Marko Stanojević*
https://orcid.org/0009-0007-7241-5503

UDC: 005.21:334.72.021
005.334:334.72
658.11:004.056.5
DOI: 10.5937/MegRev2501231S
Original scientific paper
Received 14.06.2025.
Approved: 17.08.2025.

THE ROLE OF INFORMATION TECHNOLOGIES IN MODERN CORPORATE SECURITY

Abstract: *Today's business environment is moving at lightning speed, and with digital transformation at the forefront, corporate security has changed from just an operational responsibility to a significant strategic element. This review paper explores the ways in which information technologies are transforming the current landscape of corporate security models. It highlights the importance of integrating automated systems, digital tools for spotting and preventing risks, and effective incident management strategies. A multidisciplinary approach is emphasized, covering physical, technical, human, and organizational aspects of protection. The paper discusses the contemporary challenges in cyber security, focusing on the increasing intricacy of cyber-attacks, the push for tougher regulatory standards, and the ethical and legal issues that emerge in a globalized digital landscape. By examining real-world cases, it brings to light the necessity of adopting a proactive mindset when developing security strategies that can stand up to the constantly evolving and intricate digital threats. Ultimately, it concludes that information security must be regularly updated, intricately linked to the broader corporate strategy, and based on realistic risk assessments to ensure the organization's long-term stability, reputation, and competitiveness.*

Keywords: *Corporate security, Information technologies, Cyber threats, Digital transformation*

* Stanojevic.marko799@gmail.com

1. INTRODUCTION

In a business landscape that's increasingly influenced by digital transformation, corporate security has transitioned from a secondary issue to a core strategic priority. At its core, corporate security is all about the teamwork involved in protecting an organization's assets, be they physical, intellectual, informational, or human, from potential threats that can come from both inside and outside. Keeping operations running smoothly, safeguarding the organization's image, and building resilience against various risks is absolutely vital. Scholars have described corporate security in many ways, often pointing out the necessity of ensuring the physical safety of property, employees, and data. They also highlight how crucial it is to spot, minimize, and handle any threats that could impact the organization's overall stability and longevity.[1] Other definitions focus on the governance aspect of corporate security. Essentially, it involves implementing governance practices to make sure that policies, protocols, and procedures are well-defined and executed, all in the name of protecting the company's interests.[2]

These days, our perspective on corporate security has shifted quite a bit. It's no longer just about protecting physical assets or keeping information safe. Now, it's all about weaving together these elements with safety protocols, crisis management, business continuity plans, regulatory compliance, insider threat management, and risk management, among other things. This means corporate security is quite complex, involving preventive, detective, and responsive measures that operate across physical, technical, human, and organizational dimensions.

The growing importance of information technologies is a crucial component of the corporate security environment of today. The digital transformation of security processes, like surveillance, access control, and incident logging, along with automated systems for identifying, evaluating, and addressing threats, has created new opportunities for detecting risks earlier, responding more swiftly, and using security resources more effectively. Studies suggest that implementing IT strategies and security investments, including technical network control systems (like intrusion detection and antivirus) and identity and access management systems, can effectively reduce specific types of security breaches in organizations. That being said, the effectiveness of these initiatives really depends on how well-developed the organization's digital infrastructure is from the start.[3]

---

1 Shapiro, L. & Maras, M-H. (2021): *Encyclopedia of Security and Emergency Management*, Springer Nature. ISBN: 978-3-319-70487-6

2 Cassidy, K. (2019): "Corporate Security (Structure, Roles, Duties)", in: Shapiro, L., Maras, MH. (eds), *Encyclopedia of Security and Emergency Management*, Springer, Cham. DOI: 10.1007/978-3-319-69891-5_19-1

3 Li, H., Yoo, S. & Kettinger, W. J. (2021): "The Roles of IT Strategies and Security Investments in Reducing Organizational Security Breaches", *Journal of Management Information Systems*,

Businesses are allowed to conduct their operations thanks to corporate security. It adapts to shifts in the company's risk appetite, alerts executives to the probable consequences of risks, and makes sure that riskier operations can be undertaken with the highest level of security by combining several levels of protection.[4] This review paper examines in detail the impact of information technology on modern corporate security. It underscores how automation and digitization have transformed our methods for identifying and responding to potential risks. The paper discusses the tools and frameworks currently in use and addresses the ongoing challenges we face, whether they are organizational, ethical, or technical. Every one of these points circles back to the key aim of protecting the company's assets.

