Aleksandra Nikolova Marković*
https://orcid.org/0009-0000-9724-8739

UDC: 347.72.036/.037

DOI: 10.5937/MegRev2503201M
Review scientific paper
Received 03.10.2025.
Approved: 24.12.2025.

CYBERSECURITY AND DIRECTORS' DUTIES UNDER CORPORATE LAW AS ELEMENTS OF CORPORATE SECURITY

Abstract: *In recent years, with the increased use of information technology, cybersecurity has gained a central place in corporate security strategies, overcoming the traditional perception of cybersecurity as a strictly technical issue. This paper examines cybersecurity through the prism of corporate law, focusing on directors' duties of care and oversight as fundamental aspects for maintaining sustainable corporate security system. Special attention is devoted to the role of the board of directors in identifying, assessing, and managing cyber risks. Through an analysis of relevant academic literature, legal regulations, and case studies, the paper demonstrates that insufficient board oversight, inadequate risk reporting, and weak integration of cyber risk into corporate decision-making processes can cause multidimensional consequences for the company's reputation. The analysis shows that even though corporate law does not provide norms regarding cybersecurity issues, it establishes clear procedures and norms regarding informed decision-making, oversight, and risk recognition. In this sense, the paper concludes that the responsibilities of directors under corporate law represent the most important element in preserving corporate values, the trust of stakeholders, and in the preserving corporate security resilience.*

Keywords: *cybersecurity, corporate law, corporate security, directors' duties*

* Faculty of Law, Megatrend University, Belgrade, Republic of Serbia.
E-mail: anikmarkovic@gmail.com

INTRODUCTION

The emergence of the Internet and information technologies in the last few decades has fundamentally changed the way society, the economy and the way business is perceived. Information technology is an integral part of the execution of a huge number of critical business operations in modern organizations. In this sense, the advancement of digital technology has enabled the rapid exchange of information and more efficient execution of business organizations, but at the same time has made organizations vulnerable to cyber attacks and data security issues.[1] In the modern business environment, with the advancement of technology, cybersecurity has ceased to be an exclusively technical issue that is resolved within the IT sector. The frequency of cyber attacks and the risks associated with the storage and processing of business data have inevitably imposed the issue of redefining the position of cybersecurity in a business entity. The consequences of cyber attacks can seriously disrupt the operation of the organization and contribute to the occurrence of financial losses, loss of trust by stakeholders, and legal consequences for both the business entity and the organization's management. Furthermore, cyber attacks in modern times cannot be considered as an isolated incident that is addressed by the IT sector, but rather need to be understood as one of the key aspects of corporate security. The challenge and opportunity lie in harnessing AI's capabilities while being critically aware of its implications.[2]

In the academic literature, in the last few years, there has been a gradual abandonment of the traditional approach, according to which cybersecurity is viewed only as an area of technical nature. The traditional approach is inapplicable in modern organizations because digital technologies are involved in almost every business operation, which makes them particularly sensitive to cyber threats and various abuses of information. Given that the consequences of cyber attacks also affect customers, investors and all other interested parties, i.e. they go beyond the organization as a closed entity, it is necessary to think about corporate security, sustainability and resilience of the company from external influences.[3] Precisely for this reason, cyber-security is increasingly connected with the concept of corporate security, with the aim of protecting the integrity of the organization.

In regulating the corporate security system in an organization, corporate law plays an important role, through legal rules that relate to the position, powers and

1 Baltezarević, I. & Baltezarević, R. (2021): "Sajber bezbednost: Izgradnja digitalnog poverenja", *Megatrend revija*, *18*(4), 269–280.

2 Borivoje, B. (2023): "Decoding identity and representation in the age of AI", *Megatrend revija*, *20*(2), 141–146.

3 Kamiya, S., Kang, J. K., Kim, J., Milidonis, A. & Stulz, R. M. (2018): "What is the impact of successful cyberattacks on target firms?", *National Bureau of Economic Research*, 24409.

responsibilities of management bodies. Corporate law does not directly provide norms that relate to corporate security or cybersecurity, but it determines in detail the powers and responsibilities of the management body in the management of the company. In this sense, important for the topic of this paper are the norms that relate to the obligations to inform the management body, the obligation to act in good faith, the obligation to supervise and carefully perform management functions.

Based on the above, this paper aims to analyze the rights and obligations of directors and other responsible persons in maintaining a robust cybersecurity framework in the organization's corporate security system, through the prism of corporate law. Through the analysis of various legal concepts, case studies and academic literature, the paper aims to emphasize the importance of the role of effective organizational management by directors in creating a robust and sustainable cybersecurity system, as an integral part of corporate security.

