizations.

Of course, the question arises as to what would motivate businesses to spend on technical improvements if the performance on these is not outstanding at the national level. The answer lies in the global nature of cyber threats, as any business, regardless of its geographical location, can be the target of a cyber-attack.

V. LIMITATIONS

This section of the paper acknowledges several limitations of the study. Firstly, the use of data for only three years (2020-2022) provides a narrow overview of the situation, although these years were critical for digitization due to the pandemic.

Second, the number of respondents to the questionnaires varied each year, and this influenced the extent to which companies' attitudes towards IS have changed.

Third, there is a general lack of data on digitalization in Hungary, which made it challenging to conduct a qualitative survey. IS and cyber defense is underdeveloped and under-researched in Hungary, which limits the availability of information to companies and affects their perception of the seriousness of the issue.

VI. CONCLUSION

The analysis concludes that forced digitalization has harmed the level of IS in the life of SMEs in Hungary. The research shows that a critical mass of SMEs that have started digitization in the last two years have low levels of IS.

The results suggest that SMEs in Hungary are not able to cover a wide range of IS due to a lack of time, facilities, and expertise. The authors emphasize that all businesses are vulnerable to cyber-attacks and that SMES shouldn't excuse themselves by saying that they are small and not priority targets. Moreover, Hungary is lagging in this area, not only in e-commerce but also among SMEs as a whole.

The authors recommend repeating the survey, as the rapid development of IS can lead to major changes in one or two years.

REFERENCES

[1] Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study Design and Implementation for Novice Researchers. The Qualitative Report, 13(4): 544-559.

[2] Mertens, D.M. (2005). Research methods in education and psychology: integrating diversity with quantitative and qualitative approaches (2nd ed.) Thousand Oaks: Sage.

[3] Mackenzie, N., & Knipe, S. (2006). Research dilemmas: paradigms, methods and methodology Issues in Educational Research. 16. 193-205.

[4] Creswell, J.W. (2003). Research design: qualitative, quantitative, and mixed methods approaches (2nd ed.) Thousand Oaks: Sage.

[5] Edmondson, A. & McManus, S. (2007). methodological fit in management field research. Academy of management review. 32(4): 1155-1179.

[6] Mullarkey, M. T. and Hevner, A. R. (2018). An elaborated action design research process model. European journal of information systems. 28(1): 1-15.

[7] Simon, J. (2006). Applications of cluster analysis in marketing research. Statistical Review. 84(7): 627-649.

[8] Ključnikov, A. & Mura, L. & Sklenár, D. (2019). Information security management in SMEs: factors of success. Entrepreneurship and Sustainability Issues. 6(4): 2081-2094.

[9] Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, 4(10): 13-21.

[10] DHS. (2014). A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. 1 October.

[11] ITU (2009). Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). Link: https://rb.gy/xszzxm (accessed on 02.02.2023).

[12] Sadok, M., Alter, S. & Bednar, P. (2020). It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs, Information and Computer Security, 28(3): 467-483.

[13] Dr. Michelberger Pál & Lábodi Csaba (2012). Vállalati információbiztonság szervezése, Tanulmánykötet - Vállalkozásfejlesztés a XXI. században II. Óbuda University, Keleti Faculty of Business and Management.

[14] Simmonds, M. (2017). How businesses can navigate the rising tide of ransomware attacks. Computer Fraud St Security, 2017(3): 9-12.

[15] Bryan, L. L. (2020). Effective Information Security Strategies for Small Business. International Journal of Cyber Criminology, 14(1): 341-360.

[16] Digital Economy and Society Development Index, 2022 Hungary. Link: https://rb.gy/oq2ddk (accessed on 28.01.2023).

[17] National Cyber Security Index (2023). Link: https://rb.gy/vlp67s (accessed on 29.01.2023).

[18] Global Cybersecurity Index 2020. (2021). International Telecommunication Union. Link: https://rb.gy/f2wove (accessed on 29.01.2023).

[19] Bak, G., & Reicher, R. (2022). A vállalkozások és a digitális fejlődés, *in*: Baráth N.E. & Mezei J. (eds): Rendészet-Tudomány-Aktualitások 2022. Doktoranduszok Országos Szövetsége, Budapest, ISBN: 978-615-6457-06-6.

[20] Smartcommerce Consulting, Reacty Digital, Virgo & Enet. (2020). Digimeter. Link: https://digimeter.hu/ (accessed on 15.01.2023).

[21] ISO standards. Link: https://rb.gy/yxvakx (accessed on 03.02.2023).

[22] OJ L 194, 19.7.2016, pp. 1–30.

[23] OJ L 333, 27.12.2022, pp. 80–152.

[24] OJ L 119, 4.5.2016, pp. 1–88.