Security Awareness of HCI in DigitAll Reality

Veronika Szücs, Gábor Arányi and Ákos Dávid

University of Pannonia, Egyetem u. 10, H-8200 Veszprém, Hungary
szucs@mik.uni-pannon.hu, aranyi.gabor@mik.uni-pannon.hu,
david.akos@mik.uni-pannon.hu

Abstract: The rapid development of digital technologies in business operations, collectively referred to as DigitAll Reality, poses significant challenges to small and medium-sized enterprises (SMEs), in the area of IT security. This study examines the current level of IT security awareness and practice within SMEs, focusing on the role of decision makers, security solutions, employee behavior and regulatory compliance. In a comprehensive questionnaire, administered through face-to-face interviews with 46 IT managers and entrepreneurs, a number of factors were examined. Our analysis reveals a significant gap between decision-makers' IT knowledge and effective implementation of security measures. Specifically, the skills of decision makers do not show a strong correlation with the adoption of advanced security solutions or the protection of IT systems. In addition, the lack of structured IT policies and training, as well as the unregulated use of corporate resources, increases cyber threats. A clear trend has been observed, indicating that better IT education and security awareness of employees is associated with a reduced risk of ransomware attacks. This research highlights the urgent need for SMEs to improve their IT security practices, particularly through education and increased regulatory compliance. Secure systems that can respond to evolving digital threats are important. By overcoming these barriers, SMEs can better protect their operations against online threats.

Keywords: security awareness; HCI; IT security

1 Introduction

The future of interacting with digital information, digital reality refers to the way we will interact with digital information in the future. It suggests a seamless integration of digital information into our decision-making processes, possibly through the Internet of Things (IoT) and real-time data access, so from this point of view, in this paper we will refer to DigitAll Reality as a complete online, digital, interactive environment in which users apply machine and human cognition to all interactions. It includes all areas and activities, where the computer, the information system as software, is present and the user applies his/her own predictions, experiences and knowledge in the digital space according to his/her habits and conscious behavior. In the context of digitalization trends, users can be either

individuals or organizations and institutions in the interpretation. In this paper, we have examined the actors at the organizational level, and even more narrowly at the small and medium level of the economic sphere, as actors of the digital world, of DigitAll Reality, and we have examined their current situation, their behavior and their cognition as separate entities.

The scope of digitized activities varies, but typically more and more data and its handling are entering the digital space, which on the one hand carries information and represents value, and on the other hand requires continuous protection and increased attention. Globally, the protection of information systems is a major problem. There are specific legal frameworks for the protection of personal data, but it is questionable to what extent data subjects can comply with these regulations.

In the past 1-3 years, if readers have been following the news, they have read about the pandemic situation, but also about the increasing number of ransomware attacks. These attacks have unfortunately affected, almost indiscriminately, both small and large companies from all over the world.

In a recent article by the authors on these events, authors provide a detailed summary of the characteristics of the attacks and an overview of the most damaging cases. [1]

In this paper the main goal is to present an overview on the security awareness in small and medium enterprises (SMEs). The main focus points of this overview are the following:

- The role of the decision maker's IT degree in security questions
- The presented IT security solutions
- The role of employees
- The regulations related to the online tasks
- The relation between the regulations and the ransomware attacks

These questions were answered following an interview-based survey.

Section 1 describes the position of SMEs in their digital environment, the place of HCI, the range of internet-based services and the occurrence of potential cyber threats. Section 3 covers the basics of the methodology used to carry out the research, where the structure and key questions of the interviews and the method of evaluation are presented. Section 4 presents the results and Section 5 concludes the findings.

2 Background

The challenge for IT security professionals is to design and develop a system that can stand alone to reduce cyber security risks, secure the corporate infrastructure in a way that protects critical data and prevents unauthorized and malicious intrusions, at least during day-to-day online activities.

Csapó et al. [7] presented the characteristics of cognitive information systems, and Katona presented the specific aspects of VR-based HCI in [8], which places user processes in the world of cognitive information systems. What must not be forgotten is that technological advances naturally open up new possibilities for the human-machine relationship, and these will sooner or later lead us to rethink our existing rules, as Nogel et al. and Kruck et al. place it for the new, now digital reality space in [9].

