CYBERSECURITY IN HEALTHCARE, BANKING, AND INSURANCE SECTORS REGULATIONS, SIMILARITIES AND DIFFERENCES INSIGHTS FROM NORTH MACEDONIA

Nora Taravari
University Mother Theresa Skopje, Faculty of Social Sciences, North Macedonia,
nora.taravari@unt.edu.mk
Njomza Selimi Osmani
University of Tetovo, School of Law, North Macedonia, njomza.selimi.osmani@unite.edu.mk

Abstract: The roots of cybersecurity legislation can be traced to 2008, with the initiative of drafting of the first European Critical Infrastructure (ECI) Directive, which focused primarily on transport and energy infrastructure. While this Directive laid the groundwork for establishing a unified approach, it did not yet address cybersecurity-related risks. Since, North Macedonia has been progressing in cybercrime regulation, prevention, and treatment. Cybersecurity poses particular challenges in healthcare, banking, and insurance, sectors that have similarities but also significant differences, because of the types of data, regulations, and risks they manage. The progress of information and communication technologies, the digitalization of almost all areas of the society, provide benefits for the citizens and institutions but at the same time face risks and challenges of data protection, breach of protocols, and various aspects of violations of cybersecurity. According to available data, the National Cybersecurity Index is 66.67 which falls in the category of "good" but not "top tier". National legislation, strategic documents, and sectoral action plans feed towards fighting cybercrime. Healthcare, banking and insurance sectors are facing particular risks, and experience similarities and differences with respect to the specifics of the customer/ client data scope, storage, and usage. Research on cybersecurity in healthcare, banking, and insurance reveals significant social and economic consequences, including the loss of sensitive data, weakened public trust in essential services, and increased systemic vulnerabilities. This research aims to identify legislative documents and country achievements in respect to cybersecurity challenges, as well as the specifics of those in particular sectors, such as healthcare, banking and insurance. The research is based on available data analysis, official documents on legislation and cybersecurity strategies and action plans, as well as theory specifics of cybersecurity in health, banking, and insurance sectors. This research will evaluate the effectiveness of policies designed to address cybersecurity issues in those industries in North Macedonia, exploring how the consequences can be prevented and risks mitigated. These findings highlight the urgent need to address regulatory gaps, technological weaknesses, and workforce shortages to strengthen defenses, maintain stability, and ensure sustainable sectoral development. It is evident that detailed research and analysis should be further carried for each sector separately, so the purpose of this paper is to identify similarities and differences rather than to give detailed, in-depth recommendations for each sector. But the path is obvious: by addressing the issues regarding cybersecurity in these three important sectors, through legislation, country strategy and action plans, as in light to constant development of the information and communication technologies, and the sophistication of the cyber-attacks, North Macedonia can transform this challenge into an opportunity for long-term growth and development.
Keywords*:* Cybersecurity, Healthcare, Banking, Insurance, client data, data safety.