1. CYBERSECURITY AS A CORPORATE SECURITY ISSUE

In the modern economy, cybersecurity is an important part of the strategy of companies, related to corporate security. Business organizations, regardless of the type of industry, have relied on information technologies in the last few decades. Dependence on information technologies makes companies more efficient, the exchange of information is instantaneous, but at the same time increases the possibility of cyber attacks on organizations. Different kinds of malicious actors, whether they are individual cybercriminals or criminals who have become sponsored entities, use different methods to exploit the weaknesses of companies in order to gain different kind of benefits.[4] In the past, cyber attacks were addressed individually by IT departments, but due to the increasing number of cyber attacks that can cause enormous damage, ranging from financial to reputational damage to companies, an increasing debate in academic circles about integrating cybersecurity into corporate security strategies has arisen.[5] Cyber incidents are increasingly turning into serious legal and financial issues. In 2013, the American Bar Association released its first handbook on cybersecurity, highlighting the growing scale of cyber threats. The handbook notes, citing PricewaterhouseCoopers, that hacking has become so widespread that large organizations should operate on the

[4] Smith, J. & Brown, L. (2022): "Zero trust architecture in corporate networks", *Network Security Journal*, (10), 65–82.

[5] Sayjari, T. & Melo Silveira, R. (2024): "Cybersecurity and corporate risk management: Aligning information security with business strategies", in: *Proceedings of the Congresso de Gestão de Riscos Corporativos (GRC)*, São Paulo, Brazil.

assumption that their systems have already been breached and use that assumption as the starting point for testing and strengthening their security defenses.[6] The resulting cyber incidents often lead to regulatory investigations, lawsuits initiated by shareholders, and visible market reaction, which clearly shows that cybersecurity represents an important segment of overall corporate security.

Empirical research confirms the need for redefining the position of cybersecurity in the system of an organization. Maleks Smith et al. noted that the impacts of ineffective corporate cybersecurity strategy have cost the global economy USD 945 billion in 2020.[7] Romanosky has concluded that the costs of cyber security incidents are estimated to be much more than the costs of technical compensation for damages.[8] The costs of remediation of cyber security incidents also include significant legal consequences, the obligation to report to regulatory bodies, as well as the challenge of maintaining relationships of trust with investors and customers. These findings call into question the opinions that cyber risks can be dealt with exclusively at the operational level, without involving corporate governance bodies.

In that sense, the cyber incident in the Yahoo company is a central case study in the academic discussion related to the position of cyber security in the organizational setting in the company. Yahoo announced in 2016 that in the previous few years, about a billion user accounts from their customers were subject to abuse, making this data breach the largest of all the times. This misuse of data has raised serious questions regarding the internal system of reporting, supervision and decision-making. Analysis of the case indicates that the problem was not only in technical failures, but also in insufficient transparency, delay in disclosing relevant information and limited involvement of the board of directors in the supervision of cyber risks.[9] The consequences of these failures were multi-dimensional, including regulatory investigations and fines, legal proceedings, and a reduction in purchase price when selling the company to Verizon, which clearly shows how cyber incidents can affect almost all aspects of the company.

These examples and research indicate the need to consider cybersecurity as an integral part of the corporate security of a company. In that context, the cited example and academic papers show that cybersecurity cannot be fully understood and managed without a legal framework of corporate law and strictly defined

6 Rhodes & Polley, editors (2013): *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals*, American Bar Association, 173.

7 Maleks Smith, Z., Lostri, E. & Lewis, J. A. (2020): "The hidden costs of cybercrime", https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.

8 Romanosky, S. (2016): "Examining the costs and causes of cyber incidents", *Journal of Cybersecurity*, *2*(2), 121–135.

9 Trautman, L. J. & Ormerod, R. (2017): "Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach", *American University Business Law Review*, 66, 1231-1291.

duties and responsibilities of the director. Therefore, it is argued that it is the duty of directors to play a key role in the incorporation of cybersecurity in the corporate security system and in the sustainability of the company.

2. BOARD OF DIRECTORS' DUTIES UNDER CORPORATE LAW AND CYBER SECURITY

Historically, just a decade ago, board members were not required to be technically prepared and knowledgeable in the details of the measures that the company takes regarding cybersecurity. However, due to frequent cyber threats and attacks, the role of board members in relation to cybersecurity is changing significantly. In modern business, board members must be included in the reporting and discussions related to the company's cybersecurity in order to ensure the security of operations.