Communication in a virtual environment and the contents of social networks are becoming key elements of legal informatics, as organizations increasingly depend on the Internet and digital channels, which opens up risks of reputational and legal consequences if their content and public perception are inadequately managed.[5] Corporate information security procedures are now heavily regulated. These rules set minimum requirements for particular sectors and are intended to safeguard the confidence that stakeholders and consumers have in businesses involved in such sectors. However, meeting these standards shouldn't take the place of information security procedures that are founded on actual risk management requirements, nor should it ever be the organization's main goal.[6]

Cybersecurity Ventures estimates that by 2025, cybercrime-related damages might total $10.5 trillion worldwide. The largest amount ever recorded was $4.9 million, which was the average cost of a single data breach in 2024. These figures demonstrate that cyber dangers can affect even the biggest companies.[7]

2. ANALYSIS OF RECENT RESEARCH

Today, the topic of corporate security is very pertinent and of significant interest to scientists worldwide.[8] Corporations of all sizes and sorts are vulnerable to criminality

38(1), 222–245.

4 Security executive council (2025): *What Is Corporate Security?,* https://securityexecutivecouncil.com/insight/corporate-security-career/what-is-corporate-security-2097.

5 Baltezarevic, I. & Baltezarević, R. (2020): „Uticaj komunikacije u virtuelnom okruženju na pravnu informatiku", *Megatrend Revija, 17*(4), 27-40. DOI: 10.5937/MegRev2004027B

6 Andress, J. & Leary, M. (2017): *Building a practical information security program*, Syngress.

7 Datami Newsroom (2025): *Top 10 Cyberattacks That Brought Global Corporations to a Halt*, https://datami.ee/blog/top-10-major-cyberattacks-on-corporations-analysis-by-datami/.

8 Ludbey, C. R., Brooks, D. J., & Coole, M. P. (2018): "Corporate security: identifying and understanding the levels of security work in an organisation", *Asian Journal of Criminology*, *13*, 109–128. DOI: 10.1007/s11417-017-9261-x

these days. Because of the many benefits that come with investing in corporate security, it is imperative. Theft, assault, and property damage are among the workplace crimes that corporate security helps to prevent. Given the rise in these crimes, it also aids in protecting people, including clients and staff. Additionally, industrial security management contributes to the preservation of an organization's image.[9]

The corporate security function employs technology, procedures, and people to shield the company against unfavourable circumstances. In addition to managing physical crises when they arise, corporate security detects, tracks, and discourages both internal and external threats to an organization's assets, people, and property. Additionally, it evaluates the organization's risks, reports them to management and executives, and takes the necessary precautions. It is not unusual for the corporate security function to share some of its duties with other departments. For example, while hazards to digital assets and information may fall under the purview of corporate security in some organisations, they are often handled by distinct but connected cybersecurity or information security departments inside a company. Similar to this, business continuity and resilience may exist independently of corporate security but in conjunction with it in certain organisations, even though they usually come under the corporate security umbrella.[10]

For the past twenty-five years, researchers have been more interested in corporate (organisational) information security. Additionally, it has been examined from a variety of perspectives, and depending on the particular area of study, distinct time periods can be identified. The notion that "the user is the weakest link in information security" served as the foundation for the first emphasis, which was solely on behaviour and the safe use of technology. Research on organisational behaviour and information security has looked at issues such as how users should act as individuals to avoid security breaches, how to spot possible security breaches, and how to react when this danger is discovered.[11]

How businesses determine their information security requirements and set up information security procedures appropriately may be a crucial information security question.[12] Technologies such as social network analysis, sentiment analysis tools, online reputation monitoring, and neuromarketing applications are increasingly being integrated into corporate security systems. Their primary role is

9 Burge, S. (2023): *What is Corporate Security?*, https://internationalsecurityjournal.com/what-is-corporate-security/.

10 Security executive council (2025): *What Is Corporate Security?*, https://securityexecutivecouncil.com/insight/corporate-security-career/what-is-corporate-security-2097.

