A shield and a compass between two worlds – where financial rationality meets the threats of cyberspace

Éva Pintér[1]

DOI: https://doi.org/10.35551/PFQ_2026_1_7

Elemér Terták and Levente Kovács: Cybersecurity – Cyberspace

Over the past few years, I have attended dozens of conferences, workshops and closed-door professional meetings where, in conversations with banking and corporate executives, I have heard the same phrase time and again: *"Cybersecurity is no longer an IT issue, but a strategic risk at the executive level."* Whether it was the deputy CEO responsible for a major bank's digital transformation, the CIO of a medium-sized enterprise, or the head of risk management at a company operating financial infrastructure, the same sense of tension and realisation was palpable everywhere.

As a bank's security director put it after a panel discussion last autumn: *"The question today is no longer whether our shield is strong, but whether we'll notice in time if someone gets past it."* That sentence has stayed with me ever since, because it perfectly sums up the shift in mindset that the financial and corporate sectors are undergoing day by day. Cyberspace threats are no longer technically distant, abstract phenomena. They are present at the very heart of senior management decisions and have become one of the most important factors in financial stability. So the question today is no longer whether we will be attacked in cyberspace, but when we will notice it.

These experiences came to mind when I picked up Elemér Terták and Levente Kovács's book *Cybersecurity – Cyberspace*. The book describes precisely the world that provides the backdrop to these meetings: a reality in which banks, businesses, service providers, and regulators are all players in the same, invisible yet more complex than ever, risk landscape.

1 Éva Pintér, PhD (Habil.), Corvinus University of Budapest, Institute of Entrepreneurship and Innovation, Associate Professor
eva.pinter@uni-corvinus.hu https://orcid.org/0000-0003-0149-8421

The picture of the situation outlined by the authors and practical experience coincide on many points. The case studies heard at conferences, the fears and dilemmas of managers, and the tactical and strategic debates all resurface from the pages of the book — only in a more systematic, thoughtful and professionally coherent framework. This is why reading this volume has become, for me, not merely a professional experience but also a kind of interpretative anchor: it helps me understand the cybersecurity ecosystem within which every financial actor operates in Hungary and across Europe today.

In this book review, I shall attempt to explore this world: how the authors' framework of thought is structured, how the volume's chapters fit together, and how all this resonates with international cybersecurity practices and the realities of the domestic banking sector.

In the shadow of the ever-growing cyber threat, financial sector players face new challenges. According to the book's authors, the rise of digital financial services has simultaneously triggered a cybersecurity 'war': a 2024 ENISA study found that cyber incidents accounted for 46% of cases involving European financial institutions. This highlights the fact that today, anyone can suffer losses not only in the stock market but also through computer networks.

The aim of this volume is precisely to provide financial professionals and decision-makers with a well-founded framework of interrelationships. The authors, well-known figures in the Hungarian banking sector and financial education, present a wide-ranging analysis of the challenges posed by cyberspace and the possibilities for defence within the country. In our book review, we outline the volume's main chapters, evaluate its glossary, and examine the topics discussed in an international context.

Cybersecurity – Cyberspace is divided into nine main chapters that build on one another rather than treating the topics in isolation. The first four chapters are fact-finding in nature: they begin with the history and global trends of cybercrime, then examine international cooperation, legal statistics, and, finally, the financial damage caused by cyber incidents.

The introduction presents the technological revolution brought about by the processing of Big Data, artificial intelligence (AI), machine learning (ML), data mining and predictive analytics, from the innocent participant in the digital ecosystem to the professional cybercriminal. These technologies simultaneously open up new markets and create business opportunities, yet they also exponentially increase the vulnerability of IT systems. For the financial sector, this means that the automation of customer service, the digitisation of payment methods and transcontinental data flows are constantly exposed to external attacks. The introduction also highlights the paradox that has characterised the last decade: whilst financial institutions' security investments are growing by 15–20% annually, the number and effectiveness of successful attacks are escalating even faster. This is not due to shortcomings in the financial sector, but rather to the increasing sophistication of attackers

and the interdependence of supply chains. The introduction is therefore not alarmist but rather a realistic assessment that leads into the chapters.

The first chapter on the history of cybercrime is extremely interesting and informative. The authors begin by examining the first known case – a telecommunications network fraud committed at the French Société Générale in 1834. This shows that cybercrime is not a new phenomenon; its forms have changed over time and with technology. As we follow the chapter's chronological progression, we learn about historically significant events such as the Creeper virus (1971), the Morris Worm (1988) and the ILOVEYOU virus (2000), which once shook the entire computer-controlled world. This is followed by takeovers, data leaks, the expansion of phishing, the first major bank hacking incidents, and, finally, the sophisticated attacks of the 21st century: Stuxnet (2010), NotPetya (2017), WannaCry (2017), Petya (2017), and CrowdStrike (2024). International regulatory and technological responses are also inevitable, including the US NIST framework, the EU's GDPR (2018), the ISO/IEC 27001 and 27005 standards (2005–2022), and the recommendations of the FSB and the OECD. The chapter highlights that stronger regulations have emerged in response to every threat, but the problem of incompatibility – differing legal systems, geopolitical conflicts and the transnational nature of cybercrime – remains unresolved.

Concerning Hungary, the chapter covers the history of domestic bank hacking over the past 10–15 years, the 2012 breach at the University of Szeged, attacks against government systems, and the major incidents affecting members of the Hungarian Banking Association over the past 2–3 years (customer fraud, breaches of internal networks). This chapter serves as an extremely useful 'case study collection', which fosters organisational memory and the embedding of lessons learnt within an organisation.

The second chapter interprets cybercrime as a complex ecosystem. It systematises the frameworks for global cooperation in the fight against cybercrime. It focuses in particular on the Budapest Convention on Cybercrime, its global scope, and cooperation with various international organisations (the EU, the UN, NATO, etc.). The authors present international frameworks and innovations in the collection of electronic evidence and detail the rationale for introducing comparative statistical terminology (ICCS, i.e., International Classification of Cybercrime Statistics). In this context, they note that the Council of Europe's programme office, which brings together more than 90 countries worldwide, also supports the fight against cybercrime. At the end of the chapter, a comprehensive table outlines the EU's current cybersecurity legislation and institutional framework (ENISA Regulation, NIS/NIS2 Directive, European Cyber Crisis Network, etc.), noting that financial institutions must also comply with these regulations.

Chapter Three provides an overview of international 'indicators' of cybercrime. It covers global cybercrime rankings, including the countries and continents most affected, based on UN data. It details the situation in the United States, the EU and the successor states of the former Soviet Union. American statistics are highlighted

– it emerges that the corporate sector has become a significant target. Although the level of protection is higher there, complaints and reports indicate that significant damage is still being incurred. Finally, the authors present the situation in Hungary: they map Hungary's cybersecurity indicators against those of other countries. It is interesting to note that, according to the NKI (National Cyber Security Institute), the cyber maturity of companies in Hungary is currently low, particularly among SMEs, where cybersecurity awareness is lower.

In the fourth chapter, the authors analyse the financial implications of cyber incidents. They calculate the direct and indirect costs of incidents, including stock market reactions and reputational damage. They also discuss system-level risks arising from the supply chain and the costs of delayed reporting. In conclusion, they put forward important recommendations, such as regulatory incentives for transparent damage assessment and rapid reporting. To this end, they also cite examples from abroad (for example, detailing the cyber insurance costs of industrial players) drawn from the international literature.

The second half of the work is dominated by a solution-oriented approach, with the authors focusing on presenting technological possibilities, new guidelines and methods.

Chapter Five reviews new technologies and methods applicable to corporate cyber defence. The examination of the role of technological innovation is one of the book's most complex and analytical sections, exploring how digital innovation is changing the functioning of cybersecurity, its risks, defence options, and decision-making. It highlights the dual nature of technological innovation: on the one hand, digitalisation and new solutions such as artificial intelligence, big data analytics and cloud-based services enable massive efficiency gains; on the other hand, however, they also create new vulnerabilities and risks within the corporate environment. The chapter approaches the subject from the perspectives of the financial sector and corporate practice, but its findings clearly align with international cybersecurity trends (CISA, ENISA, WEF) and provide a detailed overview of the factors shaping the risk landscape for modern enterprises. It discusses the impact of the NIS2 Directive on the financial sector as a separate section, comparing it with the situation in the Hungarian banking sector as described. For example, NIS2, adopted in 2024, prescribes stricter risk management and executive accountability. This chapter goes into detail on risk measurement methods, their limitations, and the difficulties of interpretation (e.g., the pitfalls of manipulating quantitative indicators). An important element is drawing lessons from cyberattacks; the necessity of a conscious security strategy is outlined, with an emphasis on defence systems. The authors provide a detailed overview of modern defence technologies, primarily UEBA and SIEM systems based on behavioural analysis and machine learning, capable of recognising patterns, generating risk scores, and identifying suspicious behaviour. The chapter also discusses the phenomenon of lateral movement, one of the most critical elements of cyberattacks, as it enables attackers to spread across multiple systems within

a network. It specifically addresses the role of cyber insurance, emphasising that whilst it is a useful supplement, it cannot replace adequate technical and organisational defences, and does not provide cover for certain risks – such as insider attacks. One of the chapter's key messages is that technological innovation is not only a technical issue but also a human and organisational one; therefore, the human factor plays at least as significant a role in defence as advanced tools.

Chapter Six presents a systematic, taxonomic approach to cyber threats, which is essential for identifying attacks and developing effective defences. The authors emphasise that the rapidly increasing scale of cybercrime – particularly in financial fraud – poses a significant economic and reputational risk, which justifies precise categorisation. The chapter outlines various types of attacks, including client-side, server-side and targeted attacks involving human intervention, as well as threats affecting supply chains and critical systems. The authors devote particular attention to insider threats and their typical scenarios, which often remain hidden yet can have serious consequences. Overall, the chapter emphasises that, in a rapidly changing and increasingly complex threat environment, well-founded prevention and response strategies can only be developed with the aid of a clear, multidimensional framework.

Chapter seven examines social manipulation, a dangerous and rapidly spreading form of cybercrime that exploits people's carelessness, gullibility, and emotional reactions rather than technical attacks. The authors emphasise that a significant proportion of cyber incidents can be attributed not to technical shortcomings but to human error, underscoring the importance of conscious user behaviour as a key line of defence. In the field of cyberpsychology, it outlines social engineering techniques – from phishing and 'whaling' to 'know-it-all' persuasion – and then makes recommendations for defence, such as regular risk-awareness training, testing and the involvement of 'ethical hackers'. The authors also address customer service practices: they describe how bank staff should support victims empathetically yet professionally and how trust can be restored. The main message of the chapter is that protection against social engineering is based on raising awareness, effective communication, and the widespread training of customers and company staff.

Chapter 8 summarises the practical principles and methods of cybersecurity defence, primarily from the perspective of everyday users. The authors emphasise that a significant proportion of attacks stem from simple carelessness, gullibility or inattention; therefore, the most important defence is conscious, prudent digital behaviour. The chapter provides detailed advice on managing passwords, using online accounts securely, recognising phishing messages and dealing with suspicious requests, with a particular focus on how users can reduce the risk of unauthorised access to their personal data.

The authors emphasise that modern technical solutions – such as two-factor authentication or regular software updates – are only effective when accompanied by appropriate user discipline and awareness. Finally, the chapter

stresses that security is not a one-off state but a continuous process requiring constant vigilance and regular risk assessment. In addition to fostering a security culture, it is necessary to develop incident response plans that outline steps to improve security practices.

The volume concludes with a 36-page glossary containing detailed definitions of the most important cybersecurity and IT terms. This lexical appendix deserves special attention. The authors emphasise that, due to the accelerating pace of terminological change, the continuous definition of key terms is essential. The glossary in the book's concluding chapter effectively summarises the essence of the entire work: it explains every important concept in an accessible manner, thereby helping novice readers catch up and standardising professional conceptual knowledge. As the authors write, this glossary forms the foundation of *the digital immune system*. The lexical appendix is particularly useful for financial professionals who have not previously encountered detailed technical texts on cybersecurity: it serves as a brief guide should one get stuck on an unfamiliar term, whilst also providing a reference for developing a common technical vocabulary. Overall, the glossary is one of the most practical elements of the volume, enhancing the handbook's suitability for both educational and up-to-date reference purposes.

The book's outstanding relevance stems from the fact that in Hungary, as in other EU countries, cybersecurity regulation and awareness have intensified in recent years. The Hungarian National Cybersecurity Strategy, for example, states that achieving a secure cyberspace is a 'shared responsibility' for all stakeholders. Cybersecurity – Cyberspace, therefore, comes at just the right time for Hungarian readers. The volume is not intended solely for IT specialists, but is also useful reading for decision-makers, lawyers, and risk managers at banks and financial institutions. It demonstrates how global cyber regulation relates to domestic practices and highlights that harmonising the internal rules of Hungarian financial institutions with international recommendations is an urgent task. At the same time, the book offers original academic insights: it includes up-to-date analysis of domestic statistical and legal data not found in other Hungarian publications, and the authors summarise numerous international sources that are difficult to access in Hungarian (European statistics, UN/Europol data). The publication is comprehensive, bridging the gap between the Hungarian financial and information technology sectors. Whilst numerous domestic handbooks address individual sub-areas (such as cyber risk management, the legal environment, or information security), this volume also comprehensively covers the financial dimension. Compared to the existing Hungarian literature, it fills a gap, is written from the perspective of banking executives and reflects on financial interrelationships – thus offering new insights in the Hungarian context as well. It is an urgent question not only in the business world but also in the legislative, regulatory, and educational spheres: how can the ever-evolving, increasingly sophisticated cyber threats be identified and addressed effectively? Significant legislative changes in the European and Hungarian

financial sectors in recent years (NIS2, DORA, MNB guidelines), as well as the drastic rise in the number of incidents, have both necessitated the creation of such a comprehensive handbook. It is worth noting that, for example, in 2024, a CrowdStrike vulnerability caused more than 8 million systems worldwide to crash – a stark reminder of the importance of proactive, professionally grounded cybersecurity management, even in critical infrastructure.

The book makes it abundantly clear that Hungary's level of financial digitalisation is above the European average, yet attack surfaces have grown disproportionately. It is uniquely useful to demonstrate, through examples such as the KiberPajzs programme alongside banking security systems, as well as the Financial Navigator and KiberPajzs educational projects, how the public's financial awareness can be strengthened against cybercrime. Certain chapters of the book can be used directly by professional teams involved in training, compliance, digital transformation, or even the development of consumer protection strategies. ■