Professional paper

APPLICATION OF THE NIS 2 DIRECTIVE AND THE CYBERSECURITY ACT IN ESSENTIAL AND IMPORTANT ENTITIES

Tomić Rotim, S.[1], **Landeka, K.**[2]

[1]Zavod za informatičku djelatnost Hrvatske, University of Applied Sciences Velika Gorica, stomic@zih.hr
[2]University of Applied Sciences Velika Gorica, katarina.landeka@vvg.hr

Abstract: *The aim of this article is to provide a clear understanding of the regulatory landscape in the field of cybersecurity. In today's era of increasing cyberattacks, the EU has recognized the associated risks and taken necessary measures to regulate this domain. One such measure is the adoption of the NIS 2 Directive, which aims to establish a uniform cybersecurity standard across the EU. This paper seeks to elucidate the regulatory framework, standards, and guidelines that can assist all entities required to comply with the NIS 2 Directive in effectively implementing the necessary organizational and technical security measures. The proactive adoption of the NIS 2 Directive is essential for building a resilient and secure digital environment across the EU. By understanding and applying the principles outlined in this paper, organizations can safeguard their operations against the evolving landscape of cyber threats and contribute to the collective security of the European digital ecosystem.*

Keywords: *cybersecurity, NIS 2, security measures, cyber risks*

1. INTRODUCTION

The NIS 2 Directive (European Parliament and Council, 2022b) and the Cybersecurity Act *(Croatian Parliament, 2024)* are key components of the EU's regulatory framework designed to strengthen the cybersecurity of essential and important entities. The Directive on measures for a high common level of security of network and information systems (NIS 2) is an upgrade of the previous directive (NIS), aimed at enhancing the EU's cyber resilience. NIS 2 covers a broader range of sectors, including digital services, energy, transport, healthcare, and financial services, and adds new sectors such as postal and courier services, waste management, and chemical production.

This paper will focus on describing the directive and law, their application, and the obligations and challenges that entities face. Additionally, it aims to provide an effective methodology that can assist essential and important entities in implementing this directive and law. This will create the prerequisites for more successful implementation of cybersecurity measures in these entities, thereby raising the level of cybersecurity at the EU level.

NIS 2 distinguishes between essential and important entities. Essential entities are those whose interruption or disruption of service could have a significant impact on public welfare,

health, safety, or economic stability. Important entities, although having a lesser impact, are still vital for societal and economic activities.

2. PROBLEM ANALYSIS

In our modern world, where the invisible threads of the digital realm weave through every facet of our lives, the importance of cybersecurity cannot be overstated. The digital age, with all its marvels and conveniences, brings with it a shadowy counterpart—an array of cyber threats that lurk in the depths of the internet, poised to exploit any vulnerability.

Cybersecurity is not merely a technical concern relegated to the IT department of an organization. It is a vital shield that protects the very essence of our digital existence. Personal information, financial transactions, critical infrastructure, and even national security are intertwined within the vast networks of cyberspace. Without robust cybersecurity measures, these precious assets are left vulnerable to the predations of malicious actors, whose intentions range from mere mischief to malevolent sabotage.

The importance of cybersecurity lies in its role as a guardian of trust. In the absence of trust, the digital economy would crumble. Consumers rely on the assurance that their private information is secure when they shop online, communicate through social media, or conduct banking transactions. Businesses depend on the stability and security of their digital operations to maintain competitiveness and credibility. Governments need to protect national security and ensure the integrity of essential services, from healthcare to energy supply.

Furthermore, the interconnected nature of our world means that a breach in one area can have cascading effects, leading to widespread disruption and damage. A cyber attack on a single utility provider, for example, could result in power outages affecting millions, causing chaos and endangering lives. The ripple effects of such incidents can be profound, underscoring the necessity for comprehensive and proactive cybersecurity strategies.

Implementing adequate cybersecurity measures is akin to fortifying a castle against invaders. It involves not only erecting formidable barriers but also maintaining vigilance through constant monitoring and swift responses to emerging threats. It requires a culture of security awareness where individuals and organizations alike recognize the value of their digital assets and the potential risks they face. It is important to reimagine awareness efforts, making them more engaging and effective in fostering a culture of cybersecurity across organizations and societies (Bada, M., Sasse, M. A., Nurse, J. R., 2021).

In essence, caring about cybersecurity is about preserving the integrity, confidentiality, and availability of the digital realm that has become integral to our daily lives. It is about ensuring that the digital wonders we have come to rely upon remain secure, allowing us to navigate this brave new world with confidence and peace of mind.