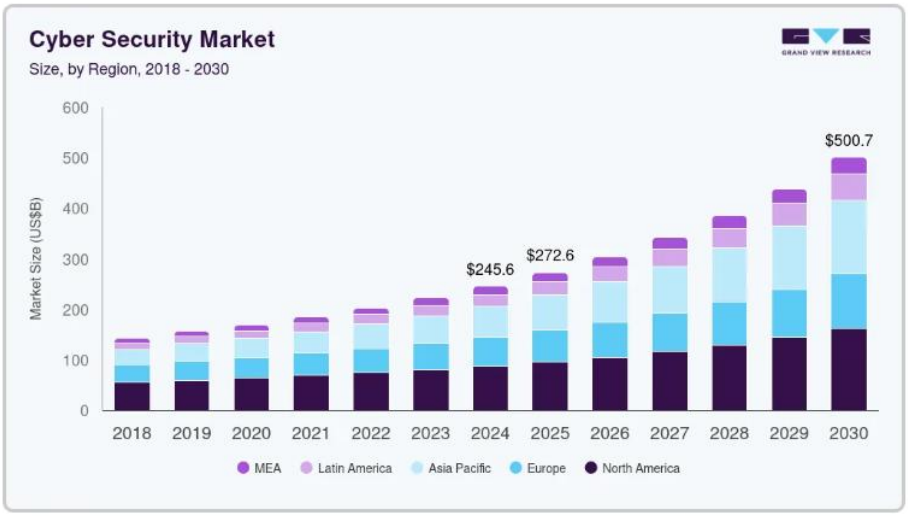
1. INTRODUCTION

Contemporary life relies heavily on information and communication technologies. There is no sector that is not digitized/digitalized, although the extent varies on the specifics of each sector, ranging from agriculture, mining, recreation, construction, and even healthcare as least digitized (Cheema, 2023), to the obvious technology sector, followed by media, financial services (banking and insurance), and professional services (Manyika et all, 2016). Digitization is often a foundational step in the more profound process of digitalization. To clarify: "Digitization refers to the process of converting information into a digital format, while digitalization refers to the broader transformation of business processes and activities to take advantage of digital technologies and data" (Honeywell, 2023).

The digitalization process poses twofold challenges to any business. The first set of challenges pertains to the process of introduction of the technologies, and the second derives from the use of the technologies, and the maintenance of data safety and security. While the first set of challenges involves factors which are predominantly internal and conditioned by the companies, ranging from vision, strategy, and budget to employee buy-in and

respective training, the second involves external factors which are harder to control and thus bearing higher risks, involving regulations, competition, keeping up with technological advancements, and – above all - cybersecurity.
The roots of cybersecurity legislation can be traced to 2008, with the drafting of the first European Critical Infrastructure (ECI) Directive, which focused primarily on transport and energy infrastructure. While this directive laid the groundwork for establishing a unified approach, it did not yet address cybersecurity-related risks. Since, North Macedonia has been progressing in cybercrime regulation, prevention, and treatment. According to available data, the National Cybersecurity Index is 66.67 which falls in the category of "good" but not "top tier" (e-Governance Academy, n.d.). National legislation, strategic documents, and sectoral action plans feed towards fighting cybercrime. Healthcare, banking and insurance sectors are facing particular risks, and experience similarities and differences due to the types of data, regulations, and risks they manage.

Figure 1: Growth of cybersecurity market



Source: Grand View Research, 2025

Research on cybersecurity in healthcare, banking, and insurance reveals significant social and economic consequences, including the loss of sensitive data, weakened public trust in essential services, and increased systemic vulnerabilities. The purpose of this paper is to explore major specifics of cybersecurity in the above sectors, based on available data analysis, official documents on legislation and cybersecurity strategies and action plans, as well as theory specifics of cybersecurity in health, banking, and insurance sectors. These findings highlight the urgent need to address regulatory gaps, technological weaknesses, and workforce shortages to strengthen defenses, maintain stability, and ensure sustainable sectoral development.

2. METHODOLOGY

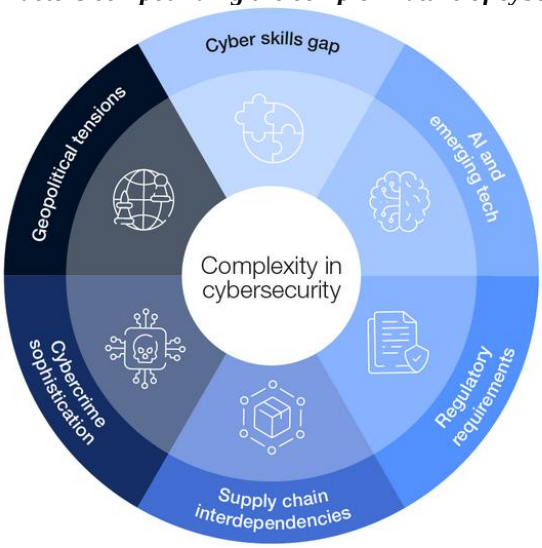
The protection of sensitive financial and personal data in North Macedonia's banking and insurance and healthcare sectors has become an essential cybersecurity matter. The analysis of system operations enables the identification of vulnerabilities which leads to developing enhanced legal and institutional security measures. The solution of these problems leads to dual benefits of protecting information while enhancing the dependability of essential services and strengthening public trust in them.
It is of utmost importance and necessity to implement the European standards through national policy alignment with NIS2 (European Commission, 2022) and GDPR (European Union, 2016) regulations to achieve data protection and security practices that match EU member state standards. The European Union Agency for Cybersecurity (ENISA, 2023) publishes reports which analyze healthcare and financial service risks and provide specific recommendations for mitigation. North Macedonia can achieve EU standards and enhance its critical infrastructure security through the implementation of these insights while strengthening its regulatory frameworks to create a safer digital space for citizens and businesses.
For this paper, examining digitalization and cybersecurity in banking, insurance, and healthcare, and obtaining information pertinent to North Macedonia was able through reviewing secondary sources and data available online, ranging from the EU Directive to national regulations, for the legislative part, as well as sector specific information – general and local, for each of the explored sectors.