This is a specific aspect of the digital reality introduced earlier by Baranyi et al. in [5] and [6] that carries a new approach, the role of cognitive information systems is amplified and it is expected that the solution will result in the development of an autonomous system that can follow the changed nature of the human-machine relationship in all aspects of the digital reality.

The emergence of the internet has fundamentally transformed communication, by overcoming geographical barriers and creating completely new possibilities for worldwide connectivity. The expansion of bandwidth has additionally bolstered this progress, facilitating more advanced modes of communication such as video conferencing.

An increasing number of online services and activities has resulted in a multitude of new communication tools, such as instant messaging applications, chatbots, meeting and social media platforms. Moreover, there is a growing trend of hosting activities on cloud-based platforms, which enables easier collaboration and remote access to information.

The advent of the internet has facilitated the proliferation of digital platforms, allowing for the growth of online commercial environments, including e-commerce, digital advertising, and remote employment prospects. Online education platforms have increased the flexibility of learning, while online banking and billing have simplified financial operations. The implementation of e-administration has completely transformed the way citizens and governments interact, while virtual private networks (VPNs) have ensured safe remote access for individuals working from home.

Both businesses and individuals increasingly utilize a combination of communication methods to meet their respective requirements. This combination of communication modalities typically encompasses email, instant messaging applications, and video conferencing.

Fundamentally, the internet has revolutionized communication by enabling us to connect, cooperate, and engage in business effortlessly across great distances, transcending geographical limitations.

Marketing, advertisements methodologies related to companies regular producing activity are changed dramatically in the last years. The volume of TV viewing and the usage of online streaming surge.

The growing number of video and live streaming applications has taken the advancement of social media to a new level. According to a survey by App Annie, there was a projected increase in spending of $1.2 billion in 2020, primarily due to the influence of these platforms. This phenomenon indicates a worldwide change in the allocation of people's time on social media, with video and live content assuming a prominent position [2].

This expansion is not solely due to increased popularity, but rather it is fundamentally altering the economy of social media. In 2021, it was estimated that live streaming platforms such as Twitch and Bigo Live will accumulate a staggering 548 billion hours of viewership. App Annie emphasizes the emergence of a new "creator economy" in social media, where users provide support to producers through "gifts" rather than conventional transactions.

This trend has been further expedited by the COVID-19 pandemic. Due to the growing amount of time people spend on the internet, the popularity of live streaming and video applications has significantly expanded. Twitch and similar platforms have experienced a significant increase in their user base, with the number of monthly active users almost tripling from January 2019 to 2021. This change is also evident in consumer expenditure. According to App Annie, YouTube and TikTok have overtaken major platforms such as Disney+ and Netflix in the categories of social, communication, and entertainment applications. The data indicates a distinct shift towards an economy that is more influenced by creators in the realm of social media.

The changing didn’t avoid the educational imperative. The pandemic period played a strong catalyzing role in the digitization process. The coronavirus outbreak sent shockwaves through education systems across Europe, demanding a radical shift towards innovative, creative, and inclusive teaching methods. This disruption has become a catalyst for dramatic change, with e-learning – distance learning and teaching on digital platforms – experiencing a meteoric rise.

However, the seeds of this transformation were already sown. Even before COVID-19, the global education technology (edtech) market was booming, with investments reaching $18.66 billion in 2019 and the online education market projected to hit a staggering $350 billion by 2025. From language learning apps and virtual tutoring platforms to video conferencing tools and online learning software, the adoption of edtech solutions had already been on a sharp incline [3].

The pandemic served as a powerful accelerant. While some concerns linger about the unplanned and rapid transition – highlighting issues like lack of training, insufficient bandwidth, and minimal preparation leading to a subpar user experience – there's also a sense of optimism. Many believe this crisis will pave the way for a new, hybrid model of education, one that leverages the strengths of both traditional in-person learning and the innovative potential of edtech, ultimately leading to a more robust and beneficial learning experience for all.

The events mentioned above have raised a number of security concerns.