2.1. ANALYSIS OF THE PROBLEM FROM THE PERSPECTIVE OF THE EU

The European Union places significant emphasis on protection against cyberattacks and enacting regulations in this domain due to the profound implications such threats have on our interconnected world. In this digital era, where information flows as freely as air and data serves as the lifeblood of society, the EU recognizes that the integrity and security of cyberspace are paramount to the well-being and progress of its member states. There is the

need for harmonized frameworks to address inconsistent cybersecurity practices among member states while fostering innovation. It is important to balance strict cybersecurity measures with the flexibility required for technological advancement (Chertoff, M., Simon, 2021).

Firstly, the digital infrastructure underpinning our societies is a vast and intricate web, supporting everything from communication networks to financial systems, healthcare services to critical utilities. A single breach in this delicate fabric can trigger a domino effect, disrupting essential services, eroding public trust, and potentially causing significant economic and social upheaval. Thus, the EU understands that safeguarding this infrastructure is not merely a technical necessity but a fundamental imperative for societal stability and prosperity.

Moreover, the EU's commitment to cybersecurity reflects its broader values of privacy, democracy, and the rule of law. In a world where data is increasingly weaponized, ensuring that personal information remains private and secure is essential to protecting individual freedoms and human rights. Cyberattacks that compromise personal data or manipulate digital information can undermine democratic processes, erode trust in public institutions, and threaten national security. Therefore, robust cybersecurity measures are crucial in preserving the democratic fabric and upholding the rule of law across Europe.

The enactment of regulations, such as the NIS 2 Directive, is a testament to the EU's proactive stance in this arena. These regulations aim to create a unified and resilient framework that enhances cooperation and coordination among member states, ensuring that all adhere to a high standard of cybersecurity practices. By harmonizing efforts and establishing clear guidelines and obligations, the EU seeks to fortify its defenses against an ever-evolving landscape of cyber threats.

Furthermore, the EU's regulatory approach addresses the need for preparedness and adaptability. Cyber threats are not static; they evolve rapidly, becoming more sophisticated and pervasive. The EU's regulatory framework is designed to be dynamic, allowing for continuous improvements and swift responses to new challenges. This adaptability is essential in maintaining a robust defense posture that can anticipate and counteract emerging threats effectively.

In essence, the EU's emphasis on protection against cyberattacks and the enactment of regulations in this sphere stem from a profound recognition of the critical role that cybersecurity plays in ensuring the safety, stability, and prosperity of its member states. It is an acknowledgment that in safeguarding the digital frontier, the EU is not only protecting its infrastructure and economies but also its values, freedoms, and way of life.

The NIS Directive (Directive on the security of network and information systems) represented the first comprehensive legislation at the European Union level aimed at enhancing the overall cybersecurity landscape within the EU. However, several years into its implementation, various challenges and shortcomings were identified, prompting the adoption of a new directive, NIS 2. The primary issues with the original NIS Directive were as follows:

- *Inconsistent Application Among Member States*: Different member states adopted varied approaches to implementing the directive, resulting in uneven levels of security and protection across the EU.
- *Limited Scope*: The NIS Directive covered only specific sectors (such as energy, transport, banking, and healthcare) and providers of essential digital services, leaving many other critical sectors and services outside its purview.
- *Unclear Criteria for Identifying Key Operators*: The criteria for designating key operators were not sufficiently clear, leading to uncertainty and inconsistency in determining which entities fell under the directive's jurisdiction.
- *Lack of Resources and Capacities*: Many member states lacked the necessary resources or capacities to effectively implement the directive and to respond adequately to cyber threats.
- *Insufficient Coordination and Collaboration*: The NIS Directive did not adequately promote cooperation and information sharing between member states, which was crucial for effectively addressing cross-border cyber threats.
- *Limited Adaptability to Emerging Threats*: Given the rapid evolution of cyber threats, the NIS Directive was not flexible enough to quickly adapt to new challenges.

3. METHODS

3.1. APPLICABLE REGULATIONS IN EU

In today's interconnected digital landscape, the importance of robust cybersecurity cannot be overstated. To safeguard sensitive data, critical infrastructure, and the seamless functioning of our societies, comprehensive regulatory frameworks have been established. This chapter delves into the key regulations and directives that form the backbone of cybersecurity across various sectors, highlighting their objectives, key provisions, and the overarching need for a unified and resilient approach to countering cyber threats.