Therefore, this paper will explore the methodology in identifying cybersecurity index, major cybersecurity risks in each sector, compare similarities and identify differences, and examine regulations that address these sectors in EU and in North Macedonia, to identify areas where strengthening regulation and prevention is necessary.
In addition, it is noteworthy to acknowledge the limitations to this research due to data availability and the daily changes in the cybersecurity landscape.

3. RESULTS

Banks, insurance companies, and health institutions operate with large volumes of personal data that should be stored and granted access to with maximum caution and prudence. Any information leakage, manipulation, or data loss can have extreme consequences and put people's well-being at risk, both in terms of health and financial wealth.
The latest Global Security Outlook report, published in January 2025 reveals the increasing complexity of the cyber landscape, which has profound and far-reaching implications for organizations and nations. Two of the main drivers include issues pertinent to this paper:
- The rapid adoption of emerging technologies, contributing to new vulnerabilities as cybercriminals harness them effectively to achieve greater sophistication and scale; and
- The proliferation of regulatory requirements around the world is adding a significant compliance burden for organizations. (World Economic Forum, 2025).

Figure 2: Factors compounding the complex nature of cybersecurity



Source: World Economic Forum, Global Cybersecurity Outlook 2025

According to the same source, cybercriminals are using advanced tools to enhance the impact and reach of traditional attacks like ransomware and business email compromise (BEC). Generative AI technologies are making phishing and social engineering campaigns cheaper and easier to execute, giving attackers easier access to organizations. As a result, although the basic nature of cyberattacks has not changed, organizations should focus more on defending against sophisticated phishing schemes and cyber fraud.
To better understand North Macedonia's overall cybersecurity preparedness, the National Cyber Security Index provides valuable insight into the country's progress and current position.
Based on the methodology of the NCSI, North Macedonia has progressed from 61st to 45th position, with the NCSI value of 66.67 and the DDL of 58.31, showing a difference of 8.36 (e-Governance Academy, n.d.).

Figure 3: Detailed overview of cybersecurity indicators for North Macedonia

Category	No.	Indicator	Score	Max Score
Strategic Cybersecurity Indicators	1	Cybersecurity Policy	12	15
	2	Global Cybersecurity Contribution	4	6
	3	Education and Professional Development	9	10
	4	Cybersecurity Research and Development	0	4
Preventive Cybersecurity Indicators	5	Cybersecurity of Critical Information Infrastructure	3	12
	6	Cybersecurity of Digital Enablers	8	12
	7	Cyber Threat Analysis and Awareness Raising	6	12
	8	Protection of Personal Data	4	4
Responsive Cybersecurity Indicators	9	Cyber Incident Response	11	14
	10	Cyber Crisis Management	5	9
	11	Fight Against Cybercrime	16	16
	12	Military Cyber Defence	2	6

Source: e-Governance Academy, n.d.

While each of the above indicators is presented relative to the maximum score, some values are less encouraging than others, with the one on inexistent R&D with respect to cybersecurity.

Turning now to the sectoral specifics, it is clear that banking, insurance, and healthcare share certain challenges, yet face distinct risks due to their unique data types, regulations, and technological maturity.

Specific for the banks, yet pertinent to at least the insurance companies, and other institutions within the financial sector, these are the major cybersecurity threats in 2025 (Duncan, 2024): 1. Ransomware - files are encrypted, and users are locked out, with the criminals demanding money to re-access the system; 2. Ongoing risks from remote work - Employees are no longer always accessing data on systems and networks that are controlled by the organization, so extra vigilance is necessary; 3. Cloud-based cyberattacks on the rise - Banks need to ensure that the cloud infrastructure is configured securely to protect from harmful breaches; 4. Social engineering - People can be tricked into giving over sensitive details and credentials. This can equally affect a bank's employees or its customers; and 5. Supply chain attacks - targeting a software vendor and then deliver malicious code to customers and others in the supply chain which would compromise the distribution systems and enable the cybercriminals to enter the supplier's customers' networks.

