The Intersection of Personal ICT Use and Company Risk Exposure

Adam Bela Horvath

Obuda University, Keleti Károly Faculty of Business and Management, Budapest, Hungary, horvath.adam@kgk.uni-obuda.hu

Abstract: Profit-oriented and non-profit organizations face increasingly complex security challenges due to the growing use of shared devices for both professional and personal purposes. The line between the public and private domains is becoming progressively blurred, particularly in the digital realm: as users access a wider array of online services, they become more vulnerable to various forms of cybercrime, notably identity theft. Current research is exploring how the rising frequency of cybercrime impacts national security as a whole. To complement these studies, this paper aims to develop an integrated risk map for both profit-oriented and non-profit organizations. This map will be informed by data on information security incidents sourced from national and international publications. Furthermore, the paper will examine the role of information security management systems in mitigating these risks. The central research question, 'How can existing information security standards effectively address emerging threats?' will be addressed in this analysis.

Keywords: ISMS, cybersecurity

1 Introduction

This study explores the potential risks to corporate IT infrastructure when ICT resources owned and operated by employees are incorporated into an organization's daily operations. It presumes the existence of the two widely recognized categories of IT crimes, as defined in [1]:

Cyber-dependent crimes are criminal activities that can only be executed with the use of information and communication technologies (ICT), such as computers, networks, or other digital tools. These crimes are distinct from traditional criminal acts in that their commission is inherently tied to the technological environment. The motivations behind cyber-dependent crimes can be varied and multifaceted. In many cases, financial gain is a primary driving factor, as cybercriminals exploit digital platforms to generate illicit profits, whether through fraud, theft, or other illicit financial activities. Additionally, some criminals may aim to disrupt or damage the operation of computer systems or networks, causing widespread operational failures that can severely affect both individuals and organizations. Another significant motivation is the theft of personal data, which is often used for fraudulent activities, including identity theft and financial exploitation. The methods employed to carry out these crimes are diverse and increasingly sophisticated. One common approach is the deployment of viruses and other forms of malicious software, which can infiltrate systems and cause extensive harm, ranging from data loss to unauthorized access to sensitive information. In many cases, cybercriminals use malware to gain control over systems, often leaving the victims unaware of the breach until it is too late. Another prevalent technique is hacking, where attackers exploit vulnerabilities in computer systems or networks to gain unauthorized access to private data or disrupt normal operations. In addition, denial-of-service (DDoS) attacks are a widespread method of cybercriminals, wherein internet servers are overloaded with massive amounts of traffic, effectively rendering websites or entire networks inaccessible. This type of attack is particularly disruptive for businesses and organizations that rely on their online presence for daily operations, as it can lead to significant downtime and financial losses. Cyber-dependent crimes are intrinsically linked to the digital world, and as technology advances, the frequency and complexity of these crimes continue to increase. The rise of digital platforms, combined with the growing interconnection of networks, has created new opportunities for cybercriminals to exploit vulnerabilities in cyberspace. As these crimes become more sophisticated, they pose ever-greater challenges to cybersecurity professionals and organizations seeking to protect their digital assets and sensitive information. The evolving nature of these threats requires continuous adaptation of security measures and strategies to mitigate risks and respond to new and emerging cyber threats effectively [1-3].

Cyber-enabled crimes refer to criminal activities that use information and communication technology (ICT) to facilitate or enhance traditional criminal acts. These crimes, which include online fraud, harassment, and intimidation, are distinct from cyber-dependent crimes in that they can still be committed without the use of ICT. However, the application of digital tools and technologies significantly increases the scale and reach of these crimes. The primary motivation behind cyber-enabled crimes often revolves around financial gain, with cybercriminals exploiting the digital environment to carry out fraudulent activities. Typical examples of these crimes include phishing, where fraudsters send deceptive emails pretending to be from legitimate sources to steal sensitive information, large-scale fraud schemes, theft, and sexual offenses against children. In the context of profit-oriented environments, economic crimes such as fraud are particularly prevalent. These types of crimes, made more efficient through the use of ICT, often have a significant financial impact on individuals, companies, and organizations. **Cyber-enabled data theft** is a prominent issue in this regard, as cybercriminals seek to steal personal, financial, or corporate information to commit fraud. The data targeted by cybercriminals is highly valuable and can include personal information such as names, bank details, and National Insurance numbers, as well as corporate data like company accounts, client databases, and intellectual property such as new products or innovations. The theft of such data can lead to significant financial losses and reputational damage for both individuals and organizations. **Cyber-enabled crimes** are, in essence, hybrid crimes, arising from the integration of traditional criminal behavior and networked technologies. According to Wall (2007), these crimes have become increasingly prominent as a result of the rapid growth of networked technologies, which provide criminals with new opportunities to commit offenses on a larger scale and across broader geographical areas. The ability to access individuals in remote locations and the anonymity provided by the internet have significantly expanded the potential for such crimes. While these crimes could still be carried out in the absence of networked technologies, the opportunities for large-scale attacks, as well as the ease of reaching potential victims, would be greatly reduced (Levi et al., 2015). Examples of cyber-enabled crimes include phishing, identity theft, large-scale fraud, and the distribution of illegal content, such as online pornography. These crimes illustrate the growing intersection of traditional criminal behaviors and the evolving capabilities of digital technology, making them increasingly difficult to prevent and prosecute. [2-4]