On the other hand, corporate law provides for fiduciary duties for directors that aim to ensure an efficient corporate framework and effective oversight of operations. Duties of care and duties of oversight are of the utmost importance for corporate cybersecurity. The duty of care requires directors to make decisions on an informed basis and with appropriate diligence, while the duty of oversight obliges them to monitor the corporation's operations and risk management systems.

The norms of corporate law aim to regulate the organizational setup in a company that would enable the identification of potential risks, their addressing, and the formation of a system that would be resistant to cyber attacks. In this sense, corporate law does not require directors to have technical knowledge to take all necessary actions to prevent cyber attacks, but rather gives them the authority to form a corporate structure so that the risks of cyber attacks are minimized. This also means that the board of directors must provide a corporate structure that ensures the timely receipt of information regarding cyber threats or cyber incidents, so that they can react in a timely manner. Hill and Conaglen (2018) highlight that directors' duties focus on decision-making processes and the flow of information within the organization.[10] Payne (2019) notes that cybersecurity is a modern risk that should be under directors' oversight responsibilities.[11] As cyber threats are now widely recognized and potentially significant, boards can no longer treat them as irrelevant or insignificant, as cyber risk can be foreseeable and a material concern within directors' fiduciary duties.

[10] Hill, J. G. & Conaglen, M. (2018): *Directors' duties and corporate governance*, Oxford University Press.

[11] Payne, A. M. (2019): "What the Hack?! Reexamining the Duty of Oversight in an Age of Cybersecurity", *Georgia Law Review*, 54, 1–59.

2.1. Duties and Responsibilities of the Director of Corporate Law in Relation to Cybersecurity in the Republic of Serbia

Corporate law norms of the Republic of Serbia have been translated into the Law on Commercial Companies. This law does not regulate cybersecurity, but it has set a clearly arranged system of rules on the duties and responsibilities of directors, who can be included in the corporate security system of a company.

In Article 61 of the Law on Commercial Entities,[12] **a group of persons who have special duties towards the legal entity has been established. Among others, directors and representatives of companies have special duties.** According to Article 63 of the Law on Commercial Entities, the director is obliged to act with the care of a good businessman, i.e. to provide a level of care with which a reasonably careful person possessing knowledge and skills would act. In the context of cybersecurity, this standard means that a director must insist on receiving relevant and timely information regarding existing cyber risks and threats, as well as the duty to take relevant measures for the protection of the company. In the same article, the Law on Commercial Entities stipulates that the director is obliged to act in the best interest of the company. As we have already concluded, cyber incidents can have serious consequences for the financial position and reputation of the company. In this sense, it is in the best interest of the company to implement an adequate strategy for managing cyber risks, while neglecting the cyber threat can be considered as a breach of duty of acting in the best interest of the company, on the side of the managing director.

In addition to the above-mentioned duties of attention and actions in the interest of companies, it is also important to arise the question for the director's responsibilities for damage. According to the Article 64 of the Law on Commercial Entities[13], the director is liable to the company for the damage caused when breach of the duty of care. In the case of filing a lawsuit, the burden of proof that he has acted with due care falls on the director. In the context of cyber security, the question of actions of the director can be raised in the case of a cyber incident that has a multidimensional consequence, with the aim of examining whether the director has taken measures to prevent the damage caused.

The responsibility of the director can also be considered from the point of view of obligation law. According to Article 154 of the Law on Obligatory Relations,[14] a person who causes damage to another is obliged to compensate him, if he does

[12] Law on companies (Official Gazette of the Republic of Serbia, No. 36/2011, 99/2011, 83/2014, 5/2015, 44/2018, 95/2018, 91/2019, 109/2021, 19/2025).

[13] Ibid.

[14] Law on Obligations (Official Gazette of SFRY Nos. 29/78, 39/85, 45/89; Official Gazette of FRY No. 31/93; Official Gazette of SCG No. 1/2003; Official Gazette of the Republic of Serbia No. 18/2020).

not prove that the damage occurred without his fault. In the situation in which a cyber incident has led to increased risks of damage or damage to the company or third parties, and it is determined to be a failure in management, the director will be held accountable regardless of the fault.