Cybersecurity in Banking: North Macedonia is served by banks subject to strong regulations which ensure financial data stays secure, stability is preserved, and fraud is outpaced. National Bank of the Republic of North Macedonia (NBRNM) The National Bank sets concrete cybersecurity requirements for banks to have strong IT security in place, to conduct regular risk assessments and to report incidents in a timely manner. Banks must also adhere to EU regulation, such as the Payment Services Directive (PSD2), which requires secure authentication of a customer for online transactions and places stringent restrictions on electronic payments. Cyber threats in the banking sector are phishing, malware, ransomware, and insider threat, while it can pose risk to both financial stability and customer confidence.

To help manage these risks, banks employ layered security measures such as, firewalls, intrusion detection systems, encryption and ongoing monitoring. There's also the issue of staff education on being cyber aware, as human error continues to be one of the top causes of breaches. In addition, the banking industry puts a high level of 'resilience' into their business continuity so they can continue to operate during such events. The sector is already supported by compliance audits and cybersecurity certification that enhance security, aligning with global best practices (Security Boulevard, 2024).

Cybersecurity in Insurance: The insurance sector in North Macedonia, while not as digitized as banking, is increasingly adopting digital platforms for policy management, claims processing, and customer service. This digital shift introduces new cybersecurity challenges which include: Phishing Attacks aimed at stealing login credentials and personal information; Data Breaches: The collection of personal and financial information makes insurance companies attractive targets for cybercriminals; and Third-Party Risks: Collaborations with third-party vendors can introduce vulnerabilities if these partners have inadequate cybersecurity measures.

Cybersecurity in Healthcare: The healthcare sector in North Macedonia faces specific cybersecurity challenges because of the sensitive nature of health data and the growing digitalization of health services. Although the country has progressed in digital transformation, the healthcare sector has been slower to focus on cybersecurity. Cyberthreats in healthcare include: Ransomware Attacks: Healthcare institutions are prime targets for these attacks because their services are critical and patient data is sensitive; Data Breaches: Unauthorized access to patient records

can result in serious privacy violations and legal issues; and Insider Threats: Employees or contractors with access to sensitive information may cause data breaches, either intentionally or accidentally.

Looking further into the regulatory environment, North Macedonia has taken significant steps to align its frameworks with EU standards, but also faces challenges in implementation and enforcement.

In May 2025, the Government approved North Macedonia's first-ever Cybersecurity Law along with a revised Law on Electronic Communications, aligning both with the EU's NIS2 Directive. The Cybersecurity Law establishes critical institutional bodies: National Cybersecurity Council, Government Security Operations Centre (SOC), and a dedicated Cybersecurity Department within the government. It mandates cybersecurity roles in all strategic public institutions and critical infrastructure operators. These laws are part of the broader Reform Agenda for Digitalization and Transparency and aim to elevate cybersecurity across the public and private sectors (Karanovic & Partners, 2025).

Cybersecurity regulation in North Macedonia's banking sector is primarily overseen by the National Bank of the Republic of North Macedonia (NBRM), which enforces the Decision on the Bank's Information System Security, first adopted in 2003 and most recently updated in 2018. This bylaw requires banks to comply with internationally recognized frameworks such as ISO 27001, the Basel Committee's Principles for Sound Management of Operational Risk, and guidelines from the Bank for International Settlements and NIST, while allowing for the adoption of additional standards provided they do not conflict with mandated requirements.