11 Cram, W. A., Proudfoot, J. G. & D'Arcy, J. (2017): "Organizational information security policies: A review and research framework", *European journal of information systems*, *26*(6), 605-641. DOI: 10.1057/s41303-017-0059-9

12 Straub, D. W., Goodman, S., Baskerville, R. L., & Goodman, S. B. (2008): *Framing the Information Security Process in Modern Society*, Routledge. DOI: 10.4324/9781315288697-2

reflected in the timely recognition and prevention of digital risks, especially those that can affect the image and trust in the organization.[13]

An organisation may need to improve its information security posture for a variety of reasons relating to sound corporate governance. For instance, before establishing or maintaining a stakeholder relationship, a stakeholder may demand that the organization's information security be well handled. Since regulations are becoming more stringent and noncompliance can have major repercussions, senior management's dedication to information security has grown dramatically.[14] Systems were the main responsibility of IT departments, which also had part-time responsibility for preventing intruders from accessing systems. However, as information technology has become more widely used in organisations, technical personnel are no longer the only ones responsible for its deployment. Additionally, information security has experienced the same changes as information technology as a whole.[15] Nevertheless, the corporation is solely in charge of overseeing a safe IT and information environment and processing data securely. In order to meet the company's internal and external information security standards, the organisation controls its technical, human, and procedural resources.[16]

Policies pertaining to data privacy and compliance are necessary to guarantee that sensitive data is protected within corporate security. These guidelines are essential for preventing unwanted access to private information and helping to preserve the accuracy and dependability of security protocols. Enforcing stringent data privacy and compliance standards is essential because it lowers the risk of security-related incidents by preventing security breaches. Furthermore, following these guidelines is essential for achieving industry-specific standards and legal obligations in addition to improving organisational security. Businesses can give confidentiality and ethical information handling first priority by incorporating robust data privacy and compliance procedures, which is essential for any corporate security plan. For instance, 68% of organisations rank compliance with data privacy laws as one of their biggest obstacles to attaining full cybersecurity readiness, per recent surveys on corporate security trends.[17]

---

13 Baltezarević, R. & Baltezarević, V. (2022): "The influence of digital political communication supported by neuromarketing methods on consumer perception towards a tourist destination", *Megatrend revija,19*(2), 13-34. DOI: 10.5937/MegRev2202013B

14 Ransbotham, S., & Mitra, S. (2009): "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise", *Information systems research*, *20*(1), 121-139. DOI: 10.1287/isre.1080.0174

15 Andress, J. & Leary, M. (2017): *Building a practical information security program*, Syngress.

16 Ransbotham, S., & Mitra, S. (2009): "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise", *Information systems research*, *20*(1), 121-139. DOI: 10.1287/isre.1080.0174

17 Cybersecurity-insiders (2021): *Insider threat report*, https://www.cybersecurity-insiders.com/wp-content/uploads/2021/06/2021-Insider-Threat-Report-Gurucul-Final-dd8f5a75.pdf.

These days, there are several reasons why corporate security is so important. Being well-prepared is essential since the hazards are quite real and, regrettably, there are many different threats all around us. Regardless of size, every business can become a victim of a cybersecurity incident. However, since they think they are less likely to be targeted, small business owners are often indifferent. Given the prevalence of threats, a strong corporate security policy is necessary to control these risks. In addition to the concerns that exist now, it's crucial to remember that some risks are always changing. We must acknowledge that the hazards have grown and changed over time as e-commerce and remote employment have become more popular in recent years. Therefore, it's imperative that the company's corporate security plan changes along with it.[18]

Using cutting-edge tools and procedures to protect against malevolent internet activity is known as cybersecurity. Data protection also entails safeguarding private data against breaches or illegal access. Crucially, spending money on cybersecurity infrastructure strengthens defences against possible intrusions that can jeopardise vital company information. Furthermore, maintaining the integrity of sensitive company data and complying with legal requirements are guaranteed by following established data protection procedures. Furthermore, current patterns show an increase in security-related events that target companies all over the world. This highlights how crucial it is for security experts to remain current on changing cybersecurity tactics and use preventative measures designed to successfully counter contemporary cyberthreats. Strict access restrictions and encryption methods must be put in place in order to protect company networks and digital assets from illegal access and exploitation by threat actors who are constantly looking for weaknesses in organisational systems.[19]