In recent years, there has been a significant increase in the usage of video conferencing software. Nevertheless, the growing dependence on these platforms has exposed several security issues, which have prompted worries regarding the confidentiality and well-being of video conferencing.

An exemplary instance of security concerns in video conferencing is the Zoom affair. Zoom faced significant backlash in 2020 due to its deceptive claims on its ability to provide end-to-end encryption to users. The company first promoted its technology as offering genuine end-to-end encryption, ensuring that only the sender and recipient of a video conference could decipher its content. Subsequently, it was disclosed that Zoom's encryption did not truly provide end-to-end security, allowing Zoom servers to access and decipher video call data. [4]

The disclosure of this information, in addition to other security weaknesses identified in Zoom's system, such as the capability for unauthorized individuals to participate in meetings ("Zoombombing") and the potential for hackers to pilfer passwords, has generated significant apprehension regarding the company's dedication to safeguarding user privacy and security. The vulnerabilities in video conferencing applications such as Zoom have brought attention to the possibility of privacy breaches and the improper usage of these services. Video calls frequently involve sensitive material, such as private talks, confidential corporate negotiations, and even classified government secrets. If this data is inadequately safeguarded, it could be intercepted by unauthorized entities, resulting in privacy infringements, data breaches, and potential harm to one's reputation.

Furthermore, the convenient availability of video conferencing platforms has rendered them appealing to malevolent individuals aiming to capitalize on these weaknesses for diverse objectives. For example, hackers have the ability to utilize video conferencing as a means to disseminate malware, carry out phishing attacks, or even partake in cyber espionage.

The security issues related to video conferencing platforms require a renewed emphasis on building strong security measures and promoting appropriate usage habits. Platform providers should give utmost importance to being transparent about their encryption algorithms and proactively resolve any vulnerabilities that are uncovered. However, it is essential to provide users with proper education regarding potential security vulnerabilities and encourage them to follow best practices. These

practices include utilizing robust passwords, refraining from using public Wi-Fi networks for critical communications, recognizing spams and scams, while also exercising caution when providing meeting links.

Video conferencing tools are now essential in our networked environment. Nevertheless, the security issues linked to these platforms must not be disregarded. To tackle these concerns, it is imperative for platform providers, security specialists, and users to work together in order to guarantee the safety and security of video conferencing as a reliable mode of communication.

And finally, in quantitative terms, the number of digitalizing environments and the number of users involved support (Figure 1) the trends and developments described above.

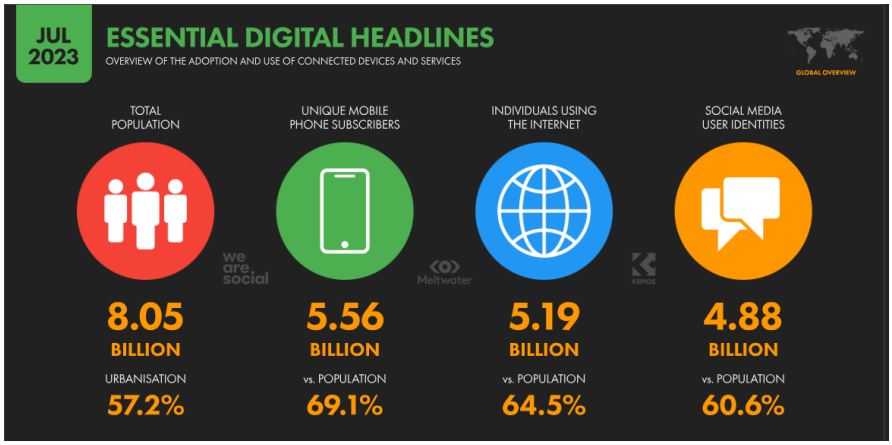

Figure 1
Source: https://datareportal.com/reports/digital-2023-global-overview-report

2.1 The Changes Seen from the Perspective of DigitAll Reality Mentioned in the Introduction Chapter

The extent of digitalization has inevitably led to a shift in the interests of the entities involved, as well as to a shift in the expectations of the different layers of actors with different interests. Expectations, due to the initial routines of activities carried out in the mainly still digitizing environment of previous years, have adapted differently to the large scale and rapidity of change.