Figure 4: Overview of sectors' cybersecurity specifics

	Banking	**Insurance**	**Healthcare**
Protecting Customer	Banks handle sensitive personal and financial information. Keeping it safe from identity theft, fraud, and breaches is essential.	Insurers collect vast amounts of personal, financial, and even health information. Safeguarding this data from breaches is critical to maintaining trust.	Medical records hold some of the most personal details about us. Keeping electronic health records (EHRs) and other sensitive data safe from hackers or leaks is a top priority.
Securing Transactions	From online banking apps to ATMs and payment systems, cybersecurity ensures that every transaction is accurate and tamper-proof.	With more customers using apps and online portals, strong cybersecurity ensures quotes, claims, and payments are processed safely.	Securing Medical Devices From heart monitors to infusion pumps, many medical devices are now connected online. Strong cybersecurity ensures they keep working properly and aren't tampered with.
Defending Against	Cybercriminals constantly try to exploit weaknesses through phishing, ransomware, or account takeovers. Banks must stay one step ahead.	Fraudsters exploit weak spots to file fake claims or steal identities. Advanced monitoring and cyber controls help insurers detect and stop them.	Keeping Hospitals Running Cyberattacks can shut down systems and delay treatment. Safeguards help hospitals stay resilient and make sure patients get uninterrupted care.
Regulatory Compliance	Banking regulations (like PSD2 in the EU or DORA from 2025) set strict rules for managing risks and reporting incidents.	Insurance regulators demand strict adherence to cybersecurity and data protection standards, requiring firms to manage risks and report incidents.	Following the Rules Healthcare providers must meet strict regulations, like HIPAA, which set standards for protecting patient data.
Incident Response	Even the best defenses can be breached. Banks need strong plans to detect, respond, and quickly recover to minimize customer impact.	Even well-defended insurers can face breaches. A clear plan for detection, response, and recovery helps protect customers and the business	Being Ready for Attacks Even with strong defenses, breaches can happen. A good plan for detecting, responding to, and recovering from incidents reduces the damage.
The Bigger Picture	Customer Trust: A breach can erode confidence and drive customers away. Financial Integrity: Cyberattacks can compromise transactions and financial records. Business Continuity: Disrupted services can paralyze payment systems and cause widespread economic effects. Regulatory & Legal Costs: Fines and lawsuits can be massive after a breach. Reputation: Trust is a bank's greatest asset — once lost, it's hard to rebuild	Customer Trust: Insurance is built on promises. A data breach can break that trust. Data Accuracy: Reliable information is essential for fair risk assessment, pricing, and claims processing. Operational Resilience: Cyberattacks can stall claims and disrupt customer service. Financial Costs: Breaches bring regulatory fines, lawsuits, and remediation expenses. Reputation: Public confidence can take years to restore after a major cyber incident.	Patient Safety: Cyber risks can affect treatments and even endanger lives. Trustworthy Data: Doctors rely on accurate records to make the right medical decisions. Smooth Operations: Attacks can cause delays, cancellations, and extra costs. Financial Impact: Breaches bring fines, lawsuits, and recovery expenses. Reputation: A single incident can damage public trust in a healthcare organization.

Source: Global Cyber Security Capacity Centre, University of Oxford, 2018

Compliance is supervised through the NBRM's dedicated IT supervision unit, with sanctions for violations. Beyond sector-specific rules, North Macedonia recently adopted its first Cybersecurity Law and a revised Law on Electronic Communications in 2025, aligning national policies with the EU's NIS2 Directive and establishing a National Cybersecurity Council, a government Security Operations Centre, and institutional cybersecurity roles across critical infrastructure (Ministry of Digital Transformation, 2025; Karanovic & Partners, 2025). Within the financial sector, the Macedonian Banking Association (MBA) coordinates through its Commission for Information Security, which facilitates collaboration between banks and public institutions on regulatory alignment, particularly under the new Law on Payment Services and Payment Systems (MBA). Together, these measures demonstrate North Macedonia's dual approach of sector-specific enforcement through the NBRM and broader national alignment with European cybersecurity standards, aimed at strengthening resilience and trust in its banking system.

In addition, the regulations below have been adopted to address issues with cybersecurity across the sectors: Law on Personal Data Protection (DP Law): Enacted in 2020, this law regulates the processing of personal data, including sensitive health information. It aligns with the EU's General Data Protection Regulation (GDPR), emphasizing the protection of personal data and the rights of individuals. Similar to the healthcare sector, the insurance industry must comply with the DP Law, ensuring the protection of personal data and adherence to GDPR principles; and National Cybersecurity Strategy (2022): North Macedonia's first comprehensive cybersecurity strategy, adopted in 2022, reflects the country's European ambitions and is based on the principles of the EU's Cybersecurity Strategy and the NATO Cyber Defense Pledge. This strategy aims to enhance the country's cybersecurity posture across all sectors, including healthcare. Also, the insurance sector is included in the national strategy, which outlines measures to protect critical infrastructure and sensitive data across all sectors.