Challenges in cybercrime investigation stem from the criminal innovation of perpetrators, the difficulty of accessing electronic evidence, and internal resource, capacity, and logistical constraints. Suspects often use anonymization and cloaking technologies, and new techniques quickly reach a wide criminal audience through the online crime marketplace.[20] The majority of cyberspace literature identifies cybercrime and espionage as the two main cyberthreats. According to scholars in this field, national security is also seriously threatened by large-scale strategic cyberattacks. Because the attack is inexpensive and the attacker is anonymous, the enemy gains the advantage. Additionally, they contend that because cyber defence

[18] Burge, S. (2023): *What is Corporate Security?*, https://internationalsecurityjournal.com/what-is-corporate-security/.S

[19] Therms (2025): *Corporate Security: What Companies Must Know*, https://www.therms.io/blog/corporate-security-what-companies-must-know/.

[20] Sandage, J. et al. eds. (2013): *Comprehensive Study on Cybercrime (United Nations Office on Drugs and Crime).*

tactics impose little to no cost on the unsuccessful attacker, who is then free to attempt again, they do not offer adequate security against cyberattacks.[21]

There are numerous national, regional, and international legal systems in the modern, globalised world. There are several layers of interaction between these systems. Because of this, the provisions occasionally conflict with one another, creating a conflict of laws, or they do not sufficiently overlap, creating gaps in jurisdiction. The question of whether and to what extent national legal distinctions in cybercrime laws can and should be minimised arises from these variations in national laws. Stated differently, what is the significance of harmonising cybercrime laws? There are several ways to do this, including regional or multinational initiatives that are both binding and non-binding. A united national approach can serve as the foundation for harmonisation.[22]

Ease of use and utility for end users and their organisations are key factors in the acceptance of ICT (information and communication technologies) developments; in other words, the functionality is user-friendly. Their findings indicate that cyber security is not a factor in ICT innovation. One would think that with the several cycles of ICT innovation we have experienced, cyber security requirements would be more prominent, but this is obviously not the case.[23] Nearly 30% of cyber-attacks identified in the previous 12 months as of September 2024 were hacking incidents. 15.2% of detections showed malware attacks, and another 28.7% involved abuse events.[24] One of the most often examined and debated types of cybercrime is hacking, which is a major source of public anxiety due to the danger that such behaviour presents to society. Unauthorised access to and subsequent usage of another person's computer system is a clear definition of hacking.[25]

By 2025, ransomware attacks had impacted around 63% of enterprises globally. All things considered, since 2018, almost 50% of all poll participants reported that ransomware has affected their companies. In total, 258 cyberattacks were reported against manufacturing industry organisations during the year under study. With 238 and 220 cyberattacks, respectively, government facilities came in second, followed by the healthcare and public health sectors.[26] The following are noteworthy recent

21 Clark, W. K. & Levin, P. L. (2009): "Securing the information highway: How to enhance the United States' electronic defenses", *Foreign affairs*, 2-10.

22 Sandage, J. et al. eds. (2013): *Comprehensive Study on Cybercrime (United Nations Office on Drugs and Crime)*.

23 Averill, B., Luiijf, E.A.M., (2010): "Canvassing the cyber security landscape: Why energy companies need to pay attention", *Journal on Energy Security*.

24 Petrosyan, A. (2025): *Global cyber incidents 2024, by type*, https://www.statista.com/statistics/1483769/global-cyber-incidents-by-type/?srsltid=AfmBOopKo2AbBCCwP_To4WFJicMebXmUHOZvPAb31dJ5ecNis-FFwuKL.

25 Yar, M., (2006): *Cybercrime and Society*, Sage Publication Ltd, London.

26 Petrosyan, A. (2025): *Businesses worldwide affected by ransomware 2018-2025*, https://www.statista.com/statistics/204457/businesses-ransomware-attackrate/?srsltid=AfmBOoptaUQk945PecCiCR3XZymMUPzrSzp1Ds7G7smxIa-JfCxqrsoZ.