As for the liability of the director in the event of a cyber incident, it is important to note that directors are not legally liable for each individual cyber attack or incident. Given that cyber attacks can be very sophisticated and impossible to completely eliminate, the director is liable only if it is shown that he did not act conscientiously, with due care, or ignored potential risks that could indicate a possible cyber attack. Duties and responsibilities of directors in Serbian corporate law provide a flexible, but also clear normative framework for treating cybersecurity as an element of corporate security. Although the law does not deal directly with cybersecurity, it prescribes general rules for the actions of directors, in order to avoid possible damage. In this sense, the fact that cybersecurity is not just a technical issue, but an issue that can have large-scale legal consequences and should be included in the company's corporate security strategy, is once again confirmed.

3. REASONABLE CYBER OVERSIGHT AND RECOMMENDATIONS FOR OVERSIGHT ACTIONS

Given the evolving nature of cyber threats, directors regularly face the challenge of how to recognize a cyber threat while simultaneously upholding their duties of care, oversight, and the best interests of the company. When we add to that the lack of technical knowledge of directors, cybersecurity risk management becomes increasingly difficult. In these cases, the decision made may have multiple consequences, but it is important to emphasize that in the event of a dispute, the court will give greater importance to the decision-making process by the directors, in terms of whether it was made reasonably and informedly, than to the decision itself. Lunn (2014)[15] in his paper, emphasizes that effective board-level cybersecurity oversight should require a structured and proactive governance process that integrates systematic risk management, informed judgment, and access to appropriate expertise. In assessing cyber risk, boards should consider the likelihood and potential losses, including high-impact and hard-to-quantify consequences such as reputational damage, stakeholder trust loss, and other ultra-high-value risks. When the expected impact of a cyber-risk outweighs the cost of prevention, appropriate mitigation measures should be implemented, with greater attention

[15] Lunn, B. (2014): "Strengthened director duties of care for cybersecurity oversight: Evolving expectations of existing legal doctrine", *Journal of Law & Cyber Warfare*, *4*(1), 109–137.

given to risks that pose more significant potential harm.[16] Specific caution should be applied in high-value cases, as certain losses may be unacceptable under almost any circumstances. Some of the oversight actions that should be undertaken by the board of directors when addressing to cyber threats are as follows:

- regular involvement of the board in all processes related to cybersecurity;
- existence of clear rules and programs for corporate security that include procedures in case of cyber threats;
- existence of a legal framework that precisely defines the directors' obligations,[17]
- education of directors related to cybersecurity;
- engagement of external experts in the field of cybersecurity in order to supervise the implementation of relevant programs;
- existence of a clear legal framework in terms of determining the obligations for conducting cybersecurity oversight.

These recommendations will help to surpass the unrealistic expectations on directors while recognizing their central role in shaping organizational responses to cyber risk.

CONCLUSION

In the era of accelerated digital expansion, corporate security systems are increasingly exposed to complex and evolving threats that frequently exceed the capabilities of traditional security approaches.[18] This paper has shown that in these evolving times, cybersecurity should exceed the traditional approach, where it was observed only as a technical or operational matter. Also, the role of directors in addressing the cyber threats is of essential importance for creating and maintaining sustainable and resilient corporate security systems.

This paper has demonstrated that directors' duties under corporate law can provide a comprehensive legal framework for addressing cybersecurity as a corporate governance and security issue. By focusing on the duties of care and oversight, the analysis shows how corporate law shapes requirements regarding the management of cyber risks. The paper highlights that a lack of supervision, inadequate reporting on cyber risks, and directors' weak involvement in cybersecurity decision-making processes can lead to serious consequences for the company's

[16] Kaplan, R. S. & Mikes, A. (2012): "Managing Risks: A New Framework", *Harvard Business Review*.

[17] Đorđević, I. Lj. & Ljubojević, R. (2018): "Ekonomski aspekti korporativne bezbednosti", *Megatrend revija*, *15*(3), 113–128.

[18] Stanojević, M., and Izgarević, D. (2025). Integration of artificial intelligence in corporate information security systems. Megatrend Review, 22(2), 51–60.

reputation, as well as liability for the caused damage. Furthermore, it can be concluded that cybersecurity is the area in which corporate law and corporate security are clearly interconnected. Fulfilling the duties of directors in accordance with corporate law can contribute to strengthening corporate values, increasing stakeholder loyalty, and maintaining a stable corporate security system.