Even within the context of traditional employment, where work is performed at the workplace during standard working hours, organizations must consider two primary types of potential risks, partly driven by limited rationality. The first involves the employee's own fault, such as the deliberate commission of an illegal act (e.g., internal fraud), while the second pertains to situations where the employee becomes a victim of external manipulation, such as social engineering. In what was previously referred to as "classic" employment, employees represent one of the most vulnerable points in the organizational security framework. In this context, employees utilize assets that belong to the organization—specifically, information and communication technologies (ICT) embedded in the organization's infrastructure. These assets are legally authorized and are typically under the control of designated personnel.

Today, this issue has become a central topic in discussions surrounding information security and human resources management. A pressing concern is the fact that IT-related attacks often serve as the precursor to further vulnerabilities within an organization’s systems [5]. Focusing disproportionately on social engineering attacks tends to divert attention, thereby underestimating other associated risks.

Recent studies indicate that young professionals entering the workforce today—partly as a result of changes brought about by the global COVID-19 pandemic—possess significantly more advanced user knowledge compared to previous generations. Their use of ICT tools has become substantially more pervasive, further amplifying the challenges faced by organizations [6]. (This process was already identifiable and demonstrable well before the outbreak of the pandemic, but these trends have been significantly amplified and made irreversible by the global health challenge [7-8].) This situation can be mitigated by equipping the ICT infrastructure with a monitoring system capable of overseeing processes and transactions, enabling proactive defense mechanisms. However, organizations also face heightened risks from adopting Bring Your Own Device (BYOD) policies, where personal devices owned by employees are used for business purposes. This practice limits the organization’s previously legitimate control rights over its assets, both legally (due to the lack of ownership) and practically (since full access rights rest primarily with the users) [9]. Consequently, the risk exposure to the organization is significantly increased.

2 Problem statement: ISMS , BYOD, teleworking

Currently, ISMS (based on ISO 27001 or other standards) follow the widely recognized PDCA model- This iterative process begins with the "P" phase, where the ISMS is designed within the context of company policy, ensuring alignment with other organizational policies and identifying the necessary objects, processes, and procedures for continuous risk management. In the "D" phase, the operational aspect of the information security framework is implemented, which had been previously designed and integrated into the organization (e.g., creating regulations). The "C" phase involves evaluating the performance of the process, considering ISMS guidelines, objectives, and practical experience, followed by reporting activities. The results from this evaluation inform the final "A" phase, during which corrective actions are implemented to enhance the system [10].

Risk assessment is a key component of corporate security, as IT security is an integral part of operational risk management. This implies that both intentional harm and force majeure, along with human errors and technical/engineering failures, must be addressed. A homogeneous approach to risk management must be established to handle these diverse risks efficiently [10-11].

In the context of BYOD (Bring Your Own Device) tools, these are devices, typically smart tools, that are owned by the employee. These devices can be integrated into the company's information system in various ways. For example, they can be synchronized with company directories and calendars via an IMAP server, or files can be linked with widely used services such as Dropbox. Additionally, several enterprise management systems offer interfaces that are optimized for use with these smart devices [12].

High-latency incidents often correlate with information security breaches. A study by Crowd Research Partners (2016) surveyed 800 respondents and provided the following alarming results:

- 39% of respondents confirmed that malware had been downloaded at some point. However, 35% were uncertain about whether such an event had occurred.
- 24% confirmed that their BYOD device had been connected to an untrusted Wi-Fi network at some point, while 48% were uncertain.
- 21% acknowledged their BYOD device's involvement in a previous incident, with 37% unsure whether such an event had taken place.

My qualitative research focuses on how businesses can respond to global challenges and adapt to emerging trends in the digital age [11]. Specifically, it examines how companies are equipped to address the unique challenges posed by Bring Your Own Device (BYOD) policies. The research explores the strategies businesses can implement to effectively mitigate the security risks associated with BYOD while maintaining operational efficiency.

3 Qualitative analysis

After examining the Bring Your Own Device (BYOD) phenomenon and the advantages it brings, it is crucial to identify why these tools are often considered vulnerable. The risks associated with BYOD devices can be categorized into several types [14]: One of the primary concerns is physical risks, such as the device being stolen or the owner losing it. Another significant issue arises when a mobile device becomes damaged, rendering it unusable. Unauthorized access is also a critical concern, especially when a device is left unattended and accessed by a third party. Moreover, there are risks related to data logging through the mobile device, which could allow malicious actors to gain control over it via a data connection. In these cases, there are several potential outcomes:

- Data loss can occur if important information is deleted.
- Data loss can also occur while giving the attacker access to stored data.
- Data modification may happen either directly on the device or, in cases where a client is installed, on the company server, which might record unintended changes.

The installation and distribution of malicious programs within the company's infrastructure is another key risk, as is the potential for unauthorized SMS and MMS messages to be sent, contradicting the owner’s intentions. Additionally, applications installed from trusted sources may still contain bugs that put security at risk.

In some cases, users may install applications that inadvertently cause harm, either directly or indirectly. Finally, misuse by attackers can occur both logically and physically, by using the mobile phone to exploit services that the user is automatically logged into, often bypassing the need for further authentication.

In the earlier sections of this study, I analyzed how the integration of external elements, such as ICT devices and remote workers, increases the vulnerability of corporate infrastructures compared to previous setups. Due to the lack of primary data, I draw conclusions based on quantitative analysis. Specifically, I evaluate the ISO 27001 standards in the context of BYOD devices and teleworking, while also considering additional factors that can enhance corporate security.

However, these ISMS systems have a fundamental weakness: the integration of IT infrastructures into the corporate environment, which significantly impacts corporate security. It remains questionable whether the scope of corporate standards applies effectively or whether compliance can even be enforced. Since these IT tools are not owned by the company, the ability to control them is inherently limited. Information security standards often implicitly assume that a company's tangible and intangible assets are fully under its control, but this assumption does not hold when external elements are involved [10].

Moreover, the traditional ISMS framework is increasingly inadequate because enforcing information security rules becomes substantially more difficult when those involved are not in close geographical proximity. In such cases, other cultural mechanisms may be required to maintain security standards [16-17]. highlights that the tools and institutions linked to the "visible" aspects of security tend to adopt a retrospective approach, while the development of values and attitudes is continuously evolving as part of the broader progression of information security practices.

If the illusion of security in collaboration with teleworkers can be dispelled, it becomes possible to raise security awareness through effective education and training programs (such as e-learning). Focusing on the real risks, such as “identity theft,” serves as a powerful motivational tool. The risks discussed in this study are not only a threat to specific organizations but can also lead to substantial personal damage. A security-conscious attitude enables individuals to not only defend against known threats but also to develop skills for handling unexpected and unusual incidents, potentially raising awareness of malicious intent and better equipping individuals to address unforeseen situations effectively [15, 17].

Conclusions

This study focuses on the challenges organizations face when the logical components of their information infrastructure (such as BYOD tools) and both physical and logical tools are situated outside the company’s control. These were considered "simpler cases," yet even in these relatively straightforward instances, each study revealed disturbing data.

Considering current employment trends, there is a theoretical need to develop a risk assessment model that identifies vulnerabilities and potential risk events that pose threats to organizations, but for which defenses are either not feasible or only partially effective.

Furthermore, it remains unexplored to what extent an organization might be at risk if an employee, whether a regular or teleworking staff member, were responsible for a complex IT crime such as identity theft. A survey is necessary to evaluate how widely these incidents affect organizations, examining how known cases reflect the severity of the impact on the respective employer. Additionally, individual attack profiles could be identified by analyzing case studies on specific incidents.

Acknowledgement

PROJECT NO. EKÖP-24-KDP-2 HAS BEEN IMPLEMENTED WITH THE SUPPORT PROVIDED BY THE MINISTRY OF CULTURE AND INNOVATION OF HUNGARY FROM THE NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION FUND, FINANCED UNDER THE 2024-2.1.2 UNIVERSITY RESEARCH SCHOLARSHIP PROGRAM - COOPERATIVE DOCTORAL PROGRAM FUNDING SCHEME.

References

[1] M. McGuire and S. Dowling, "Cyber crime: A review of the evidence," Research Report 75, Chapter 2: Cyber-enabled crimes, Home Office, 2013. [Online]. Available: https://assets.publishing.service.gov.uk/media/5a755a94e5274a59fa7177f7/horr75-chap2.pdf. [Accessed: 19-Jul-2025].

[2] S. Furnell, D. Emm, and M. Papadaki, "The challenge of measuring cyber-dependent crimes," Computer Fraud & Security, vol. 2015, no. 10, pp. 5–12, 2015. DOI: 10.1016/S1361-3723(15)30093-2.

[3] M. Weulen Kranenbarg, "Cyber-Dependent Crime Versus Traditional Crime: Empirical Evidence for Clusters of Offenses and Related Motives," in Cybercrime in Context, M. Weulen Kranenbarg and R. Leukfeldt, Eds. Cham: Springer, 2021, vol. 1, pp. 123-145. DOI: 10.1007/978-3-030-60527-8_12. [Accessed: 19-Jul-2025].

[4] C. S. A. P. Joshi and S. R. S. Sharma, "Exploring the human factor in cyber-enabled and cyber-dependent crimes," Internet Research, vol. 30, no. 6, pp. 1665-1675, Dec. 2015. DOI: 10.1108/INTR-10-2019-0400

[5] K. D. Mitnick and W. L. Simon, The Art of Deception: Controlling the Human Element of Security. New York: Wiley, 2002.

[6] P. Szikora, K. Lazányi, and A. Vincze, "The digital skills in the Hungarian higher education during the first wave of Covid-19," in Higher Education Policies for Developing Digital Skills to Respond to the Covid-19 Crisis: European and Global Perspectives, T. Nina, D. Ravšelj, and A. Aristovnik, Eds. Brussels, Belgium: European Liberal Forum, 2021, pp. 4–18, ISBN 978-2-39067-005-6.

[7] B. Ali and P. Szikora, "Az Y generáció és az internet kapcsolata," in Vállalkozásfejlesztés a XXI. században: VII. tanulmánykötet, Á. Csiszárik-Kocsir, Ed. Budapest, Hungary: Óbudai Egyetem, Keleti Károly Gazdasági Kar, 2017, pp. 11–23.

[8] B. Ali and P. Szikora, "Információbiztonság az Y generáció körében," in Vállalkozásfejlesztés a XXI. században: VII. tanulmánykötet, Á. Csiszárik-Kocsir, Ed. Budapest, Hungary: Óbudai Egyetem, Keleti Károly Gazdasági Kar, 2017, pp. 24–40.

[9] P. Szikora, "The Role of the Tools and Methods of Implementation in Information System Efficiency," in Teaching and Learning: 2nd International Conference for Theory and Practice in Education: 29 May 2009, Budapest: Programme, Abstracts, J. T. Karlovitz, Ed. Budapest, Hungary: Association of Educational Sciences, 2009, p. 50.

[10] T. Harich, IT-Sicherheitsmanagement. 4. Aufl. Bonn, Deutschland: mitp-Verlag, 2025, ISBN 9783747509920.

[11] P. Szikora, "Döntések szerepe a vállalkozások fejlesztésében," in Vállalkozásfejlesztés a XXI. században: tanulmánykötet, I. Z. Nagy, Ed. Budapest, Hungary: Óbudai Egyetem, Keleti Károly Gazdasági Kar, 2011, pp. 171–180.

[12] J. Keyes, Bring Your Own Devices (BYOD) Survival Guide, 1st ed. Boca Raton, FL, USA: Auerbach Publications, 2013.

[13] Crowd Research Partners, BYOD & Mobile Security Spotlight Report, 2016.

[14] G. S. Kearns, "Countering mobile device threats: A mobile device security model," Journal of Forensic & Investigative Accounting, vol. 8, no. 1, pp. 36–48, 2016. [Online]. Available: https://digitalcommons.usf.edu/fac_publications/809/. [Accessed: 23-Jul-2025].

[15] B. D. G. Bak and A. Kelemen-Erdős, "Stressz, opportunizmus és bizalom a szervezeti információs és kommunikációs technológiabiztonság tükrében," Információs Társadalom: Társadalomtudományi Folyóirat, vol. 23, no. 3, pp. 9–26, 2023.

[16] J. Répás, L. Berek, G. B. Bak, N. Oláh, and P. Ujhegyi, "Kisvállalkozások Nagy Kihívásai: Útmutató az Információbiztonsághoz," in XL. Kandó Konferencia Kiadvány, T. Wührl, Ed. Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2025, pp. 179–186.

[17] R. Kuusisto, K. Nyberg, and T. Virtanen, "Unite Security Culture: May a unified security culture be plausible?" Proceedings of the 3rd European Conference on Information Warfare and Security, 2004.