The different roles and interests can be identified as follows.

Stakeholder actors are in the following roles: end-user, CEO, owner, regulators, IT security professionals, system administrators. Stakeholders have different goals, and the stakeholders' goals often do not match, they do not point in the same direction. As it can be seen in Table 1, regarding to the secure digital activity, the various stakeholders' goals and aims are different.

As a result of the different priorities in the table (Table 1) above, the interests of the stakeholders are constantly in conflict, but from a security point of view, a balance must be found that is acceptable to all participants.

In our questionnaire detailed in the next section, we are seeking to find out what level of security maturity the companies we interviewed represented, and what security practices they employ in response to contemporary threats. Our goal is to understand the nuances of IT security management in small and medium-sized enterprises (SMEs). SMEs often face unique challenges due to their size and limited resources.

We explore various aspects, such as the scale of business activities, IT infrastructure and the IT competence level of decision-makers. We also address aspects related to international business relationships, internal IT processes, employee training and concrete experiences with malware and ransomware attacks.

With this structured approach, we seek to gain key insights into how SMEs manage their IT security and what factors influence their vulnerability to cyber threats.

The survey uncovers the effectiveness of current practices and highlights areas that need improvement to improve overall security resilience.

Table 1
Different priorities for stakeholders

End-user goals	Easy-to-use system
	Less difficult authentication
	Easy-to-remember type passwords
Owner goals	Cheap acquisition
	Minimum resources
	Operation without an expert (if possible)
System administrator goals	Minimal changes in operation
	Automated processes
	Minimized time consumption
	New knowledge rarely needed
IT professional goals	End-users with basic knowledge
	End-users with security awareness
	System administrators with high level of knowledge
Goals of cyber criminals	Easy access into the closed systems (low hanging fruits)
	Weak passwords and weak AAA mechanisms
	“Lazy” system operators
	Minimal or missing security solutions

3 Material and Method

A complex questionnaire was designed, with relevant questions grouped around key issues. The questionnaire survey was conducted through face-to-face interviews in 2021-22. One of the criteria for selecting the interview subjects was the size of the enterprise. The survey focused specifically on small and medium-sized enterprises, because it can be generally stated that the majority of enterprises in Hungary and the European Union (almost 85%) currently belong to this category. This also means that the number of firms interviewed, although not significant, is proportionally representative of the sector.

When compiling the questionnaire, we tried to analyze and map the IT systems and security situation of the companies and at the same time to assess their previous experience with malware attacks.

3.1 The Structure of the Questionnaire

The questionnaire on which the interviews are based contains a total of 86 questions, some of which focus on the scope of the company's activities, the number of employees and the IT skills of the IT decision-makers. Another set of questions focused on international business relations. The next set of questions related to the structure of the IT infrastructure of the company, e.g., how many computers are used, whether there is an internal network, whether servers are operated, whether the company uses shared resources (file server, network printer, scanner, etc.). Further questions were asked about IT operations, internal training of staff, characteristics related to IT security awareness. At the end of the interviews, questions were asked about malware attacks and ransomware attacks suffered in the past, and related questions about IT system protection. During the survey, 46 IT managers, company directors or owners were invited to respond.

4 Results and Summary of the Interviews

Based on the results of the interviews, it can be concluded that there are specific characteristics among SMEs that make it difficult to operate and maintain secure systems from an IT security perspective.

The first questions we sought answers to during the research were the role of the IT skills of the decision maker in IT security issues and the suffered virus attacks (results can be seen in Figure 2).

Based on the interviews, we found that the IT skills of the decision maker on IT issues are not closely related to the security technologies and anti-malware solutions used (Figures 3-4).