LITERATURE

- Baltezarević, I. & Baltezarević, R. (2021): "Sajber bezbednost: Izgradnja digitalnog poverenja", *Megatrend revija*, *18*(4), 269–280.
- Borivoje, B. (2023): "Decoding identity and representation in the age of AI", *Megatrend revija*, *20*(2), 141–146.
- Đorđević, I. Lj. & Ljubojević, R. (2018): "Ekonomski aspekti korporativne bezbednosti", *Megatrend revija*, *15*(3), 113–128.
- Hill, J. G. & Conaglen, M. (2018): *Directors' duties and corporate governance*, Oxford University Press.
- Kaplan, R. S. & Mikes, A. (2012): "Managing Risks: A New Framework", *Harvard Business Review*.
- Kamiya, S., Kang, J. K., Kim, J., Milidonis, A. & Stulz, R. M. (2018): "What is the impact of successful cyberattacks on target firms?", *National Bureau of Economic Research*, 24409.
- Law on companies (Official Gazette of the Republic of Serbia, Nos. 36/2011, 99/2011, 83/2014, 5/2015, 44/2018, 95/2018, 91/2019, 109/2021, 19/2025).
- Law on Obligations (Official Gazette of SFRY Nos. 29/78, 39/85, 45/89; Official Gazette of FRY No. 31/93; Official Gazette of SCG No. 1/2003; Official Gazette of the Republic of Serbia No. 18/2020).
- Lunn, B. (2014): "Strengthened director duties of care for cybersecurity oversight: Evolving expectations of existing legal doctrine", *Journal of Law & Cyber Warfare*, *4*(1), 109–137.
- Maleks Smith, Z., Lostri, E. & Lewis, J. A. (2020): "The hidden costs of cybercrime", https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.
- Payne, A. M. (2019): "What the Hack?! Reexamining the Duty of Oversight in an Age of Cybersecurity", *Georgia Law Review*, 54, 1–59.
- Romanosky, S. (2016): "Examining the costs and causes of cyber incidents", *Journal of Cybersecurity*, *2*(2), 121–135.
- Rhodes & Polley, editors (2013): *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals*, American Bar Association, 173.

- Sayjari, T. & Melo Silveira, R. (2024): "Cybersecurity and corporate risk management: Aligning information security with business strategies", in: *Proceedings of the Congresso de Gestão de Riscos Corporativos (GRC)*, São Paulo, Brazil.
- Smith, J. & Brown, L. (2022): "Zero trust architecture in corporate networks", *Network Security Journal*, (10), 65–82.
- Stanojević, M. & Izgarević, D. (2025): "Integration of artificial intelligence in corporate information security systems", *Megatrend Review*, *22*(2), 51–60.
- Trautman, L. J. & Ormerod, R. (2017): "Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach", *American University Business Law Review*, 66, 1231-1291.

Aleksandra Nikolova Marković

Pregledni naučni rad
Primljen 03.10.2025.
Odobren 24.12.2025.

SAJBER-BEZBEDNOST I DUŽNOSTI DIREKTORA U OKVIRU POSLOVNOG PRAVA KAO ELEMENTI KORPORATIVNE BEZBEDNOSTI

Apstrakt: *Poslednjih godina, usled sve intenzivnije upotrebe informacionih tehnologija, sajber-bezbednost je zauzela centralno mesto u strategijama korporativne bezbednosti, prevazilazeći tradicionalno shvatanje prema kojem je bila posmatrana isključivo kao tehničko pitanje. Ovaj rad razmatra sajber-bezbednost iz ugla poslovnog prava, sa posebnim osvrtom na dužnosti pažnje i nadzora direktora kao ključne elemente održivog sistema korporativne bezbednosti. Posebna pažnja posvećena je ulozi odbora direktora u identifikaciji, proceni i upravljanju sajber rizicima. Kroz analizu relevantne akademske literature, pravnih propisa i odabranih studija slučaja, u radu se ukazuje da nedovoljan nadzor odbora direktora, neadekvatno izveštavanje o rizicima i slaba integracija sajber rizika u procese korporativnog odlučivanja mogu dovesti do višedimenzionalnih posledica, naročito u pogledu ugleda kompanije. Analiza pokazuje da, iako korporativno pravo ne propisuje posebne norme koje se direktno odnose na sajber-bezbednost, ono uspostavlja jasne standarde u pogledu informisanog odlučivanja, efikasnog nadzora i prepoznavanja relevantnih rizika. U tom smislu, rad zaključuje da dužnosti direktora u okviru korporativnog prava predstavljaju jedan od ključnih elemenata očuvanja korporativne vrednosti, poverenja zainteresovanih strana i izgradnje otpornog sistema korporativne bezbednosti.*

Ključne reči: *sajber-bezbednost, poslovno pravo, korporativna bezbednost, dužnosti direktora*