cyberattacks on corporations: Ascension Health, a healthcare network that runs 140 hospitals in 19 U.S. states, was the target of a significant ransomware attack in May 2024. Communication systems, pharmacy services, and electronic medical records were all rendered inoperable by the intrusion. Consequently, Ascension announced operating losses of $1.8 billion for the fiscal year 2024, and patient numbers decreased by 8–12% in May and June over the prior year. Millions of patients' financial and medical information was also compromised in the hack. Around 270,000 people's personal information was compromised in a hack that hit the UK Ministry of Defence that same year. This contained the names, bank account information, and, in certain situations, the residential addresses of veterans, reservists, and active military personnel. A weakness in the payroll system used by contractor Shared Services Connected Ltd (SSCL) caused the intrusion. Although no official culprit was identified, some reports suggested that the hackers were Chinese. Finally, the hacking group DragonForce launched an attack on the British shop Marks & Spencer in 2025. Online sales were suspended as a result of the attack, and £300 million in losses resulted. The business was compelled to make significant investments in cybersecurity upgrades and temporarily halt its online operations.[27]

Advanced robotics and state-of-the-art surveillance systems are just two of the many cutting-edge tools and tactics that will be available to us as we enter a new era of corporate security by 2033. Future developments in technology will play a key role in corporate security.[28]

3. CONCLUSION

In our current environment, everything centres around digital connections, networking, and our reliance on technology. Corporate security has shifted from being a standalone task to becoming a vital part of the overall business strategy. This shift means that security now plays a crucial role in shaping an organization's sustainability, reputation, and competitive edge.

The paper emphasizes the vital role that information technologies play in boosting security measures. They do this by streamlining various processes, identifying risks at an early stage, and effectively managing incidents. It also points out the escalating complexity of cyber threats, particularly in our interconnected world. There's been a noticeable uptick in attacks on critical infrastructure and

[27] Datami Newsroom (2025): *Top 10 Cyberattacks That Brought Global Corporations to a Halt*, https://datami.ee/blog/top-10-major-cyberattacks-on-corporations-analysis-by-datami/.

[28] Francisco, C. (2023): *The Future of Corporate Security: A Fusion of Innovation and Expertise in 2033*, https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2023/december/the-future-of-corporate-security-a-fusion-of-innovation-and-expertise-in-2033/.

the misuse of data. Looking at real-world cases makes it abundantly clear just how much financial, legal, and reputational damage organizations could incur if they fail to allocate sufficient resources to both preventive and reactive security strategies.

As we step into the future, organizations will be challenged to balance regulatory obligations, adapt to rapid tech changes, and roll out security measures effectively. All of this will happen while they strive to boost the human element through ongoing employee training and awareness. The key to effective corporate security will be its ability to adapt dynamically to changes in the digital landscape, with collaboration among IT, management, and legal institutions being absolutely crucial.

With the rapid pace at which technology and digital threats are evolving, it's crucial to ramp up multidisciplinary research in this field. By connecting scientific insights with practical applications, we can develop security models that are not only more flexible but also stronger. The future of corporate security relies on an organization's capacity to foresee risks, recognize patterns in how attackers behave, and quickly roll out innovative solutions, all while keeping user trust intact, protecting data, and handling information responsibly.

Literature

- Andress, J. & Leary, M. (2017): *Building a practical information security program*, Syngress.
- Averill, B., Luiijf, E.A.M., (2010): "Canvassing the cyber security landscape: Why energy companies need to pay attention", *Journal on Energy Security.*
- Baltezarevic, I. & Baltezarević, R. (2020): „Uticaj komunikacije u virtuelnom okruženju na pravnu informatiku", *Megatrend Revija, 17*(4), 27-40. DOI: 10.5937/MegRev2004027B
- Baltezarević, R. & Baltezarević, V. (2022): "The influence of digital political communication supported by neuromarketing methods on consumer perception towards a tourist destination, *Megatrend revija, 19*(2), 13-34. DOI: 10.5937/MegRev2202013B
- Burge, S. (2023): What is Corporate Security?, https://internationalsecurityjournal.com/what-is-corporate-security/.
- Cassidy, K. (2019): "Corporate Security (Structure, Roles, Duties)", in: Shapiro, L., Maras, MH. (eds), *Encyclopedia of Security and Emergency Management*, Springer, Cham. DOI: 10.1007/978-3-319-69891-5_19-1
- Clark, W. K. & Levin, P. L. (2009): "Securing the information highway: how to enhance the United States' electronic defenses", *Foreign affairs*, 2-10.

- Cram, W. A., Proudfoot, J. G. & D'Arcy, J. (2017): "Organizational information security policies: A review and research framework", *European journal of information systems*, *26*(6), 605-641. DOI: 10.1057/s41303-017-0059-9
- Cybersecurity-insiders (2021): *Insider threat report*, https://www.cybersecurity-insiders.com/wp-content/uploads/2021/06/2021-Insider-Threat-Report-Gurucul-Final-dd8f5a75.pdf.
- Datami Newsroom (2025): *Top 10 Cyberattacks That Brought Global Corporations to a Halt*, https://datami.ee/blog/top-10-major-cyberattacks-on-corporations-analysis-by-datami/.
- Francisco, C. (2023): *The Future of Corporate Security: A Fusion of Innovation and Expertise in 2033*, https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2023/december/the-future-of-corporate-security-a-fusion-of-innovation-and-expertise-in-2033/.
- Li, H., Yoo, S. & Kettinger, W. J. (2021): "The Roles of IT Strategies and Security Investments in Reducing Organizational Security Breaches", *Journal of Management Information Systems*, *38*(1), 222–245.
- Ludbey, C. R., Brooks, D. J., & Coole, M. P. (2018): "Corporate security: Identifying and understanding the levels of security work in an organisation", *Asian Journal of Criminology*, 13, 109–128. DOI: 10.1007/s11417-017-9261-x
- Petrosyan, A. (2025): *Global cyber incidents 2024, by type*, https://www.statista.com/statistics/1483769/global-cyber-incidents-by-type/?srsltid=AfmBOopKo2AbBCCwP_To4WFJicMebXmUHOZvPAb-31dJ5ecNis-FFwuKL.
- Ransbotham, S., & Mitra, S. (2009): "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise", *Information systems research*, *20*(1), 121-139. DOI: 10.1287/isre.1080.0174
- Sandage, J. et al. eds. (2013): *Comprehensive Study on Cybercrime (United Nations Office on Drugs and Crime).*
- Security executive council (2025): *What Is Corporate Security?*, https://securityexecutivecouncil.com/insight/corporate-security-career/what-is-corporate-security-2097.
- Shapiro, L. & Maras, M-H. (2021): *Encyclopedia of Security and Emergency Management*, Springer Nature. ISBN: 978-3-319-70487-6
- Straub, D. W., Goodman, S., Baskerville, R. L., & Goodman, S. B. (2008): *Framing the Information Security Process in Modern Society*, Routledge. DOI: 10.4324/9781315288697-2
- Therms (2025): *Corporate Security: What Companies Must Know*, https://www.therms.io/blog/corporate-security-what-companies-must-know/.
- Yar, M., (2006): *Cybercrime and Society*, Sage Publication Ltd, London.

Marko Stanojević

Originalni naučni rad
Primljen 14.06.2025.
Odobren 17.08.2025.

ULOGA INFORMACIONIH TEHNOLOGIJA U SAVREMENOJ KORPORATIVNOJ BEZBEDNOSTI

Sažetak: *Današnje poslovno okruženje se kreće velikom brzinom, a sa digitalnom transformacijom u prvom planu, korporativna bezbednost se promenila od puko operativne odgovornosti do značajnog strateškog elementa. Ovaj pregledni rad istražuje načine na koje informacione tehnologije transformišu trenutni pejzaž modela korporativne bezbednosti. Ističe važnost integracije automatizovanih sistema, digitalnih alata za uočavanje i sprečavanje rizika i efikasnih strategija upravljanja incidentima. Naglašen je multidisciplinarni pristup, koji obuhvata fizičke, tehničke, ljudske i organizacione aspekte zaštite. Rad razmatra savremene izazove u sajber bezbednosti, fokusirajući se na sve veću složenost sajber napada, pritisak na strože regulatorne standarde i etička i pravna pitanja koja se javljaju u globalizovanom digitalnom okruženju. Ispitivanjem slučajeva iz stvarnog sveta, ističe se potreba za usvajanjem proaktivnog načina razmišljanja prilikom razvoja bezbednosnih strategija koje mogu da se suprotstave stalno evoluirajućim i složenim digitalnim pretnjama. Na kraju, zaključuje se da se informaciona bezbednost mora redovno ažurirati, biti usko povezana sa širom korporativnom strategijom i zasnivati na realnim procenama rizika kako bi se osigurala dugoročna stabilnost, ugled i konkurentnost organizacije.*

Ključne reči: *Korporativna bezbednost, Informacione tehnologije, Sajber pretnje, Digitalna transformacija*