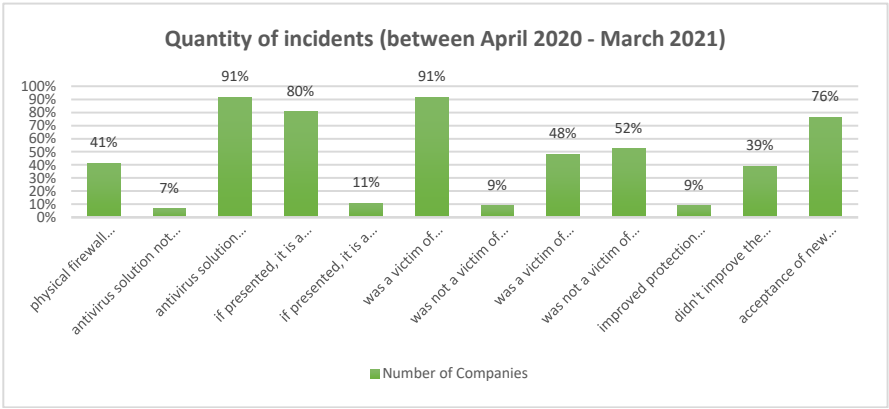

Figure 2
Quantity of incidents in proportion to the affected enterprises

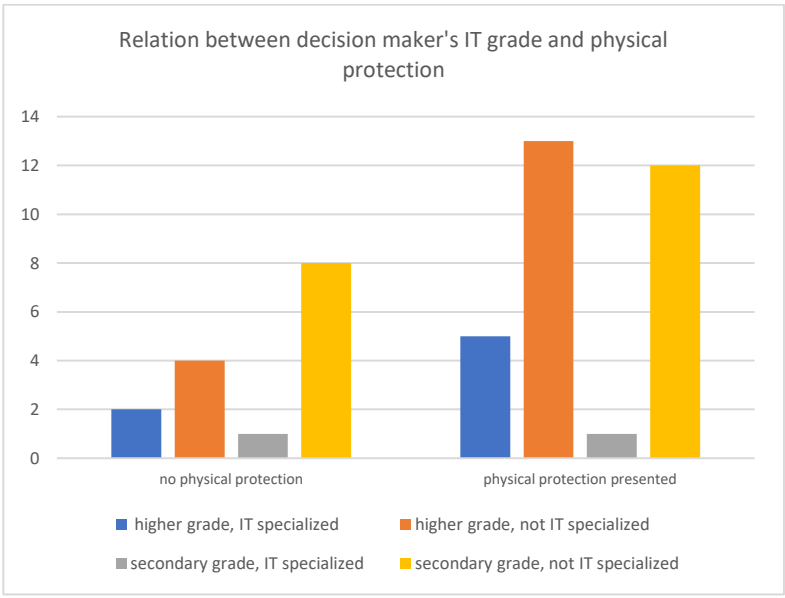

Figure 3
Relation between decision maker's IT grade and physical protection

None of the SMEs interviewed had a decision maker who was solely responsible for decision making on IT system issues. This role was invariably played by the owner of the enterprises surveyed, irrespective of whether he or she had IT qualifications (Figure 5).

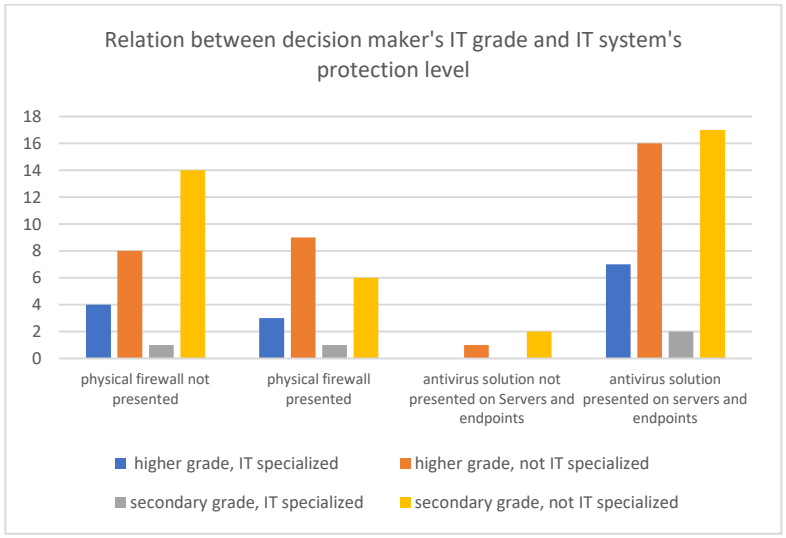

Figure 4
Relation between decision maker's IT grade and IT system's protection level

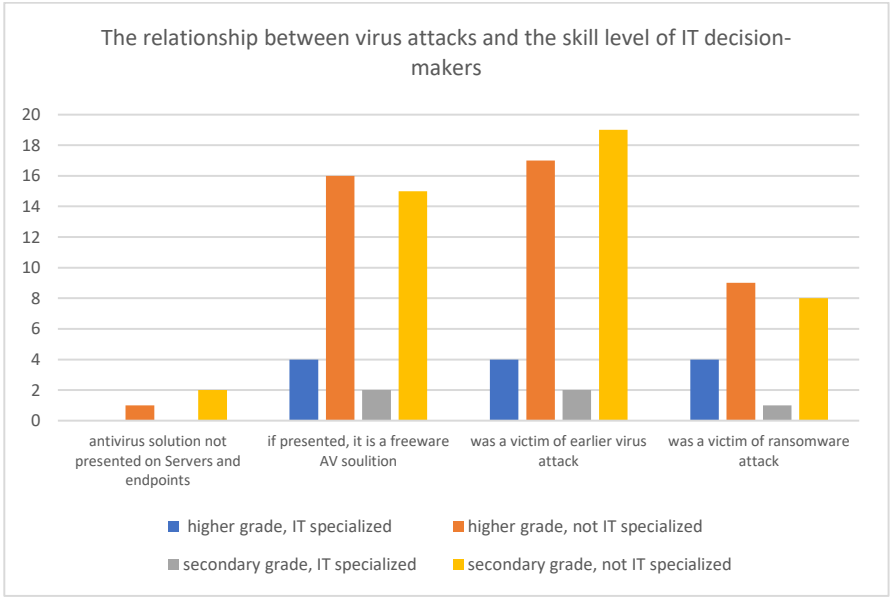

Figure 5
Relationship between decision maker's IT grade - IT systems' protection level and suffered virus attacks

The study also included an analysis of the IT security solutions available (also in Figure 5).

The interviews revealed that the education and IT skills of the decision-maker were not strongly correlated with whether the IT systems were protected by professional software, either free or commercially available. Nor is there a strong correlation with the level of physical protection – if any – that is built into the IT system.

An interesting result was the role of employees and the possibility to work online.

Of the 46 companies surveyed, 35 allowed employees to work from home office, and in these companies 10-50% of the employees work from home office. In all cases, they use their own computers to work from home (Table 2).

The situations we examined were as follows:

- Situation A: Home office enabled for employees
- Situation B: If home office is enabled, business email can be used for private tasks
- Situation C: In case home office is enabled, the company was a victim of ransomware attack
- Situation D: In case home office is enabled AND business email can be used for private task, the company was a victim of ransomware attack

Table 2
Work from Home scenarios

Situation A	Situation B	Situation C	Situation D
35	25	17	11
76.10%	71.42%	48.60%	68.75%

In 25 out of the 35 companies above, employees have their own company email address, and in 24 out of the 25 companies, employees can use their company email account for private purposes without any regulation.

For the SMEs surveyed, an average of 2-10 employees work on an online platform on a daily basis, e.g., invoicing, banking, compulsory data reporting, and performing business-specific tasks online in the digital space (Figure 6).

It is interesting to note that all the enterprises surveyed use online services, e.g., banking, money transfers, but there is no internal IT training or policy for using online platforms, and on the other hand the enterprise infrastructure does not have the security technologies that would be expected (Figure 7 and Table 3). There is no proxy server in the enterprises surveyed, and the guest network is not separated from the corporate wireless network, which poses a serious threat.

A high number of the surveyed enterprises have been victims of some form of malware attack, in some cases ransomware, between April 2020 and March 2021.