Ultimately, the following sector specific measures are promoted: a) Digital Health Initiatives: The introduction of digital health records and eHealth platforms has improved service delivery but also increased exposure to cyber threats; b) Security Awareness Training: There is a growing emphasis on training healthcare professionals to recognize and respond to cybersecurity threats; c) Investment in Cybersecurity Infrastructure: Some healthcare institutions are beginning to invest in advanced cybersecurity measures, though resources remain limited; d) Adoption of Cybersecurity Standards: Some insurance companies are adopting international cybersecurity standards, such as ISO/IEC 27001, to enhance their security posture; e) Cyber Insurance Policies: The uptake of cyber insurance policies is increasing, providing financial protection against potential cyber incidents; and f) Regulatory Compliance: Insurance companies are working to ensure compliance with national and international regulations to avoid legal and financial penalties.

4. CONCLUSION

Along with the quick digitalization in North Macedonia, there are opportunities as well as risks especially in the banking, insurance and health sector, being areas with extremely sensitive personal and financial data - crucial for the health of citizens and for their trust, yet attractive for cybercriminals. Although the fundamentals behind cyber threats have not significantly changed, attackers now have better instruments to their disposal, in particular with the use of generative AI and other techniques, which forces institutions to constantly modify defenses.

Meanwhile, North Macedonia has taken strides to enhance its cybersecurity offerings. Its rise in the National Cybersecurity Index and alignment of national laws with EU laws (like the NIS2 Directive, GDPR) clearly shows country's dedication on raising the level of resilience in cyberspace. The creation of permanent institutional entities (e.g. the National Cybersecurity Council) as well as a government Security Operations Centre are major progress towards systemic defense. Yet the lack of significant cybersecurity R&D and the resource pressures on organizations highlight important gaps that need to be filled to meet new threats.

The comparison of banking, insurance, and healthcare demonstrates that although these sectors have similar threats, risks, and responses, the latter vary in relation to the digital heritage and regulatory constraints. The most digitized and regulated sector being banking, has the strongest institutional security and layered defense, but is still susceptible to ransomware, phishing and supply chain attacks. Insurance, which is moving to digital solutions slowly yet inescapably, faces challenges in data protection and third-party risks, but is gradually standardizing with worldwide risk models and looking at cyber insurance. Healthcare is especially at risk because of the lack of investment in cyber security, sluggish tendencies to adopt digital technology, and because it is providing life-critical services, where a single failure could prove fatal for a patient. It's that in each industry — and across the three in general — maintaining a company's compliance with new regulations, investing in high-level cybersecurity and training humans to spot and thwart possible security threats remain the most challenging aspects of a robust security program. Labor shortages and low cybersecurity literacy among individuals continue to be pressing challenges that weaken the resilience of institutions. Furthermore, the overhead of quickly evolving regulations is essential to lift security requirements but may become a burden to organizations who struggle budget-wise. This is notably the case

for North Macedonia, which has to align its own instruments with those of the EU, while guaranteeing that the relevant local institutions enjoy the necessary capacity to successfully apply these instruments.

5. RECOMMENDATIONS

The level of cybersecurity of North Macedonia represents a country in transition –progressing through legal and institutional amendments but struggling with practical constraints in terms of resources, infrastructure and knowledge. The country's trend towards adoption of EU cybersecurity models bodes well for rebuilding better in the future. Nevertheless, in order to protect and enable other important segments such as banking, healthcare, insurance, etc., North Macedonia will have to continue investing in cybersecurity infrastructure, enhance public-private collaboration and create human resources that will be able to cope with the changing cyber threat landscape. Trust, safety and stability of the digital society in North Macedonia are feasible only via an inclusive combination of the regulatory alignment, technology development and capacity growth.

REFERENCES

Asset Voyager. (2024). Understanding the Cybersecurity Risks in Banking Sector: A Critical Overview. *Asset Voyager*. https://assetvoyager.com/cybersecurity-risks-in-banking-sector/

Belfry Software. (2024). How To Do Bank Security Right: Best Practices for 2024. *Belfry*. https://www.belfrysoftware.com/blog/bank-security/

Cheema, R. (2023, May 15). 5 least digitized industries that are ripe for digital transformation. *Insider Monkey*. https://www.insidermonkey.com/blog/5-least-digitized-industries-that-are-ripe-for-digital-transformation-1150942/?singlepage=1

Duncan, C. (2024, April 2). Cybersecurity in banking: 5 biggest threats in 2025. *DeskAlerts Blog*. https://www.alert-software.com/blog/cybersecurity-in-banking

e-Governance Academy. (n.d.). National cyber security index. *NCSI*. https://ncsi.ega.ee/ncsi-index/