The European Union has established a comprehensive framework of regulations and directives aimed at enhancing cybersecurity across its member states. Here are some of the key regulations and frameworks:

- NIS 2 Directive (European Parliament and Council, 2022b)

The Directive (EU) 2022/2555, known as NIS 2 Directive (EU Directive, 2022), aims to elevate the common level of cybersecurity across the European Union. It replaces the earlier Directive (EU Directive, 2016), enhancing previous frameworks and addressing emerging challenges in the cybersecurity landscape. The Directive emphasizes the importance of cybersecurity in ensuring the functioning of the internal market and the continuity of economic activities, highlighting the need for coordinated and innovative responses to the expanding cyber threat landscape. It aims to reduce fragmentation within the internal market by setting out minimum rules and mechanisms for cooperation among Member States, updating the list of sectors subject to cybersecurity obligations, and providing effective remedies and enforcement measures. Overall, the NIS 2 Directive is a significant step

towards a unified and resilient cybersecurity framework within the EU, aiming to safeguard the digital infrastructure and promote a secure digital market.

- General Data Protection Regulation (European Parliament and Council, 2016)

The General Data Protection Regulation (EU Regulation, 2016) represents a comprehensive initiative by the European Union to enhance data protection for all individuals within the EU and the EEA. It aims to unify privacy laws across Europe, boosting individual control over personal data while imposing strict rules on those hosting and 'processing' this data anywhere in the world. The GDPR enhances transparency regarding the processing of personal data and sets out clear consent requirements. It strengthens individuals' rights by ensuring access to data, the right to erase, restrict processing, and port data. Organizations must incorporate data protection from the design stage of system development, and they are obliged to report data breaches within tight deadlines. The regulation's scope is global, affecting any organization handling data of EU residents. Severe penalties for non-compliance highlight its emphasis on protecting data privacy and ensuring data security.

- Cybersecurity Act (European Parliament and Council, 2019)

The Cybersecurity Act (EU Regulation, 2019) represents a substantial evolution in European cybersecurity policy, enhancing the European Union Agency for Cybersecurity (ENISA) and introducing a new framework for ICT cybersecurity certification. This regulation seeks to address the increasing complexity and pervasiveness of cyber threats by bolstering cybersecurity standards across the EU. Its primary objectives are to establish ENISA as a permanent agency, provide it with a strong mandate to improve the cybersecurity posture of the EU, and create a harmonized certification framework for ICT products, services, and processes. This unified certification is intended to raise the security levels across the digital market, instilling greater trust and ensuring a high standard of cybersecurity practices among member states. The act emphasizes resilience and response to cyber threats and stresses the importance of a collective effort in elevating the cybersecurity readiness of the EU.

- Digital Operational Resilience Act (European Parliament and Council, 2022c)

The Digital Operational Resilience Act (DORA) is a comprehensive regulation aimed at strengthening the digital operational resilience of financial entities in the European Union. The regulation addresses various aspects of information and communication technology (ICT) risk management to ensure that financial entities can withstand, respond to, and recover from all types of ICT-related disruptions and threats. DORA aims to enhance the stability and integrity of the EU's financial system by ensuring that financial entities are prepared to handle ICT disruptions effectively. This proactive approach to ICT risk management is designed to protect both financial institutions and their customers from the growing threats in the digital landscape.

- eIDAS Regulation (European Parliament and Council, 2014)

The eIDAS Regulation aims to enhance trust in electronic transactions within the internal market by providing a secure foundation for electronic interactions between citizens, businesses, and public authorities. It addresses the legal recognition of electronic identification and trust services, ensuring electronic transactions are as secure as traditional paper-based processes. The regulation establishes a legal framework for electronic signatures, seals, time stamps, electronic documents, and registered delivery services, mandating mutual recognition of electronic identification schemes across EU member states. This promotes cross-border digital services and ensures that electronic signatures and other trust services have the same legal status as their paper-based counterparts.

- Digital Markets Act (European Parliament and Council, 2022a).

This regulation aims to ensure contestable and fair markets in the digital sector, benefiting businesses and consumers in the European Union. Its key objectives are to ensure the proper functioning of the internal market by establishing harmonized rules that create fair markets where gatekeepers are present, promoting innovation and high-quality digital products and services, ensuring competitive prices and a wide choice for end users, and addressing the adverse impacts of unfair practices on the internal market. It seeks to create regulatory safeguards against the unfair practices of gatekeepers and facilitate cross-border business within the Union.

These regulations and frameworks collectively form a robust approach to enhancing cybersecurity within the European Union, ensuring that both public and private sectors are well-equipped to face the challenges posed by the rapidly evolving digital landscape.

3.2. APPLICABLE STANDARDS AND FRAMEWORKS IN CYBERSECURITY

In an era where cyber threats are ever-evolving and increasingly sophisticated, adherence to established standards and frameworks is crucial for ensuring robust cybersecurity practices. This chapter explores the key standards and frameworks that provide comprehensive guidelines and best practices for managing and securing information systems, enhancing resilience, and mitigating risks across diverse industries. By delving into these foundational elements, we uncover the strategies that organizations can employ to safeguard their digital assets and maintain the integrity of their operations.

- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls
- ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks
- ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- ISO/IEC 27032:2023 Cybersecurity — Guidelines for Internet security
- ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

- ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC TS 27110:2021 Information technology, cybersecurity and privacy protection, Cybersecurity framework development guidelines
- ISO/IEC TS 27100:2020 Information technology – Cybersecurity - Overview and concepts
- ISO 22313:2020 Security and resilience - Business continuity management systems - Guidance on the use of ISO 22301
- ISO/IEC 27031:2011 Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity

3.3. APPLICABLE REGULATIONS IN CROATIA

Croatia has established a comprehensive legal framework to address cybersecurity, reflecting its commitment to safeguarding digital infrastructures and data across various sectors. This framework encompasses several key regulations and directives, each serving specific aspects of cybersecurity management and response:

1. *Electronic Communications Act (Croatian Parliament, 2022):* This legislation governs the security of electronic communications networks and services. It mandates service providers to implement technical and organizational measures to manage risks to network security and to report significant security breaches to the relevant authorities.
2. *Act on the implementation of the GDPR (Croatian Parliament, 2018):* Croatia enforces the EU's GDPR through national legislation, which includes provisions for the security of personal data. This act requires data controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
3. *National Cyber Security Strategy (Government of the Republic of Croatia, 2015):* This strategic document outlines the overarching goals and objectives for cybersecurity in the country. It aims to strengthen the resilience of national information systems and critical infrastructure, promote cybersecurity awareness and education, and enhance collaboration between the public and private sectors.
4. *Cybersecurity Act (Croatian Parliament, 2024):* Designed to establish and maintain a high common level of cybersecurity across all critical sectors. It defines procedures and measures for achieving and sustaining this security standard and specifies criteria for categorizing entities subject to these regulations. The law emphasizes the importance of strategic planning and decision-making within the realm of cybersecurity, setting national frameworks for managing significant cyber incidents and crises. It is aligned with the EU's Directive on the security of network and information systems (NIS 2).

5. *Critical Infrastructure Act (Croatian Parliament, 2013):* Although broader in scope, this regulation is crucial for cybersecurity as it identifies and protects infrastructure vital to maintaining crucial societal and economic activities. It mandates the implementation of security measures to prevent, mitigate, and manage cyber threats.
6. *Information Security Act (Croatian Parliament, 2007):* This law governs the protection of information assets that are not personal data within public administration bodies. It provides guidelines for the security of such information, including measures against cyber threats.
7. *Act on the Implementation of Regulation on Electronic Identification and Trust Services for Electronic Transactions (Croatian Parliament, 2017):* This set of regulations implements the EU's eIDAS Regulation, providing a framework for electronic identification and trusted services used in electronic transactions, which includes ensuring the security of related services.

These laws and regulations form the backbone of Croatia's approach to cybersecurity, ensuring a coordinated and robust defense against cyber threats while aligning with European Union standards and directives. They reflect an evolving cybersecurity landscape where continuous improvement, education, and cooperation are key to maintaining security and trust in digital environments.

Below is more information about the Cybersecurity Law. It is designed to establish and maintain a high common level of cybersecurity across all critical sectors. It defines procedures and measures for achieving and sustaining this security standard and specifies criteria for categorizing entities subject to these regulations. The law emphasizes the importance of strategic planning and decision-making within the realm of cybersecurity, setting national frameworks for managing significant cyber incidents and crises.

Key objectives include:

1. Enhancing Cybersecurity Protections: By developing and continuously improving cybersecurity policies and their implementation, the law aims to safeguard critical infrastructures and sensitive information against cyber threats and vulnerabilities.
2. Building National Capabilities: The legislation mandates the development of national capabilities in cybersecurity, enhancing the skills and technologies available to public and private sector entities.
3. Promoting Public and Private Collaboration: The law encourages cooperation and coordination among all relevant bodies, fostering a collaborative environment to tackle cybersecurity challenges effectively.
4. Advancing Technology and Education: It supports the advancement and integration of relevant, innovative technologies, and the development of educational programs to raise awareness and train personnel in cybersecurity practices.

Overall, the law seeks to protect essential social and economic activities and ensure the smooth functioning of the internal market through robust cybersecurity management and response strategies.

3.4. HOW TO IMPLEMENT NIS 2?

NIS 2 requires entities to take specific technical and organizational measures to manage cyber risks, regularly assess and improve their security policies, and report incidents to competent authorities. To successfully implement this, an overview of the necessary steps is provided below:

- Initial assessment and analysis: Analyzing existing security measures, policies, and procedures in relation to the requirements of NIS 2.
- Asset inventory and risk management: Entities must regularly conduct risk assessments and vulnerability testing. Based on this, it is necessary to prepare a Risk treatment plan with the necessary organizational and technical measures.
- Implementation of the organizational and technical measures from the Risk treatment plan:
    - Development of Security policy: It is necessary to establish and implement security policies and procedures. Establish the security team.
    - Implement Incident management: It is necessary to establish and maintain the ability to manage incidents. Entities are obliged to report significant incidents to the competent national authorities.
    - Develop Business continuity plan: Conduct Business impact analysis and implement Business continuity plan.
    - Implement technical measures: Identify and implement adequate technical measures (Firewall, IPS, DLP, MFA, SIEM, VPN, Antivirus, Encryption, etc).
    - Implement all other security measures identified in the process of risk management.
- Awareness and training: Organizations must ensure awareness and training for employees about cybersecurity.
- Continuous monitoring and improvement: Applying the principles of continuous improvement (e.g., PDCA cycle) to regularly update and upgrade security measures and policies.

In the implementation process, companies may face the following challenges:

- Technical complexity: The use of advanced technologies and complex information systems can make the implementation of appropriate security measures difficult.
- Continuous compliance: The dynamic nature of cyber threats requires constant updates and adjustments to security practices.
- Resources: Ensuring sufficient financial and human resources to establish and maintain high security standards can be challenging, especially for smaller organizations.
- International cooperation: As cyber incidents often cross borders, international cooperation and information exchange are key to effective risk management.

4. DISCUSSION AND CONCLUSION

The adoption of the NIS 2 Directive was aimed at addressing the issues related to NIS Directive and achieving a higher level of cybersecurity within the EU. Key improvements introduced by the NIS 2 Directive include:

- *Broadened Scope*: NIS 2 encompasses a wider range of sectors and services, including those not covered by the original directive.
- *Stricter Security Requirements*: The directive imposes more stringent security requirements on organizations within its scope.
- *Enhanced Cooperation*: The new directive emphasizes the need for better collaboration and information sharing among member states.
- *Clearer Criteria and Obligations*: It provides clearer criteria for identifying key operators and delineates their cybersecurity responsibilities more explicitly.

The NIS 2 Directive represents a significant step forward in creating a more secure digital environment within the European Union. In conclusion, the timely and strategic preparation for the NIS 2 Directive implementation cannot be overstated. By conducting a comprehensive GAP analysis, organizations can pinpoint the exact areas that need attention and improvement. Moreover, a detailed risk assessment will highlight potential vulnerabilities and the essential security measures that need to be in place. This proactive approach not only ensures compliance with the Directive but also significantly strengthens the overall cybersecurity posture of the entities involved. As cyber threats continue to evolve, such diligence in preparation and implementation will be paramount in safeguarding critical infrastructures and services, ultimately contributing to a more secure and resilient digital landscape.

5. REFERENCES

Bada, M., Sasse, M. A., Nurse, J. R., Cybersecurity Awareness Campaigns: Why Do They Fail? Journal of Cybersecurity, 7(1), tyab001, 2021.

Chertoff, M., Simon, A., Cybersecurity Regulatory Frameworks in the EU: Balancing Innovation and Protection. Journal of Cybersecurity Policy, 3(2), 45–62., 2021.

Croatian Parliament, Information Security Act, 18 July 2007.

Croatian Parliament, Critical Infrastructures Act, 2 May 2013.

Croatian Parliament, Act on the Implementation of Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, 19 June 2017.

Croatian Parliament, Act on the Implementation of the General Regulation on Data Protection, 3 May 2018.

Croatian Parliament, Electronic Communications Act, 1 July 2022.

Croatian Parliament, Cybersecurity Act, 26 January 2024.

European Parliament and Council, Regulation (EU) on electronic identification and trust services for electronic transactions in the internal market, 23 July 2014.

European Parliament and Council, Regulation (EU) 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), 27 April 2016.

European Parliament and Council, Regulation (EU) on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act), 17 April 2019.

European Parliament and Council, Regulation (EU) on contestable and fair markets in the digital sector (Digital Markets Act), 14 September 2022 a.

European Parliament and Council, Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), 14 December 2022 b.

European Parliament and Council, Regulation (EU) on digital operational resilience for the financial sector (DORA), 14 December 2022 c.

Government of the Republic of Croatia, The National Cyber Security Strategy of the Republic of Croatia, 7 October 2015.