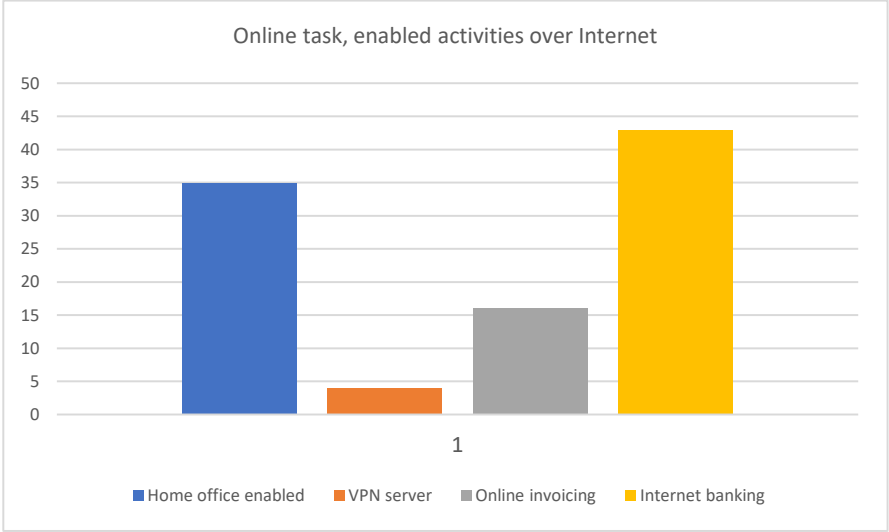

Figure 6
Volume of online tasks enabled in investigated companies

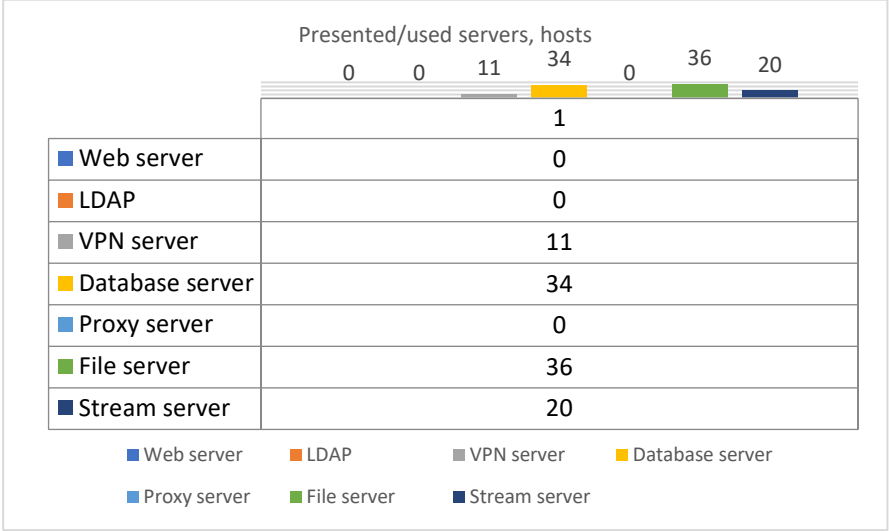

Figure 7
Presented/used servers, hosts

Table 3
Using of companies IT infrastructure and presented restrictions of it

Wi-Fi enabled	Guest Wi-Fi configured	NO Restriction to change antivirus settings or firewall setting by user	Employees know any signs of a possible attack
46	1	44	3

Based on the interviews, all but one of the 46 businesses surveyed have had a malware attack affecting their IT systems in the past, and 22 have suffered a ransomware attack.

The number of ransomware attacks suffered in the past reflects the level of security awareness among the company's employees and decision makers (Figure 5).

A clear trend emerges from the results of the questionnaire that the more knowledge (through IT education or security awareness training) a company's employees – especially the decision-makers – have, the less likely they are to fall victim to a possible future ransomware attack.

One important consideration for the IT industry in the coming decade will be how trustworthy they, and the systems they develop and/or use, are perceived to be. The ability to detect even the slightest changes to our systems will therefore become extremely valuable. The solution we proposed in [1] not only enables the early detection of ransomware-type attacks, but it can also use the same principles to effectively detect the increasingly serious threat of “framing” activities, which refer to the planting of false or compromising information on a victim's computer to falsely implicate the victim in illegal activities or to discredit them. This may include planting evidence, such as illicit files or documents, to misrepresent the victim's activities. This is followed by the 'smearing' of the company and/or individual, which has a horrendously damaging effect on the company's reputation. However, the model of the system we propose not only facilitates the detection of this phenomenon, but also provides evidence that the various compromising materials have been placed on the data store by external attackers, thus preventing or mitigating the cancel culture that is so fashionable today.

Conclusions

This research examines the impact of IT infrastructure governance and employee engagement in IT services on security outcomes in small and medium-sized enterprises (SMEs). The results of the survey, based on input from IT managers and business owners, provide important insights into prevailing IT security practices and vulnerabilities faced by these organizations.

A noteworthy finding, is the gap between the expertise of IT decision makers and the effective implementation of security strategies. Contrary to expectations, the technical proficiency of these managers does not necessarily equate to their

adoption of advanced security technologies or solutions to malware. This suggests that their technical knowledge may not be comprehensive in their understanding of current security technologies or their effective application.

In addition, the study found a lack of structured IT policies and training within SMEs. This lack, together with the unregulated use of corporate resources, increases the risk of cyber threats. The critical importance of thorough training and compliance is highlighted by the fact that SMEs that invest in IT education and promote security awareness among their employees tend to experience fewer ransomware incidents.

The results underline the urgent need for SMEs to improve their IT security practices by implementing comprehensive, tailored security solutions and developing a culture of continuous security awareness.

Future research should focus on identifying effective strategies to improve IT decision-makers' understanding of security technologies and developing scalable training programs. Such initiatives will help SMEs mitigate risks and strengthen their defenses against increasingly complex digital threats.

Acknowledgement

We acknowledge the financial support of Széchenyi 2020 under the EFOP-3.6.1-16-2016-00015.

Project TKP2020-IKA-07 has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the 2020-4.1.1-TKP2020 Thematic Excellence Programme 2020 - Institutional Excellence sub-program funding scheme.

References

[1] V. Szücs, G. Aranyi, and A. David, “Introduction of the ARDS - anti-ransomware defense system model - based on the systematic review of worldwide ransomware attacks”, Applied Sciences, Vol. 11, No. 13, 2021 [Online] Available: https://www.mdpi.com/2076-3417/11/13/6070

[2] Lexi Sydow: The Evolution of Social Media Apps: Live Streaming: The New Frontier for Social Media (App Annie report) https://www.appannie.com/en/insights/market-data/evolution-of-social-media-report/

[3] Ambika Selvaraj, Radhin Vishnu, Nithin KA, Noel Benson, Arun Jo Mathew: Effect of pandemic based online education on teaching and learning system, International Journal of Educational Development, Volume 85, September 2021, https://doi.org/10.1016/j.ijedudev.2021.102444

[4] Lesley Fair: Zooming in on Zoom’s unfair and deceptive security practices: More about the FTC settlement, 2020, https://www.ftc.gov/news-

events/blogs/business-blog/2020/11/zooming-zooms-unfair-deceptive-security-practices-more-about

[5] P. Baranyi, A. Csapó, T. Budai, and G. Wersényi, “Introducing theconcept of internet of digital reality – part I,”Acta Polytechnica, Vol. 18, No. 7, 2021

[6] G. Wersényi, A. Csapó, T. Budai, and P. Baranyi, “Internet of digital reality: Infrastructural background – part II,”Acta Polytechnica, Vol. 18, No. 8, 2021

[7] Csapó and G. Wersényi, “Overview of auditory representations in human machine interfaces,”ACM Computing Surveys (CSUR), Vol. 46, No. 2, 2013

[8] J. Katona, “A review of human–computer interaction and virtual reality research fields in cognitive infocommunications,”Applied Sciences, Vol. 11, No. 6, 2021

[9] M. Nogel, G. Kovács, and G. Wersényi, “Regulation of digital reality in nutshell,”12th IEEE International Conference on Cognitive Infocommunications, 2021

[10] Kruck, M. Weiss, The regulatory security state in Europe. Journal of European Public Policy, 30(7), 1205-1229, 2023