European Central Bank (ECB). (2024, July 26). Cyber resilience in the banking sector. *ECB Banking Supervision Blog*. https://www.bankingsupervision.europa.eu/press/blog/2024/html/ssm.blog240726~7bfb4e2267.en.html

European Commission. (2022, December 27). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union*. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

European Union. (2016, May 4). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Union Agency for Cybersecurity (ENISA). (2023). Cybersecurity in the healthcare sector: Threat landscape. *ENISA*. https://www.enisa.europa.eu/publications/cybersecurity-in-healthcare-sector

European Union Agency for Cybersecurity (ENISA). (2022). Financial sector cybersecurity: Threat landscape. *ENISA*. https://www.enisa.europa.eu/publications/financial-sector-cybersecurity-threat-landscape

Gandhi, P., Khanna, S., & Ramaswamy, S. (2016, April 1). Which industries are the most digital (and why)? *Harvard Business Review*. https://hbr.org/2016/04/a-chart-that-shows-which-industries-are-the-most-digital-and-why

GlobalSign. (n.d.). Difference and similarities: Digitization, digitalization, and digital transformation. https://www.globalsign.com/en/blog/difference-and-similarities-digitization-digitalization-and-digital-transformation

Grand View Research. (2025, February). *Cyber security market size, share & trends analysis report by offering (hardware, software, services), by security (endpoint security), by organization size (large enterprises), by deployment (cloud), by solution, by end use, by region, and segment forecasts, 2025–2030* [Industry report]. https://www.grandviewresearch.com/industry-analysis/cyber-security-market

Honeywell. (2023, November). What is digitalization? And why is it important?. *Honeywell*. https://www.honeywell.com/us/en/news/2023/11/what-is-digitalization-and-why-its-important

Karanovic & Partners. (2025, May 16). *North Macedonia government approves key draft laws for digital future*. https://www.karanovicpartners.com/news/north-macedonia-government-approves-key-draft-laws-for-digital-future

Macedonian Banking Association (MBA). (2024). *Commission for information security*. https://mba.mk/w/en/events/commission-for-information-security

Manyika, J., Pinkus, G., & Ramaswamy, S. (2016, January 21). *The most digital companies are leaving all the rest behind*. McKinsey Global Institute. *McKinsey & Company*.

https://www.mckinsey.com/mgi/overview/in-the-news/the-most-digital-companies-are-leaving-all-the-rest-behind

Ministry of Digital Transformation. (2025, May 15). Gov't approves electronic communications and cybersecurity laws. *MIA News Agency*. https://mia.mk/en/story/ministry-of-digital-transformation-govt-approves-electronic-communications-and-cybersecurity-laws

Oentoro, A. (2024, January 11). Digitization, digitalization, and digital transformation explained. *Agility CMS*. https://agilitycms.com/blog/digitization-digitalization-and-digital-transformation-explained

Security Boulevard. (2024, June). *Cybersecurity in banking*. https://securityboulevard.com/2024/06/cybersecurity-in-banking/

Schniering, M. (2023, September 13). Five ways to beat the odds on digital transformation. Boston Consulting Group. https://www.bcg.com/news/13september2023-five-ways-to-beat-odds-on-digital-transformation

TransforMe.AI. (2025, April 15). *Why 70% of digital transformation projects fail—and how to beat the odds*. https://transformeai.com/2025/04/15/why-70-of-digital-transformation-projects-fail-and-how-to-beat-the-odds/

Van Tonder, C., et al. (2023). Internal organizational factors driving digital transformation for business model innovation in SMEs. *Journal of Business Models, 11*(2), 86–109. https://www.researchgate.net/publication/373483456_Internal_organizational_factors_driving_digital_transformation_for_business_model_innovation_in_SMEs

Weisser H.C. & Nagyfejeo, E. (2018). Cybersecurity Capacity Review Former Yugoslav Republic of Macedonia (FYR Macedonia). *SSRN Electronic Journal*. https://www.researchgate.net/publication/344018776_Cybersecurity_Capacity_Review_Former_Yugoslav_Republic_of_Macedonia_FYR_Macedonia

World Economic Forum. (2025, January 13). *Global cybersecurity outlook 2025*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf